FUJITSU Server Plug-ins for Nagios Core

FUJITSU Server Plug-ins V3.50 for Nagios Core

Interface Documentation

March 2018 Edition

Keywords
ServerView, Nagios, Icinga, PRIMERGY, Blade, PRIMEQUEST, RAID, CIM, iRMC, RackCDU

CONTENTS

1 Introduction

"**FUJITSU Server Plug-ins for Nagios Core**" is a collection of scripts, sample configurations and more for a Nagios Core integration and all products based on Nagios Core.

These elements can be used for Nagios, Icinga V1.x series, SM-Box or other Nagios Core based variants for enhancements for Fujitsu servers.

Monitoring:

The scripts whose file names start with **check_fujitsu** can be used as Nagios Plugins. These scripts can be used standalone but are meant to be executed as Nagios Core Plugins scheduled by the Nagios daemon.

With these plugins you can see an overall hardware status of your PRIMERGY servers as well as in-depth details such as power consumption, temperatures, fan speed, and hardware issues.

Supported protocols: SNMP, CIM and REST.

Monitoring is enabled via host address or iRMC address.
Requirements for this see "Local Requirements".

Additional Tools:

- **tool_fujitsu**
  The scripts whose file names start with **tool_fujitsu** are for connection and type checks of one server.
- **discover_fujitsu**
  With the **discover_fujitsu** script, any amount of hosts and any connection protocol type can be checked and Nagios hosts configuration files can be generated.
- **inventory_fujitsu**
  The **inventory_fujitsu** script can be used to get unscheduled inventory information of systems.
- **cimindication/**
  The files under the 'cimindication' directory are tools to handle ServerView CIM indications.
- **updmanag_fujitsu**
  The scripts whose file names start with **updmanag_fujitsu** are for update management.

These scripts can be used standalone.

Supported protocols: SNMP, CIM and REST.

Sample Nagios Configurations:

A set of sample and template Nagios Core configuration files show the usage of the monitoring scripts.
With regard to the configuration elements and descriptions this document is based on Nagios and Icinga documentations.

The full description of the Nagios configurations and Nagios Plugins can be found in
"Nagios Core Version 3.x Documentation " at http://www.nagios.org
For Icinga, all documentations can be found at http://docs.icinga.org/

1.1 Change History

Date	Version	Comment
2012-07	1.0	Start of this document.
2013-03	1.10	ServerView RAID support, script extensions.
2013-08	1.20	Script extensions for IPv6 and performance values for file systems and network interfaces.
2013-12	2.00	Monitoring of update agent status, support of SNMP trap configuration files for snmptt, new plug-in for support of ESXi CIM provider via CIM-XML protocol.
2014-04	2.10	Support of ServerView CIM providers on any server, new tool script for the CIM access tests of servers.
2015-01	3.00	New script for discovery of Servers (check of server types and generation of configurations), support in monitoring via iRMC for iRMC S4 with firmware version V7.3 or higher.
2015-05	3.10	Liquid Pump monitoring via SNMP, detecting ServerView SystemMonitor URL, enhanced update monitoring information, enhanced server discovering.
2015-11	3.20	Added support of a new SNMP mib for ServerView agent monitoring and new SNMP monitoring for RackCDU™ (Liquid Cooling Managing). Two new scripts: *FUJITSU Update Management CIM Tool* and *FUJITSU SNMP Server Inventory Tool*. New ServerView CIM Indication manager to get and handle ServerView CIM indications
2016-08	3.30	New support for REST services for monitoring. Available REST services are (in-band) ServerView Agents and component Server Control (SCCI) and (out-of-band) ServerView iRMC Report.
2017-06	3.40	New ESXi CIM support of ServerView RAID CIM Provider. iRMC CIM is no longer supported. Only identification checks are enabled. iRMC S5 support is identic to iRMC S4 support.
2017-12	3.50	New support of Redfish interface of iRMC S4 version 9 and iRMC S5.

1.2 Documentation

Reference	Document Title / Remarks
[1]	http://www.nagios.org
[2]	http://docs.icinga.org/
[3]	Manual about Update Agent Status: "ServerView System Monitor"
[4]	About wbemcli: http://sblim.sourceforge.net/
[5]	OpenWSMAN link: https://github.com/Openwsman/openwsman/wiki

1.3 How to Start

Select server nodes to be monitored:
The first step is to check what kind of server nodes are to be monitored. The server nodes might require different access protocols for the monitoring.

- **ESXi** requires CIM access
- (**PRIMERGY**) Server nodes where ServerView Agent is installed can be monitored via SNMP, CIM or REST:
  CIM requires additional installation of the ServerView CIM Provider.
  SNMP and REST support more data than CIM.
- Monitoring via **iRMC** address can be performed with SNMP protocol or via REST protocol and either REST-Report.xml interface or the Redfish interface, depending on which interface is enabled in iRMC.
  REST-Report.xml support is referred to in this document as “iRMC Report” or “out-of-band REST-Report”.
  Redfish support is referred to in this documents as "iRMC Redfish".

  SNMP and Redfish support more data than REST-Report.xml.
  The amount of data depends on whether ServerView Agent or ServerView Agentless Service has been installed on the base server.

  There is no Fujitsu -specific Plugin for access via IPMI, since there are other IPMI plugins to fetch and handle data of single sensors.
- **PRIMERGY BLADE** MMB requires SNMP access
- **PRIMEQUEST** MMB requires SNMP access
- **RackCDU** MMB requires SNMP access

Prerequisites for required protocols:
There are separate scripts for each access protocol because each protocol type requires different prerequisites

Install the required software, depending on the protocols needed - see previous step.

- SNMP - requires Perl Net::SNMP class
- CIM - requires command wbemcli or OpenWSMAN Perl Class and library
  (This is dependent on the service type on the server node)
- REST - requires the curl command

For more details of these requirements, see chapter link “Requirements”.

Collect and Store Authentication:
The SNMPv3, CIM and REST interfaces require as a rule authentication data. The script plugins support storing all security relevant script options in an "Option Input File" for each authentication usage. This file must be readable for the scripts and writable for the administrator, but should not be accessible to anyone else.
For more details about security see chapter link “Security Hints”

How to use the scripts:
This document contains a description of all scripts, to show which options are available and what kind and quantity of data can be obtained.

Nagios Core Integration:
The scripts can be used stand alone or some can be used in a Nagios Core based environment. Therefore one step is to decide whether you want integration or not.

For Nagios Core integration, the Nagios sample configuration files can be used.

Discovery of server nodes:
A discovery tool is available for administrators who want to scan server addresses for server type and protocol abilities. This tool generates Nagios configuration files which are based on definitions of the sample configuration files of the FUJITSU Server Plug-ins.

1.4 Protocol Overview (SNMP, CIM, REST)

The first type of protocol supported by the FUJITSU Server Plug-ins is **SNMP**. SNMPv3 has more scope than SNMPv2c to specify and use authentication parameters.

CIM is a standard protocol based on object oriented principles. The current base services for CIM embedded in CIM-XML and for CIM embedded in a WS-MAN protocol are slower than SNMPv2c. The base services are SFCB, Pegasus or WinRM (Windows Remote Manager).

REST is the newest technique. With JSON as the data format, the amount of data is less than with CIM. The performance of the REST services depends on the REST service type itself. In the case of ServerView Agent Server Control (SCCI), it is as fast as SNMPv2c but uses SSL and authentication abilities instead of simple "community".
The iRMC Report service is of interest if SNMP is disabled on an iRMC node.
The iRMC Redfish service supports data similar to SNMP enhanced for driver monitor and storage parts.

Overview of supported features, protocol and server type

	SNMP	**CIM**	**REST**
Monitoring (in-band)	PRIMERGY Linux, Windows PRIMERGY Blade and Status of blades inside PRIMEQUEST	PRIMERGY Linux, Windows and ESXi	PRIMERGY Linux, Windows
(out-of-band)	iRMC S4/S5		iRMC S4/S5
Extended Performance *	PRIMERGY Linux, Windows		PRIMERGY Linux, Windows
Update Management		PRIMERGY Linux, Windows	PRIMERGY Linux, Windows
Inventory	PRIMERGY Linux, Windows		PRIMERGY Linux, Windows
Asynchronous Events	SNMP trap: PRIMERGY PRIMERGY Blade PRIMEQUEST	ServerView CIM indications: PRIMERGY ESXi	

* "Extended" means performance data of file system usage, physical memory usage, CPU usage (average if available) and network interface usage.

The type "**PRIMERGY"** in this table stands for all server nodes on which ServerView Agents or ServerView CIM Provider are installed.

Overview CIM and protocols

For CIM usage, wbemcli or OpenWSMAN can be used as "clients".

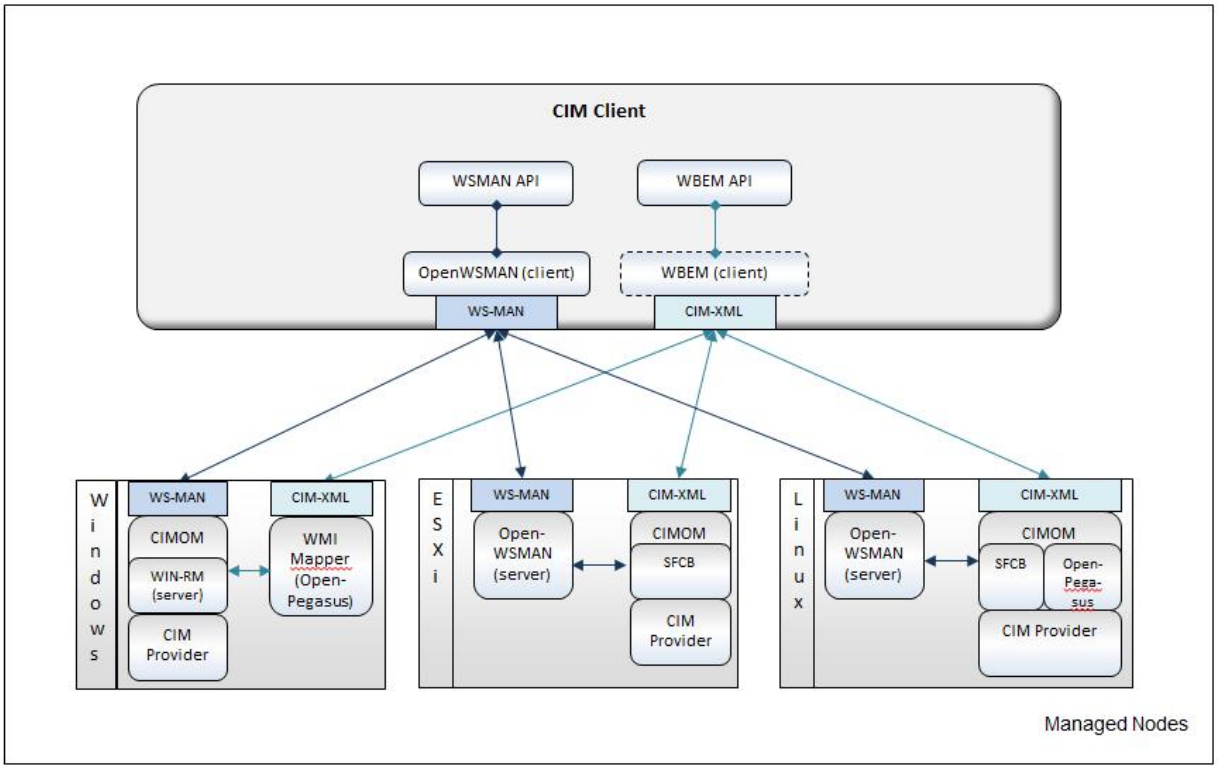


Figure: Protocol stacks

wbemcli – CIM-XML protocol:

The 'wbemcli' command is used to access the CIMOM CIM-XML service. ESXi systems come with Small Footprint CIM Broker (SFCB) as the CIMOM, which is usually already configured such that it can be accessed via basic authentication (user and password) on port 5989 (https) - access to port 5988 for http is disabled by default. Other configuration is possible. For a general description, see e.g. 'Sfcb The Book'.

With OpenPegasus, an alternative CIMOM CIM-XML service is available. This service can run on the same port numbers as sfcb.

Note:

wbemcli and *sfcb* resp. *OpenPegasus* are used as they are. For any problems running, configuring or using these tools, please refer to the originator.
This Plug-in relies on a configuration which is already set up for remote access via *wbemcli* executed on a Nagios-Core system.

Note:

There are newer CIM-XML services with disabled SSLv3 for the SSL protocol. These require wbemcli executable where TLS1 is enabled as the SSL protocol

You can check if wbemcli can access your system correctly by executing the following command lines:

wbemcli ei -nl -t -noverify 'https://root:password@host:5989/root/svs:CIM_ComputerSystem'

With this call you can also check if the given user and password authentication is accepted by the target CIM service.

Call wbemcli to get an SVS_PGY class to test if the ServerView CIM Provider information is available:

wbemcli ei -nl -t -noverify 'https://root:password@host:5989/root/svs:SVS_PGYComputerSystem'

OpenWSMAN Perl binding – WS-MAN protocol:

The Perl binding of OpenWSMAN is used to communicate with WS-MAN protocol services like OpenWSMAN service on ESXi or LINUX or Windows Remote Management (WinRM) on Windows.

The default ports are 5985 for http calls and 5986 for https calls.

The WinRM "Listener" must be configured and activated. WinRM listener must accept basic authentication (user and password).

You can check if OpenWSMAN can access your system correctly by executing the following command lines:

wsman identify -h host-P 5985 -u administrator -p password -y basic -V –v

OR for SSL usage:

wsman identify -b https://host:5986 -u administrator –p password -y basic -V -v

Call wsman to get an SVS_PGY class to test if the ServerView CIM Provider information is available:

wsman enumerate http://schemas.microsoft.com/wbem/wsman/1/wmi/root/svs/SVS_PGYComputerSystem -h host -P 5985 -u administrator -p password -y basic -V –v

With this call you can also check if the given user and password authentication is accepted by the target CIM service.

1.5 Monitoring - Supported Features and Capabilities

The FUJITSU Server Plug-ins are specially designed to monitor FUJITSU servers. They can be used as Nagios plugins within Nagios, Icinga V1.x series, SM-Box, or other Nagios Core variants.
With these plugins you can see an overall hardware status of your PRIMERGY servers as well as in-depth details such as power consumption, temperatures, fan speed, and hardware issues.

For SNMP, CIM and REST following information are available:

- Environment (fans resp. cooling devices and temperature sensors)
- Power supply and power consumption
- System board parts such as voltage, CPU, memory modules

(On some systems, not all component information is available.)

The following component information depends on the system type and the protocol type:

- DriverMonitor status (in-band via SNMP and REST, out-of-band via REST iRMC Redfish)
- RAID status (in-band SNMP and REST and in-band with CIM on ESXi. out-of-band via REST iRMC Redfish)
- Update agent status (not supported: out-of-band iRMC-Report or iRMC-Redfish)

The following blade types of a PRIMERGY Blade system can be monitored via the PRIMERGY management blade (SNMP only):

- Server blades
- IO-connection blades (e.g. the switch variants)
- KeyVideoMouse blades
- Storage blades

SNMP performance data: The FUJITSU Server Plug-in supports performance values and their thresholds if they are available in corresponding SNMP data.

- PRIMEQUEST MMB, PRIMERGY Blade MMB and PRIMERGY server temperature sensor (value and threshold)
- PRIMEQUEST power consumption (value and max-value)

- PRIMERGY Blade MMB power consumption (value)
- PRIMERGY server power consumption (value and threshold)
- PRIMERGY server "Physical Memory Usage" – special feature: the thresholds can be set as simple percent options
- PRIMERGY server "File System" – special feature: the thresholds can be set as simple percent options
- PRIMERGY server "Network Interface" – special feature: the thresholds can be set as simple KB/sec values

REST performance data: The amount of data depends on the REST service type.

- PRIMERGY server temperature sensor (value and threshold)
- PRIMERGY server power consumption (value and threshold)
- PRIMERGY server "Physical Memory Usage" – special feature: the thresholds can be set as simple percent options (only in-band)
- PRIMERGY server “File System” – special feature: the thresholds can be set as simple percent options
  (only in-band)
- PRIMERGY server “CPU usage average value” – special feature: the thresholds can be set as simple percent options
  (only in-band)

CIM performance data:

- Temperature sensor (value and threshold)
- Server power consumption (value and threshold if available)

Other available data

- RackCDU™ is a management system where the overall status and some sensor values can be monitored (via SNMP)

Overview table:

Available Data	PRIMERGY Server SNMP or REST	PRIMERGY Server CIM	PRIMERGY Blade MMB SNMP	PRIMEQUEST MMB SNMP	iRMC S4/S5 SNMP	iRMC S4 REST Report	iRM C S4-9/S5 Redfish
SUMMARY STATUS INFORMATION							
System	x	x	x	x	x	x	x
DriverMonitor	x	x					x
RAID	x	x (4)					x
Update	x	x					
INFORMATION ABOUT THE SYSTEM							
	x	x	x	x	x (2)	x (2)	x
SENSOR MONITORING AND PERFORMANCE							
Fan	x	x	x	x	x	x	x
Temperature	x	x	x	x	x	x	x
PSU	x	x	x	x	x (3)	x (3)	x
Voltage	x	x	x	x	x	x	x
CPU	x	x	x	x	x (2)	x (2)	x
Memory Mod.	x	x	x	x	x	x	x
Power Consumption	x	x (3)	x (3)	x (3)	x (3)	x	x
DriverMonitor Details	x						x
RAID Details	x						x
SPECIAL PERFORMANCE MONITORING							
Physical Memory	x						
File Systems	x						
Network	x						

NOTES:

PRIMERGY Blade MMB: Special monitoring of all blades inside is available (server blades, I/O blades, storage blades, KVM blades)
PRIMERGY Blade Server: Some component information is only assigned to the MMB and not available for a server blade
PRIMEQUEST Partition Server: Some component information is only assigned to the MMB and not available for the partition server

Footnotes

(1) Firmware V7.3 only - The Plugin must collect all sensor data and compute corresponding summary status values
(2) Some information is only available if ServerView Agent or ServerView Agentless-Service is installed or if the customer has added corresponding information via the Web UI
(3) No threshold values available
(4) ESXi only with firmware versions of the year 2017 or later

2 Requirements

2.1 Local Requirements and Installation

2.1.1 SNMP

On the Nagios/Icinga installation server, **Perl Net::SNMP** must be available.

For **IPv6,** Perl Net::SNMP V5.2 or higher must be available together with Perl Socket6 v0.23 or higher.

For **SNMPv3,** additional Perl modules are required:

Quote from the original cpan page: "The non-core modules *Crypt::DES*, *Digest::MD5*, *Digest::SHA1*, and *Digest::HMAC* are required to support SNMPv3."

For the full list of Net::SNMP requirements see

http://search.cpan.org/~dtown/Net-SNMP-v6.0.1/lib/Net/SNMP.pm#REQUIREMENTS

2.1.2 CIM

For CIM usage, wbemcli or OpenWSMAN can be used.

- **sblim-wbemcli**

  The WBEM Command Line Interface is a convenient, standalone systems management utility for CIMOM access which does not require any further CIM client library.

  All OS distributions include wbemcli.
  The newest build version can be downloaded from:
  http://download.opensuse.org/repositories/systemsmanagement:/wbem

- The most recent ESXi firmware supports TLSv1.0 by default. The wbemcli executable up to version V1.6.3 only supports SSLv3. It is necessary for the monitoring to use a wbemcli executable which is flexible regarding the SSL protocol unless ESXi is configured to allow SSLv3 again.
  A patch link for this can be found at http://sourceforge.net/p/sblim/bugs/2742/ .

- **OpenWSMAN**

  OpenWSMAN supports client and server features. For Nagios Core usage, the so-called "client" installation should be installed.

  Required packages for plugin usage:

  libwsman1, wsmancli, openwsman-perl
  OpenWSMAN Link:
  https://github.com/Openwsman/openwsman/wiki

  Download repositories:
  http://download.opensuse.org/repositories/Openwsman

  https://build.opensuse.org/project/show/Openwsman

  For additional installation and configuration tips see
  http://en.community.dell.com/techcenter/systems-management/w/wiki/4139.web-services-management-wsman-linux-client-installation-setup.aspx

2.1.3 REST

The **curl** command is used for the REST protocols.

For the ServerView Agent - Server Control service, port 3172 is used. Add this to the firewall for outgoing requests.

ServerView iRMC Report and iRMC Redfish uses port 443 (https) or, if required, port 80 (http).

Add the port usage to the local firewall configuration for outgoing requests.

2.2 Requirements for the Server to be monitored

2.2.1 SNMP Usage

The requirements depend on the server type:

- ServerView SNMP Agent V5 or higher
- Monitoring of ServerView Update Status is only available for ServerView SNMP Agent V6.20 or higher
- Any ServerView RAID version with enabled SNMP agent
- iRMC SNMP monitoring requires firmware V7.32 or higher
- PRIMEQUEST firmware from 2012 or later
- PRIMERGY Blade firmware from 2012 or later
- RackCDU and the ASETEK-RACKCDU firmware

There are three types of information to be monitored which can be fetched using the iRMC address for connection:

- iRMC agentless data independent of the OS installation on the server to be monitored. This is sometimes called “true agentless”
- Additional information from the ServerView Agent installed on the server to be monitored
- Additional information from the ServerView Agentless Service installed on the server to be monitored

2.2.2 CIM Usage

CIM support is available for server nodes where a CIM service is running and where corresponding CIM providers are installed:

- Linux or Windows with ServerView CIM Provider V6.30.04 (or higher)
- VMware® ESXi 5.x or higher with ServerView CIM Provider V6.21.08 (or higher)

CIM storage monitoring requires

- Monitoring RAID is supported with ServerView RAID Core Provider

CIM update management requires

- Linux or Windows -with ServerView CIM Provider V7.10.18 or higher

CIM indication requires:

- Windows with ServerView CIM Provider V7.10.18 or higher
- Linux ServerView CIM Provider V7.20.10 or higher
- ESXi - ServerView CIM Provider V7.20.01 or higher

CIM indication subscriptions requires:

- Linux or Windows with ServerView CIM Provider V7.10.18 or higher
- ESXi - ServerView CIM Provider V7.20.01 or higher

There are three types of information to be monitored which can be fetched using the iRMC address for connection:

- iRMC agentless data independent of the OS installation on the server to be monitored. This is sometimes called “true agentless”
- Additional information from the ServerView Agent installed on the server to be monitored
- Additional information from the ServerView Agentless Service installed on the server to be monitored

2.2.3 REST Usage

The requirements depend on the server type:

- ServerView SNMP Agent V7.10 or higher
- ServerView iRMC Report.xml monitoring requires firmware V8.24F or higher
- ServerView iRMC Redfish monitoring requires iRMC S4 V9 or iRCM S5 V1 or higher

2.3 Nagios Core Installation Hints

- To add the FUJITSU Server Plug-ins (so-called Nagios Plugins) to your Nagios installation, find **resource.cfg** within the Nagios/Icinga installation. This file contains the path variable **$USER1$**, whose value shows the path for the Nagios Plugins.
  Copy the scripts into this path and set the same access rights as for the other plugins.
- To integrate the Nagios configurations search the main configuration file of Nagios resp. Icinga. E.g. the file name is nagios.cfg or icinga.cfg for Nagios resp. Icinga user interfaces.

  One variant (Icinga example):

  ps –edalf | fgrep '**icinga.cfg**'

  This shows the Nagios daemon process and as the parameter the main configuration path used. Hint: Using the 'find' command does not help because there may be more than one file with the same name – only one is used by the Nagios daemon.
- In the Nagios main configuration path, check the **cfg_file** or **cfg_dir** directives.
  There are two waysto do this: Expand the existing configurations or add a new directory for the new ones.

  ATTENTION: Check the access rights – they should have the same rights as other configuration files.

  If configuration-tools such as NagiosQL are in use, then the configurations must be imported. (NagiosQL does not handle decentralized configurations well (seen in tests)).

3 Security Hints

3.1 Authentication and Credentials

There are servers which allow simple access for anyone via the SNMP community 'public'. Because of this the information "Community is public" is not really relevant to security.

There are other servers which allow only access, if other SNMP communities or other credentials like userid and password are set, and some require additional certificate handling as well.

The Nagios-Plugins need to know these credentials for each scheduled call.

The Nagios Core documents describe how to use 'resource.cfg' to set hidden information in this file, but resource.cfg only allows 32 user variables.

Solution for FUJITSU Server Plug-Ins:

Credential options can be specified and stored for the FUJITSU Server Plug-In usage:

The required options such as -u <userid> -p <password> (here CIM as an example) can be stored in an "Input Option File" including the '-<option>' syntax !

The required options depend on the script to be used (There a slightly different options for SNMPv3 than the ones for CIM operations). The descriptions can be found below for each script.

The "Input Option File" should only be writable for the administrator and must be readable for the script.

ATTENTION: It is RECOMMENDED that these files should not be readable by anyone else.

Example

This example is taken from an Icinga1 installation:

As part of its installation process, Icinga creates a /home/icinga directory, in which directory a subdirectory , e.g. 'AUTH' can be created:

```
drwxr-x---   5 icinga icinga 4096 Aug 26 11:59 AUTH
```

Files can be stored in this directoy – e.g. a CIM credential file:

```
-rw-r----- 1 icinga icinga 33 Aug 26 11:58 WIND09.txt
$ more WIND09.txt
-u administrator –pOurHiddenPassword
```

The CIM scripts can use this file with the option setting "-I /home/icinga/AUTH/WIND09.txt".

How to use:

This option setting can be stored in host definitions which require these credentials for monitoring.

Anyone who works with Nagios user interfaces can read the Nagios configurations, but with these definitions the user cannot read the credentials directly.

Credentials and access rights:

The scripts require simple read access – It is enough to choose community resp. user settings which allow read access.

Only the administrator requires read and write access.

NOTE: SNMPv3 usage hints

The user interface of iRMC V8 offers an SNMPv3 configuration page.: You can specify only one SNMPv3 password. This password must be set with the options **authpassword** and **privpassword**.

3.2 SSLv3 Usage and wbemcli (ESXi)

There are newer CIM-XML services with disabled SSLv3 to prevent attacks:

- ESXi CIM Service

These require a wbemcli executable where TLS1 is enabled as SSL protocol.
NOTE: wbemcli including V1.6.3 only supports SSLv3 and not TLS1!
For information on a source patch for wbemcli see http://sourceforge.net/p/sblim/bugs/2742/

Alternative - enable SSLv3:
Newer ESXi CIM Services work by default with disabled SSLv3. This service can be configured to enable SSLv3 again.
For further information on changing the ESXi configuration see
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2107293

3.3 ESXi Configurations and wbemcli

To enable monitoring via the scripts, it is necessary that the ESXi configuration enables HTTP Basic Authentication or HTTP Digest Authentication. Regarding configured SSL protocol and ciphers it must be ensured that the access via wbemcli is still available.

3.4 ServerView CIM Indication Listener and SHA1 Certificate

FUJITSU Server Plug-ins include a CIM indication listener, which uses a SHA1 default service certificate by default.This **SHA1** certificate is provided for **compatibility** reasons because most Linux operating systems do not currently support the SHA2 usage.

The default certificate can be replaced by administrators, e.g. with a SHA2 certificate, but it must be ensured that the local system and all services sending CIM indications can communicate with the listener which uses the new certificate.

4 Nagios Core Sample Configurations

These are sample configurations which might be copied or imported in the existing configurations. Not all Nagios Core systems monitor all kinds of FUJITSU server types, so the administrator should be free to integrate only required parts.

ATTENTION: – **Icinga2Changes** :

As the developers of Icinga2 have changed various interfaces., the sample configurations for the FUJITSU Server Plug-ins cannot be used as-is for Icinga2.

The following description assumes that **$USER1$** is the path of the plugins.

This description contains some predefined **Nagios/Icinga configurations**, which are printed in **blue**. If they do not exist, other, similar definitions should be used.

4.1 Sample Configurations

The FUJITSU Server Plug-ins provide sample configuration files. The contents of these files are mentioned in the descriptions below.

Sub-directory path: **cfg**.

There are several directories that provide monitoring for several server and protocol types that can be selected, e.g "SNMP", "CIM" and so on.

The central configuration of Nagios resp. Icinga or others allows the definition of **cfg_file** and **cfg_dir**. Select the parts which are to be used.

For the Nagios UI the central configuration file has the name nagios.cfg; for Icinga it is called icinga.cfg.

Newer versions of the ServerView Nagios Plug-In may add new directories in '**cfg**' and new host group definitions.

ATTENTION:

Be aware that the first configuration check might result in error messages if new host groups are added where no host is assigned. Because of this , you should only add host groups where at least one host is assigned.

Nagios Core configurations know several ways to deactivate configurations:

- Set 'register 0' in each definition to be ignored
- Rename the configuration file, e.g. by changing the file suffix "cfg"
- Move the corresponding configuration file to an area outside the configured **cfg_dir** paths
- Rename a configuration directory and add a dot before the directory name.

4.2 Nagios Host Groups and Service Definitions

The intention of FUJITSU Server Plug-ins is to specify a small number of Nagios services for a host group.

There are Nagios "hostgroup" definitions with Nagios "services" attached, which print collected monitoring information in one Nagios service.

There is one service definition for status, hardware components and performance data. (E.g. a combination of environment, power supply and consumption, system board and storage).

There are detailed or component-group host groups that are of interest if one or more servers is to have a monitoring service for each component group instead of one overall summary service (e.g. component group for "environment", "power", "system board", …). The names of these host groups contain the indication on "detail" or "group".

The 'services' described above are assigned to these host groups. The customer can choose which host group the specific 'host' is to be assigned to.

The FUJITSU Server Plug-ins have no sample host group definition with services for each individual component or single sensor. This would result in a large number of services for an assigned host node.

The Nagios administrator is free to write their own configurations to call the scripts of FUJITSU Server Plug-ins with the knowledge of these scripts described in this document.

4.3 Sample Configuration Files

There are central configuration files and there are configuration files for special features.

Here are some naming hints:

- "`command`" in the file name indicates on Nagios command definitions.
  The scripts of the FUJITSU Server Plug-ins are referenced in these definitions.
- "`hostgroup`" in the file name indicates on Nagios host group definitions

Notes on the central configuration files:

- cfg/serverview_commands_notify.cfg
  For details see chapter "Special Notification Command"
- cfg/serverview_hostgroups_ALL.cfg
  Detail:
  central host group combining all other host groups
- cfg/serverview_hosttemplates.cfg
  For details see chapter "Host Template for MMB WebServer Address or Option Settings" below
- cfg/serverview_servicegroups.cfg
  Detail:
  central service group definition

4.4 Host Template for MMB WebServer Address or Option Settings

Configuration file:

- cfg/serverview_hosttemplates.cfg

There is a Web address for calling the WebServer-interface for MMB. To add this, you can use a host template:

```
define host {
       name                            mmb-webaddress
       use                             generic-host
       notes_url                       http://$HOSTADDRESS$:80
       register                        0
}
define host {
       name                            primequest-webaddress
       use                             generic-host
       notes_url                       http://$HOSTADDRESS$:8081
       register                        0
}
```

SNMP:The following host template can be used to specify default or non-default options for the called check_fujitsu_server Plugin:

```
define host {
        name                            fujitsu-snmp-defaults
        #hostgroup                      all-fujitsu-servers
        use                             generic-host
        _SV_OPTIONS                     -Cpublic -p161
        # These are defaults - usable for SNMP2 or SNMP3 options
        register                        0
}
```

4.5 Sample Host Definitions

These configurations can be used for a 'host' if its definition configuration contains the assignment to a corresponding host group.

4.5.1 SNMP Host Samples

Here is a sample for a PRIMERGY Blade server:

```
define host {
        host_name                       BX600-3
        alias                           BX600-3
        display_name                    BX600-3
        address                         nnn.nnn.nnn.224
        parents                         servware.abg.fsc.net
        hostgroups                      primergy-blade-detail-servers
        use                             windows-server, mmb-webserv
        register                        1
}
```

Here is a sample for a PRIMERGY server (single node):

```
define host {
        host_name                       EC200S2C
        alias                           PRIMERGY Econel 200 S2
        address                         nnn.nnn.nnn.218
        parents                         servware.abg.fsc.net
        hostgroups                      primergy-servers
        use                             windows-server
        register                        1
}
```

4.5.2 CIM Host Samples

For CIM-XML usage:

```
define host {
        host_name                       PDB-ESXi-139
        address                         nnn.nnn.nnn.139
        hostgroups                      primergy-servers-CIM,linux-servers
        use                             linux-server
        #_SV_CIM_OPTIONS                 -uroot –p******
        _SV_CIM_OPTIONS                 -I/etc/authent/AuthentPDB.txt
        register                        1
}
```

For WS-MAN usage:

```
define host {
        host_name                       QA3-WIN-CIM-103
        address                         nnn.nnn.nnn.103
        hostgroups                      primergy-servers-CIM
        use                             windows-server
        SV_CIM_OPTIONS                 -UW -P5985 -IauthentQA3Win.txt
        register                        1
}
```

4.5.3 REST Host Sample

Here is a ServerView Agent REST sample:

```
define host {
        host_name       172.nnn.nnn.43_H50043LOVISSA_REST
        display_name    H50043Lovissa-REST
        address         172.nnn.nnn.43
        hostgroups      primergy-servers-REST-component-group,primergy-servers-
REST-update-monitor,primergy-servers-REST-drvmonitor
        use             windows-server
        _SV_REST_OPTIONS -SA  -I /home/icinga/AUTH/ABG/WINSW4.txt
        parents         servware.abg.fsc.net
        notes_url       https://172.nnn.nnn.143
        register        1
}
```

4.6 Special Notification Command

The notification commands seen in Icinga 1.5 only send $SERVICEOUTPUT$. The script for Fujitsu servers writes detailed information in the $LONGSERVICEOUTPUT$. Because of this it is **recommended** that this output is sent together with the summary information from the script in $SERVICEOUTPUT$.

Configuration file:

- cfg/serverview_commands_notify.cfg

Configuration sample:

```
define command {
        command_name                    notify-service-by-email-detail
        command_line                    /usr/bin/printf "%b" "***** Icinga
*****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService:
$SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState:
$SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
Info:\n\n$SERVICEOUTPUT$\n\nDetails:\n\n$LONGSERVICEOUTPUT$\n" | /bin/mail
-s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is
$SERVICESTATE$ **" $CONTACTEMAIL$
        register                        1
}
```

5 Common Options and Rules for All Scripts

There are several scripts in directory:
fujitsu/ServerViewSuite/Nagios/plugin

These scripts have common rules on how to print results and have common options for addressing, authentication and connection.

5.1 Common Rules for Printouts

A script always prints the **Nagios status** string at the beginning. This status string is printed in upper case letters.

The Nagiosstatus is followed by additional information (data, component and status values).

The original status values received by the remote provider are printed in lower case letters. Most components have more than the four Nagios status values.

Details will be printed after the first line – in Nagios this is part of the LONG_SERVICE_OUTPUT macro. This long output contains detail information in case of non-OK responses ("notifications").

It is advisable to send the Nagios macro LONG_SERVICE_OUTPUT along with notifications.

5.1.1 Text Rules for Automatic Scanning of Printouts

The following rules are used for printouts.

An example:

```
CRITICAL - ID=YKHNxxxxxx - Environment(ok) PowerSupplies(ok) MassStorage(ok)
Systemboard(majorfailure) DriverMonitor(ok)
ID=YKHNxxxxxx Name=h49006-tx120s2 Model="PRIMERGY TX120 S2" Location="Server
Room" Contact="Sysadmin (root@localhost)" AdminURL=http://n.n.n.106:80 OS="SLES
64-Bit" OSDescription="SUSE Linux Enterprise Server 11 SP3"
majorfailure: Voltage[0-0] Name=BATT_3.0V Current=2.31V Critical=2.48V Max=3.59V
```

Here is a short description for those who want to scan and analyze the text automatically.

- 1st line – the SERVER_OUTPUT line
  - Always start with
    <Nagios_status> OK, WARNING, CRITICAL, UNKNOWN

Rules for all lines:

- All status values which are NOT Nagios status are printed in lower case
- Key-Value-Pair print:
  <field>=<value>[<unit>]
- Value print
  If a value contains blanks, quotation marks are used.
  All other values may or may not have quotation marks.
- Status counter prints
  [<topic>-]<realstatus>(<counter>)-...

  Sample: CRITICAL Server-critical(1)-standby(11)
  ... for checking of PRIMERGY Server Blades via MMB

In the subsequent lines, LONG_SERVICE_OUTPUT might be single-line units or multi-line units (table contents)

- For single line unit prints
  [<title> -] <key-value-pairs> ...

  Sample:
  AgentInfo - Ident="ServerView ServerControl 2 hardware monitoring agent"
  Version=6.10.01.05 Company="Fujitsu"
- For multi-line-unit prints - Header
  * <title>
- For multi-line-unit prints - Rows
  [<status>:] <item>['['<index']'] - <key-value-pairs> ...

  Multi-line sample
  * Temperature Sensors:
  ok: Sensor[1] Name=Ambient Temperature=24C Warning=37C Critical=42C
  ok: Sensor[2] Name=Systemboard Temperature=33C Warning=60C Critical=65C
  ok: Sensor[3] Name=CPU1 Temperature=30C Warning=85C Critical=90C
  ok: Sensor[4] Name=CPU2 Temperature=30C Warning=85C Critical=90C
  ok: Sensor[5] Name=DIMM-1A Temperature=31C Warning=78C Critical=82C
  ok: Sensor[7] Name=DIMM-1B Temperature=32C Warning=78C Critical=82C
  ok: Sensor[11] Name=DIMM-1D Temperature=29C Warning=78C Critical=82C
  ok: Sensor[13] Name=DIMM-1E Temperature=29C Warning=78C Critical=82C

Performance data prints

- The performance data is printed in a new line after the above-mentioned lines starting with ' | '. The syntax complies with Nagios Core.

5.1.2 Verbose Level Usage

By default the Plugin should print output as small as possible. Any output is stored by Nagios systems in databases.

The standard – here Verbose Level 0 – prints the output as small as possible.

Verbose Level 1 – Print system information usable for administrators in case of notifications

If the plugin check has to print a WARNING or CRITICAL status, all available system information is printed automatically.

If this is to be done independently of the status, Verbose Level 1 can be used.

The output depends on the server type – the only common part is the data of the standard RFC1213.mib.

Verbose Level 2 – Print all analyzed data, regardless of the status.

By default, only the summary status is checked and printed. In the case of a non-OK status, the status of each subcomponent is checked and the data of the non-OK components is printed.

With Verbose Level 2, all subcomponents and their information are checked and printed, regardless of the status.

This depends of course on the check-options used and the server type.

This level can be used (unscheduled) for diagnostics and to analyze check-option-dependent resources of the server.

Verbose Level 3 – Print status-independent information for the "System" to analyze resources of the server.

This is very much server-type-dependent. With this level, "units", agent versions and so on can be read.

This is only to analyze server resources .

5.2 Common Script Options

-V|--version
Print version information and usage.

-h|--help
Print help text.

5.2.1 Script Processing Control Option

-t|--timeout=<timeout in seconds>
A timeout for the overall command processing can be specified.
There are special defaults for CIM:

The default value for CIM is 120 seconds. If the initial connection check fails, the command will time out after 60 seconds.

-v|--verbose=<verbose mode level>
Enable verbose mode (levels: 1, 2, 3). Generates multi-line output with inventory information or other additional information.

5.2.2 Addressing

-H|--host=<name-or-ip>
Host address as DNS name or IP address of the server

[-A|--admin=<adminaddress>]
Specify administration address with which all data for the host should be retrieved. This might be the iRMC address if a corresponding agent or provider is enabled on iRMC.

NOTE:

The two addresses are meant for Nagios administrators who want to define one host with services using two different addresses. E.g. Nagios services which are to use the original $HOSTADDRESS$ and parallel to these services other Nagios services which are to use the iRMC address specified in $_HOSTSV_ADMIN_OPTION$ or $_HOSTSV_OPTIONS$ or $_HOSTSV_CIM_OPTIONS$ or $_HOSTSV_REST_OPTIONS$

5.2.3 Connection Options

-P|-p|--port=<portnumber>
For the SNMP scripts:

SNMP port number. Default is 161.

For the CIM scripts:

CIM service port number. The **wbemcli** internal default is https with port 5989.
For WS-MAN calls the port number must be entered (e.g. 5985 or 5986)!

For WS-MAN:

For 5985 the transport type http is the default
For 5986 the transport type https is the default

For the REST scripts:

The REST services run with fixed port numbers. Do not set other port numbers.

ServerView Agent System Control uses port 3172.
iRMC Report Service uses port 80 or 443, depending on service configurations.

-T|--transport=<type>
For the SNMP scripts:
SNMP transport domain type. A full description of available values can be found in Net::SNMP->session parameters and parameter '-domain'.
The default is "udp", meaning UDP service for IPv4 addresses.
Samples for other values:

- **tcp** – for TCP connection instead of UDP
- **udp6 or tcp6** – for IPv6 addresses

For the CIM scripts:
For CIM this is the transport HTTP type. The default for **wbemcli** is "**https**".
Other value:

- **http** – for simple http calls

For WS-MAN:
For 5985 the transport type http is the default
For 5986 the transport type https is the default

For REST scripts:
Specify the HTTP transport type. The default is "**https**".
Other value:

- **http** – for simple http calls

5.2.4 CIM Protocol Usage – CIM-XML or WS-MAN

-U|--usage={C|W}

"C" Use CIM-XML protocol. This requires wbemcli installation. Connect to SFCB or OpenPegasus

"W" Use WS-MAN protocol. This requires OpenWSMAN Perl binding. Connect to OpenWSMAN services or WinRM

5.2.5 SNMP Authentication

-C|--community=<SNMP community string>
SNMP community of the server. Usable for SNMPv1 and SNMPv2. The default is **public**.

-u|--user=<username> [--authpassword=<pwd>] [--authkey=<key>] [--authprot=<prot>]
[--privpassword=<pwd>] [--privkey=<key>] [--privprot=<prot>]
SNMPv3 authentication credentials

-I|--inputfile=<file> [--inputdir=<directory>]
File in which host-specific options like the above-named ones can be stored. Use of this is **recommended** for security-relevant options like -u and other SNMPv3 credentials.
This file must be readable for the Plugin script used by the Nagios!
With inputdir a directory path for the input option file can be specified. The directory path is ignored if the input file starts with '/'.

About IPv6 Usage:

For requirements for IPv6, see chapter "Local Requirements" and "SNMP".

Before using an IPv6 address, make sure that on the host to be monitored there is an SNMP which is able to handle IPv6 addresses:

- Check SNMP configuration settings
- Check firewalls
- Check IPv6 kernel abilities and configurations of the operating system itself

ATTENTION: On SLES10 there is an SNMP which does not fully support IPv6 and is unstable if called with IPv6!

If an IPv6 address is entered, the plugin automatically sets the transport type to UDP-IPv6 (if not specified).

If an IPv4 address is entered and no '-T' option is set, the default transport type of local Perl Net::SNMP is used.

For DNS names as the host address, the default transport type of local Perl Net::SNMP is used.

5.2.6 CIM Authentication

-u|--user=<user> -p|--password=<pwd>
Authentication credentials (Please write these options into a file – see option -I)
These options must be set.

ATTENTION:

1. Credentials are verified in *sfcb* on the managed node site and this verification is done according to *sfcb* configuration. Credentials are normally checked by a library (sfcBasicPAMAuthentication) which defines the rules for how they are checked. And these rules might not be as evaluated as anyone would expect (restrictions on use of characters or length of values etc.). If you are lacking functionality, refer to sfcb for how to replace the standard library with one that meets your needs.

   The same behaviour is true for the other CIM services OpenPegasus, OpenWSMAN and WinRM.

2. Known problems:
   - For wbemcli: Passwords must not contain any dots '.'
   - Do not use characters like ' or " in the user or password string
   - User accounts and passwords which contain shell-relevant signs like $ should always be set in an option input, file see option description -I below
   - The password check might vary from system to system

--cacert=<cafile>
CA certificate file.
If this is not set, the wbemcli parameter -noverify will be used resp. the "do not verify" flags will be set for OpenWSMAN.

See wbemcli parameter -cacert resp wsman command parameter --cacert

1. Certificates are handled both in *wbemcli* and in *sfcb* on the managed node site. On the managed node site, this is done according to *sfcb* configuration and certificates are normally checked under certain conditions by a library (sfcCertificateAuthentication) which defines the rules for how certificates are checked. Regarding credential check, you might want to replace this library with your own implementation. Please refer to *sfcb* for how to do so.

   The same behaviour is true for the other CIM services OpenPegasus, OpenWSMAN and WinRM.

2. Known problems:
   - wbemcli: If <cafile> exists and is not empty but does not contain a certificate, on some systems *wbemcli* dumps a core.

--cert=<certfile> --privkey=<keyfile>
Client certificate file and client private key file.

wbemcli requires both file names if this is to be used.
It depends on the configuration on the host side whether or not these certificates are verified!

See wbemcli parameter -clientcert and --clientkey resp. wsman command and parameters --cert and --sslkey

-I|--inputfile=<file> [--inputdir=<directory>]
File in which host-specific options like those named above - with the exception of the host option - can be stored. Use of this is **recommended** for security-relevant options like –u and –p.
This file must be readable for the owner of the Nagios Plugin script used by the Nagios scheduler from within the Nagios Plugin directory!
With inputdir a directory path of the input option file can be specified. The directory path is ignored if the input file starts with '/'.

5.2.7 REST Authentication

-u|--user=<user> -p|--password=<pwd>
Authentication credentials (Please write these options into a file – see option -I)

The ServerView Server Control service,the ServerView iRMC Report and the ServerView iRMC Redfish service use user and password authentication.

--cacert=<cafile> --cert=<certfile> --privkey=<keyfile>
The meaning of these parameters is the same as for CIM authentication. The default configuration of the known REST services does not require client certificate usage.

-I|--inputfile=<file> [--inputdir=<directory>]
File in which host-specific options like those named above - with the exception of the host option - can be stored. Use of this is **recommended** for security-relevant options like –u and –p.
This file must be readable for the owner of the Plugin script used by the Nagios scheduler from within the Nagios Plugin directory!
With inputdir a directory path of the input option file can be specified. The directory path is ignored if the input file starts with '/'.

6 Check Plugin

6.1 Check Plugin: Server Status and Performance Monitoring

The scripts of FUJITSU Server Plug-ins get all names and values as-is from the providing services. Some numeric values are matched to name strings according to the descriptions of the providing services. The number of monitored sensors or components varies, depending on the server type.

Some hardware components are not assigned to virtual guests, server blades or PRIMEQUEST partition server nodes.

Script name for SNMP monitoring
check_fujitsu_server.pl

Script name for CIM monitoring
check_fujitsu_server_CIM.pl

Script name for REST monitoring
check_fujitsu_server_REST.pl

6.1.1 Initial Connection Tests

Option for SNMP
--chkuptime

ATTENTION: This option cannot be combined with other check options.

With this option the script checks if SNMP is running and whether the local server is allowed to receive SNMP responses from the host to be monitored.
The SNMP response contains the RFC1213 "UpTime" of this system.

HINT: If this call fails, check the following potential reasons on the server to be monitored:
- Is the server powered-on with SNMP running?
- Check the SNMP community data resp. SNMPv3 authentication data
- Check other permission or restriction rules on the server to be monitored, e.g. firewall settings

Option for CIM or REST
--chkidentify

ATTENTION: This option cannot be combined with other check options.

With this option the script checks if the host is running and whether the set authentication data is valid for receiving responses from the host to be monitored.
For CIM:
For this check the standard CIM providers are used. This call is independent of installed ServerView CIM Providers.
For REST:
This call checks if ServerView REST services can be detected:
- ServerView Server Control (in-band)
  HINT: for this test the authentication is not checked
- ServerView iRMC Report and iRMC Redfish

HINT: If this call fails, check the following potential reasons on the server side (the host to be monitored):
1. Is the server powered-on and the corresponding service running?
2. Check authentication data
3. Check other permission or restriction rules in the configurations, e.g. firewall settings

Nagios Configuration Sample

See the following files:

- cfg/SNMP/services/serverview_all.cfg
- cfg/CIM/ services/serverview_all_CIM.cfg
- cfg/REST/iRMCReport/serverview_service_primergy_servers_iRMCReport_REST.cfg
- cfg/REST/ServerControlAgent/serverview_service_primergy_servers_REST.cfg
- cfg/TEST/iRMCRedfish/serverview_service_primergy_servers_iRMCRedfish_REST.cfg

6.1.2 System Overall Status

If no action check option is specified, the script monitors all available hardware component parts in one go (environment, power, system board, driver monitor, mass storage).

The return code is the overall status of the monitored system.

The script always prints the Nagios Status String. For the system overall status call, this is followed by the serial number (if available) and the summary status of the component parts.

The following chapters describe the available component information.

6.1.3 Thermal Environment Monitoring

Thermal environment monitoring is performed if no other check option is specified or if the following options are used.
The additional option -v2 for the verbose level 2 prints additional property information of all sensors.

Options:

"environment" can be selected with

--chkenv

Check environment, i.e. check of cooling devices like fans and liquid pump and check temperature sensors.
This can be split with

--chkfan|--chkcooling

Check fans and, if available, liquid pump sensors

--chktemp

Check temperature sensors

Availability:

All known services support fan and temperature sensor monitoring.
Liquid pump sensor monitoring is supported by ServerView Agent V7.10 or higher (in-band) for the SNMP or REST protocol.

Fans and temperature sensors of storage cabinet devices are only supported by ServerView Agent (in-band) via the SNMP or REST protocol

Performance data:

<identification of temperature sensor>=<current>C;<warn>;<critical>

Nagios Configuration Sample

See the following files for --chkenv usage:

- cfg/SNMP/services/serverview_primergy_detail_servers.cfg
- cfg/SNMP/services/serverview_primergy_blade_detail_servers.cfg
- cfg/SNMP/services/serverview_primequest_detail_servers.cfg
- cfg/iRMCSNMP/serverview_service_primergy_servers_component_group_iRMC_SNMP.cfg
- cfg/CIM/services/serverview_primergy_servers_CIM_component_group.cfg
- cfg/REST/iRMCReport/serverview_service_primergy_servers_iRMCReport_REST_component_group.cfg
- cfg/REST/iRMCRedfish/serverview_service_primergy_servers_iRMCRedfish_REST_component_group.cfg

- cfg/REST/ServerControlAgent/serverview_service_primergy_servers_REST_component_group.cfg

6.1.4 Power Monitoring

Power monitoring is performed if no other check option is specified or if the following options are used.
The additional option -v2 for verbose level 2 prints additional property information of all sensors.

Options:

"power" can be selected with

--chkpower

Check power supplies and get the total power consumption

Availability:

Power supply sensor monitoring is supported by all known services. The current load values are not available for PRIMEQUEST MMB.

Power supply sensors of storage cabinet devices are only supported by the ServerView Agent (in-band) via the SNMP or REST protocol.

The power consumption via iRMC Report service is only available for firmware version 7.20 or higher.

The power consumption of PRIMERGY Blade is the latest one (concerning date entry) in the list of power consumption history entries.

The power consumption control mode is only supported for ServerView Agent Server Control (REST) or PRIMEQUEST 2800.

Performance data:

PowerConsumption=<average>Watt[;<warn>;<critical>]

Nagios Configuration Sample

For --chkpower usage see the files mentioned in the environment chapter above.

6.1.5 System Board Monitoring

System board monitoring is performed if no other check option is specified or if the following options are used.
The additional option -v2 for verbose level 2 prints additional property information of all sensors.

Options:

--chksystem

Check system board and mass storage.
“system board” can be selected with

--chkboard|--chkhardware

"Hardware" (Voltage, CPU and Memory Modules).
This is an option for those who want to monitor only these components.

The system hardware information can be split with the following options:

--chkcpu	CPU information
--chkvoltage	Voltage information
--chkmemmodule	Memory module information

Availability:

All known services besides PRIMERGY Blade MMB support system board monitoring.

No detail properties of memory modules will be printed for PRIMEQUEST MMB unless verbose level 651 is used. It takes a long time to retrieve these values.

Nagios Configuration Sample

For --chkboard usage see the files mentioned in the environment chapter above.

6.1.6 ServerView RAID and Mass Storage

Mass storage monitoring is performed if no other check option is specified or if the following options are used.
The additional option -v2 for verbose level 2 prints additional property information of all items.

Options:

--chksystem

Check system board and mass storage.
Only mass storage can be selected with

--chkstorage

Get the ServerView RAID status and property information if available. Get status of all mass storage adapters if available

Availability:

The ServerView RAID information via SNMP is available if ServerView RAID is installed, configured and running (stand-alone ServerView RAID).
The RAID data can also be monitored via ServerView Agent (SNMP, REST) or via ServerView RAID CIM Provider (CIM) installed on ESXi (beside the other ServerView CIM Provider).
Additional status values of all mass storage adapters are only available with the ServerView Agent (SNMP, REST) or with the ServerView iRMC Redfish (REST).

Nagios Configuration Sample

There is no ready-to-use sample configuration file for stand-alone RAID monitoring in the FUJITSU Server Plug-Ins.

```
define service {
        # hostgroup_name                primergy-detail-
servers,primergy-servers
        service_description           SV MassStorage
        servicegroups                 serverview
        use                           generic-service
        check_command                 check_fujitsu_server!--
chkstorage
        flap_detection_enabled        0
        register                      1
}
```

6.1.7 Driver Monitor

Driver monitoring is performed if no other check option is specified or if the following options are used.
The additional option -v2 for verbose level 2 prints additional property information of all items.

Option:

--chkdrvmonitor

Get driver monitor status if available.

Availability:

This information is only available if the ServerView Agent (SNMP, REST, CIM) is installed on the server or out-of-band with ServerView iRMC Redfish (REST).

Nagios Configuration Sample

See the following files for --chkdrvmonitor usage:

- cfg/SNMP/services/serverview_primergy_with_drvmonitor.cfg
- cfg/CIM/services/serverview_primergy_servers_CIM_drvmonitor.cfg
- cfg/REST/ServerControlAgent/serverview_service_primergy_servers_REST_drvmonitor.cfg
- cfg/REST/iRMCRedfish/serverview_service_primergy_servers_iRMCRedfish_REST_drvmonitor.cfg

6.1.8 ServerView Update Status

Get system update status and optional get difference list of components to be updated or get all updatable components. The lists can be stored in files in a specified output directory.

The information is based on the ServerView Agent.

Availability:

The status and lists are supported by ServerView Agent (SNMP, REST) and ServerView CIM Provider (CIM).

There is no support for server type ESXi or via iRMC.

Option:

--chkupdate
[{ --difflist | --instlist } [-O|--outputdir=<dir>]]

Nagios Configuration Sample

See the following files for --chkdrvmonitor usage:

- cfg/SNMP/services/serverview_primergy_update_monitor.cfg
- cfg/CIM/services/serverview_primergy_servers_CIM_update_monitor.cfg
- cfg/REST/ServerControlAgent/serverview_service_primergy_servers_REST_update_monitor.cfg

6.1.9 File System Usage

Options:

--chkfsperf [-w<percent>] [-c<percent>]

Performance data:

<name_of_fs>=<current>%[;<warn>;<critical>]

Availability:

This information is only available if the ServerView Agent (SNMP, REST) is installed on the server.

Nagios Configuration Sample

See the following files for --chkfsperf usage:

- cfg/SNMP/services/serverview_primergy_performance.cfg
- cfg/REST/ServerControlAgent/serverview_service_all_Agent_REST_performance.cfg

6.1.10 Memory Usage

Options:

--chkmemperf [-w<percent>] [-c<percent>]

Availability:

This information is only available if the ServerView Agent (SNMP,REST) is installed on the server.

Performance data:

PhysicalMemory=<current>%[;<warn>;<critical>]

Nagios Configuration Sample

See the following files for --chkmemperf usage:

- cfg/SNMP/services/serverview_primergy_performance.cfg
- cfg/REST/ServerControlAgent/serverview_service_all_Agent_REST_performance.cfg

6.1.11 CPU Usage

Options:

--chkcpuperf

Availability:

This information is only available if the ServerView Agent (REST) is installed on the server.
The ServerView Agent (SNMP) supports only a current value but no average.

Performance data:

CPUTotalAverage=<current>%

Nagios Configuration Sample

See the following files for --chkcpuperf usage:

- cfg/REST/ServerControlAgent/serverview_service_all_Agent_REST_performance.cfg

6.1.12 Network Interface Usage

Options:

--chknetperf

Check INVENT.mib network interface entries and get performance data.

-w <kBytesec> -c <kBytesec >

Add a warning or critical level for interfaces where the In/Out bytes can be monitored. These should be simple kByte/sec limits.

HINT: This script does not set default values for this.

ATTENTION: This option cannot be combined with other check options.

Availability:

This is only available if the ServerView Agent (SNMP) is installed on the server.

Status and Performance Printouts:

The status will be OK if no warning or critical limits are set or as long as no network interface exceeds the limits.

The network interface performance data will be set for any network interface with monitorable values – in this case only if the nominal speed is known.

<name>= <current>KB/sec

HINT - for names used in performance data:

NetIF[index] will be used if no short name can be extracted from the description field or connection field.

Loopback[index] will be used if the connection field contains the word "Loopback" (if monitorable).

vEthernet[index] will be used if the connection field contains the word "vEthernet" (if monitorable).

LAN[index] will be used if the connection field contains the word "LAN".

LocalAreaConnection[index] will be used if the connection field contains the term "Local Area Connection".

<CustomerDefinedName>[index] will be used if the connection field contains no spaces and is UTF8.

Nagios Configuration Sample

See the following files for --chknetperf usage:

- cfg/SNMP/services/serverview_primergy_performance.cfg

6.1.13 System Information in Case of WARNING or CRITICAL - for Notifications

In the case of non-OK status values, any check script tries to get and print system information for better identification of the system on which this non-OK status occurs.

The amount of this data depends very much on the server type and the service providing the information.

Printed data may include system name, system model, serial number, contact, location, OS information, administrative URLs, parent node information.

Availability:

The ServerView iRMC Report service only provides a serial number and the server model type.

The system name and some other values are not always available via iRMC (SNMP, REST). This depends on wether the ServerView Agentless Service or the ServerView Agent is installed on the base server or whether the administrator has configured identifying information via the iRMC WebUI.

6.1.14 Additional System Identification Information

With verbose level 3 in combination with option --chksystem, additional identification information is sought and printed.

This includes the version of the providing service (e.g. ServerView Agent) and UUIDs, MACs and IP addresses.

Availability:

The data is available for PRIMERGY where ServerView Agents or CIM Provider are installed and for PRIMEQUEST. There is no such data for PRIMERGY Blade MMB and RackCDU™ or via iRMC Report (REST).

6.1.15 Miscellaneous Information

Option

--systeminfo

ATTENTION: This option cannot be combined with other check options.

If one of the following checks returns WARNING or CRITICAL or if verbose level 1 is used, the system information usable for administrators will be collected (if available) and printed.
To achieve this without a status check, the above-named option can be used.

Option

--agentinfo

ATTENTION: This option cannot be combined with other check options.

This option can be used to get the version of the providing service, e.g ServerView Agent or the iRMC firmware version.

6.1.16 Nagios Configuration Samples

All Nagios Core sample files are in the directory path fujitsu/ServerViewSuite/nagios/cfg.

There are directories for features and protocol:

- **CIM** Supports any CIM monitoring
  Based on ServerView CIM Provider for Linux and Windows and ESXI.
- **iRMCSNMP** Supports iRMC SNMP monitoring.

- **REST** Supports any REST monitoring
  For REST there are central configurations and configuration directories for different REST services:
  - **iRMCReport** Supports ServerView iRMC Report monitoring
  - **iRMCRedfish** Supports ServerView iRMC Redfish monitoring
  - **ServerControlAgent** Supports ServerView Agent Server Control monitoring
- **SNMP** Supports SNMP monitoring besides iRMC SNMP
  Based on ServerView Agent for PRIMERGY and firmware of PRIMERGY Blade MMB and PRIMEQUEST MMB.

6.2 Check Plugin: Monitoring Blades Controlled by a PRIMERGY Management Blade (SNMP)

Script name for SNMP monitoring
check_fujitsu_server.pl

This depends on the existence and support of S31.mib.

Options:
With thefollowing options, as an alternative to --blade, which checks the overall status and performance of the management blade itself, additional checks for blades assigned to this management blade can be retrieved.

The "Sub-Blades" are grouped in to four types:
- Server Blades
- I/O Connection Blades - including Switch, Fibre Channel Switch, LAN Pass-Through, FSIOM, Serial Attached SCSI Switch (SAS)
- Key/Video/Mouse (KVM) Blades
- Storage Blades

--bladeinside

This is a combination of the four following options with the advantage that error messages concerning unknown blade types are suppressed.
(Do not combine with --blade.)

--bladesrv
Check server blade status values on a PRIMERGY Blade server.

--bladeio
Check all I/O connection blade status values on a PRIMERGY Blade server.

The bladeio information can be split with one or more of following options instead of option bladeio.

--bladeio-switch	Switch
--bladeio-fcswitch	Fibre Channel Switch
--bladeio-phy	LAN Pass-Through
--bladeio-fsiom	FSIOM
--bladeio-sasswitch	Serial Attached SCSI Switch

--bladekvm
Check key/video/mouse blade status values on a PRIMERGY Blade server.

--bladestore
Check storage blade status values on a PRIMERGY Blade server.

6.2.1 Server Blades

The assigned server blade monitoring is performed if option --bladeinside is specified or if --bladesrv is used.
The additional option -v2 for verbose level 2 prints additional property information.

Summary Line:

Server-<one status>(<count_of_server_with_this_status>)[-<status>(<count>[...])]]

ATTENTION: The <status> is not only limited to the four-value system of Nagios, but there are additional specific status values available as well.

User interface sample in Icinga-Classic 1.5

Service State Information

Current Status:	CRITICAL (for 1d 0h 6m 0s)
Status Information:	CRITICAL Server-critical(2)-standby(4) critical: Server[1] ID=QTFMQK83900186 ID2=System_422 AdminURL=http://172.17.52.165 critical: Server[11] ID=SQ1008MR00076 ID2=System_117 AdminURL=http://172.17.52.107
Performance Data:	
Current Attempt:	3/3 (HARD state)
Last Check Time:	10-17-2012 14:01:50
Check Type:	ACTIVE
Check Latency / Duration:	0.159 / 2.801 seconds
Next Scheduled Check:	10-17-2012 14:11:50
Last State Change:	10-16-2012 13:57:50
Last Notification:	10-17-2012 13:11:59 (notification 24)
Is This Service Flapping?	N/A
In Scheduled Downtime?	NO
Last Update:	10-17-2012 14:03:48 (0d 0h 0m 2s ago)

6.2.2 Additional Information about Server Blades

With additional verbose level 2, you can get the "Server Blade" table entries mentioned above as well as the NIC table information.

With this information you can get the host name and IP addresses (available in the NIC table if the system is on) and the management IP of each Server Blade.

Sample:

```
* Server Blades:
ok: Server[1] ID=SQ948MS00112 ID2=System_053 Hostname=localhost
AdminURL=http://nnn.nnn.nnn.nnn Product="D3030" Model="A3C40114042"
ok: Server[2] ID=SQ1124MV00162 ID2=920S3063 Hostname=SW1-BX920S3-2.v
AdminURL=http://nnn.nnn.nnn.nnn Product="D3142" Model="A3C40125624"
ok: Server[3] ID=SQ948MS00002 ID2=System_125 Hostname=pdbsm-bx924s3-
2 AdminURL=http://nnn.nnn.nnn.nnn Product="D3030"
Model="A3C40114042"
ok: Server[4] ID=SQ1143MW00050 ID2=924S3116 Hostname=SW1-BX924S3
AdminURL=http://nnn.nnn.nnn.nnn Product="D3143" Model="A3C40125625"
unknown: Server[5] ID=QTFMQK83900390 ID2=System_178 Hostname=SW1-
BX920S1-1 Product="D2860" Model="A3C40094854"
ok: Server[6] ID=SQ1146MV00171 ID2=920S3106 Hostname=SW1-BX920S3-1
AdminURL=http://nnn.nnn.nnn.nnn Product="D3142" Model="A3C40125624"
* Server Blade NIC Table:
ServerNicInfo[1.1] - MAC=00:26:9E:82:96:9A Type=on-board-lan-
controller
```

```
ServerNicInfo[3.1] - MAC=00:26:9E:82:96:36 Type=on-board-lan-
controller
ServerNicInfo[4.1] - MAC=04:7D:7B:06:D5:F8 IP=xxx.xxx.xxx.xxx
Type=on-board-lan-controller
ServerNicInfo[4.2] - MAC=04:7D:7B:06:D5:FC IP=xxx.xxx.xxx.xxx
Type=on-board-lan-ontroller
ServerNicInfo[5.1] - MAC=00:1E:68:DA:55:BC IP=xxx.xxx.xxx.xxx
Type=on-board-lan-controller
ServerNicInfo[6.1] - MAC=04:7D:7B:11:26:F8 Type=on-board-lan-
controller
```

How to Detect Host Name and IP Address of Server Blades

Use the above-mentioned --bladesrv and --verbose=2 and use the host name from the first table printout and (if available) detect the related IP addresses in the NIC table via the server index.

In the above-mentioned example it is

```
ok: Server[4] ID=SQ1143MW00050 ID2=924S3116 Hostname=SW1-BX924S3
AdminURL=http://nnn.nnn.nnn.nnn Product="D3143" Model="A3C40125625"
```

and

```
ServerNicInfo[4.1] - MAC=04:7D:7B:06:D5:F8 IP=xxx.xxx.xxx.xxx
Type=on-board-lan-controller
ServerNicInfo[4.2] - MAC=04:7D:7B:06:D5:FC IP=xxx.xxx.xxx.xxx
Type=on-board-lan-controller
```

6.2.3 IO-Connection – FSIOM

The assigned fsiom blade monitoring is performed if option **--bladesinside** is specified or if --**bladeio** or **--bladeio-fsiom** is used.
The additional option -v2 for verbose level 2 prints additional property information.

- Summary Line:

  FSIOM(<fsiom_status>)

6.2.4 IO-Connection – Switch Blades

The assigned switch blade monitoring is performed if option **--bladesinside** is specified or if --**bladeio** or **--bladeio-switch** is used.
The additional option -v2 for verbose level 2 prints additional property information.

- Summary Line:

  Switch-<one status>(<count_of_switch_with_this_status>)[-<status>(<count>[…])]]

6.2.5 IO-Connection – Fibre Channel Switch

The assigned switch blade monitoring is performed if option **--bladesinside** is specified or if --**bladeio** or **--bladeio-fcswitch** is used.
The additional option -v2 for verbose level 2 prints additional property information.

- Summary Line:

  Fibre Channel Switch-<one status>(<count_of_switch_with_this_status>)[-<status>(<count>[…])]]

6.2.6 IO-Connection – Serial Attached SCSI Switch (SASSwitch)

The assigned switch blade monitoring is performed if option **--bladesinside** is specified or if --**bladeio** or **--bladeio-sasswitch** is used.
The additional option -v2 for the verbose level 2 prints additional property information.

- Summary Line:

  Serial Attached SCSI Switch-<one status>(<count_of_switch_with_this_status>)[-<status>(<count>[…])]]

6.2.7 IO-Connection – LAN Pass-Through (Phy)

The assigned switch blade monitoring is performed if option **--bladesinside** is specified or if --**bladeio** or **--bladeio-phy** is used.
The additional option -v2 for verbose level 2 prints additional property information.

- Summary Line:

  LAN Pass Through Blades-<one status>(<count_of_switch_with_this_status>)[-<status>(<count>[…])]]

6.2.8 Key/Video/Mouse Blades (KVM)

The assigned switch blade monitoring is performed if option **--bladesinside** is specified or if --**bladekvm** is used.
The additional option -v2 for verbose level 2 prints additional property information.

- Summary Line:

  KVM-<one status>(<count_of_switch_with_this_status>)[-<status>(<count>[…])]]

6.2.9 Storage Blades

The assigned switch blade monitoring is performed if option **--bladesinside** is specified or if --**bladestore** is used.
The additional option -v2 for verbose level 2 prints additional property information.

- Summary Line:

  Storage Blades-<one status>(<count_of_switch_with_this_status>)[-<status>(<count>[…])]]

6.2.10 Nagios Configuration Sample

See the following files for the blade options:

- cfg/SNMP/services/serverview_primergy_blade_servers.cfg
- cfg/SNMP/services/serverview_primergy_blade_detail_servers.cfg
- cfg/SNMP/services/serverview_primergy_blade_with_KVM.cfg
- cfg/SNMP/services/serverview_primergy_blade_with_storage.cfg

6.3 Check Plugin: Monitoring RackCDU (SNMP)

Script name for SNMP monitoring
check_fujitsu_server.pl

The script enables status monitoring and reads sensor performance values of a RackCDU.

Options:
--rack

6.3.1 System Information in Case of WARNING or CRITICAL - for Notifications

There is not much data available for this management system:

- Customer-specified rack name
- Rack type
- Customer-specified description

Sample:

```
RackIdentifier="SNMPAGENTTEST" RackType="Asetek RackCDU Monitoring Control
Box" Description="demo description"
```

6.3.2 Special Measurement Status Values

There are two sensors with non-numeric status values.

- The detection of leaks - values are "no" or "yes"
- The coolant level - values are "ok" or "low" (server-side sensor).

Sample:

```
RackMeasurement - Leak=no CoolantLevel=ok
```

6.3.3 Temperature Information

There are five temperature sensor values that can be monitored. For each of these, thresholds might be enabled and set. The base unit is **°C "degrees Celsius**".

- Facility In
- Facility Out
- Server In
- Server Out
- Ambient (there are no thresholds for this value)

In the case of an overall error, the script checks whether one of the thresholds has been reached for the current sensor values and prints the corresponding information.

Verbose level 2 prints all temperature sensor information.

Sample:

```
ok: Temperature[] Name=FacilityIn Temperature=18.9°C Warning=55°C Critical=60°C
ok: Temperature[] Name=FacilityOut Temperature=19.6°C Warning=55°C Critical=60°C
ok: Temperature[] Name=ServerIn Temperature=19.6°C Warning=45°C Critical=50°C
warning: Temperature[] Name=ServerOut Temperature=21.8°C Warning=20°C
Critical=30°C
none: Temperature[] Name=Ambient Temperature=35.2°C
```

6.3.4 Pressure Information

There are two pressure sensor values that can be monitored. For each of these, thresholds might be enabled and set. The base unit is **bar**.

- Pressure Server
- Pressure Facility

In the case of an overall error, the script checks whether one of the thresholds has been reached for the current sensor values and prints the corresponding information.

Verbose level 2 prints all pressure sensor information.

Sample:

```
ok: Pressure[] Name=ServerPressure Pressure=0.003bar Warning=0.2bar
Critical=0.3bar
ok: Pressure[] Name=FacilityPressure Pressure=1.995bar Warning=3bar
Critical=3.5bar
```

6.3.5 Flow Information

There is one flow sensor value that can be monitored. For this sensor, thresholds might be enabled and set. The base unit is **l/h "liters per hour".**

- Flow Facility

In the case of an overall error, the script checks whether one of the thresholds has been reached for the current sensor value and prints the corresponding information.

The thresholds are printed as ranges with the Nagios syntax <min>:<max>, meaning "if value is less than <min> or higher than <max>"

Verbose level 2 prints all flow sensor information.

Sample:

```
ok: Flow[] Name=FlowFacility Flow=1008.00l/h WarningRange=100.00:3400.00l/h
CriticalRange=75.00:3500.00l/h
```

6.3.6 Other Monitoring Information

HeatLoad

The HeatLoad value returns an average Watt value for a configured time (seconds). With verbose level 2, both numbers are printed. For performance graphs only the Watt value is used.

E.g. average 987 Watt for the last 60 seconds

ControllerOut

The description of this value is in the original RackCDU™ Manual. The unit printed is percent %.

Sample:

```
none: HeatLoad[] Current=987Watt HeatAverageFactor=60sec
none: ControllerOut[] Current=35%
```

6.3.7 Nagios Configuration Sample

Example file **cfg/SNMP/serverview_RackCDU.cfg_**

This file name is given an underscore '_' at the end so that it is not automatically used by Nagios.
Read it if a RackCDU is to be monitored, then remove the trailing underscore and assign a RackCDU host to the host group name defined in this file.

The service should not be called if SNMP is not up at the time ofcalling– the service dependency forces this.

7 Connectivity and Server Type Test Tool

Script name for SNMP
tool_fujitsu_server.pl
Script name for CIM
tool_fujitsu_server_CIM.pl
Script name for REST connection tests
tool_fujitsu_server_REST.pl

Options

--mibtest (SNMP only)
This is the default for the SNMP script.
Checks if data from different MIBs can be fetched. This includes a type and a connection test.

--typetest
This is the default for the CIM or REST script.

Checks only information relevant to analyze the type of server.
One part of this is

--connectiontest

SNMP: Test only test connectivity using RFC1213 tests.This data is available for any server with a running SNMP agent.

CIM: Test only CIM connectivity: CIM-XML and WS-MAN connections.

REST: Test connections to REST services.

[-e or **--extended]**
This special option extends the scan for servers to search the following data.
For ALL protocols:

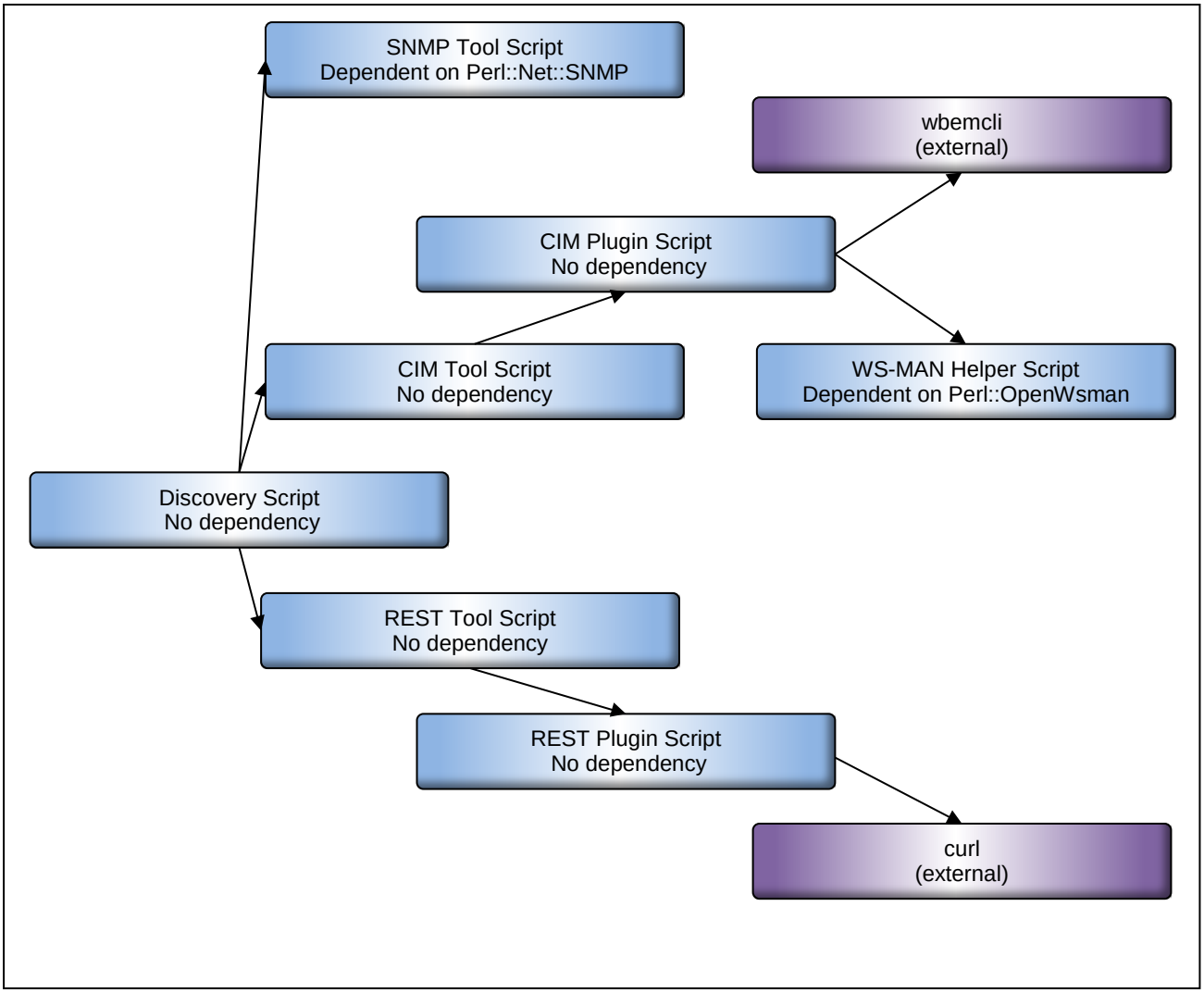
- Agent resp. firmware version if available
- ServerView System Monitor URL if available
- Fully Qualified Domain Name (FQDN) of a PRIMERGY server if available
- Parent management blade for a PRIMERGY Server Blade
- Parent PRIMERGY Multi-Node name and model information (CX series) (not for CIM)
- iRMC: Agent connection status if available
  (NoAgent, Agentless, Mgmt. Agent)

[--nopp]
This is an option for suppressing printouts in-between process results. Only a kind of summary of available system information about the host is printed.

8 Discovery – Check Server Types and Generate Configurations

8.1 Script Hierarchy

Script hierarchy:



The **discover_fujitsu_server.pl** script uses the other scripts to get the required data.
To allow this, the other scripts must be in the same directory as the discovery script.

Scripts:

- SNMP tool script: tool_fujitsu_server.pl
- CIM tool script: tool_fujitsu_server_CIM.pl
- CIM plugin script: check_fujitsu_server_CIM.pl
- WS-MAN helper script: fujitsu_server_wsman.pl
- REST tool script tool_fujitsu_server_REST.pl
- REST plugin script check_fujitsu_server_REST.pl

8.2 Basics

8.2.1 Script Name

Name of the script
discover_fujitsu_server.pl

-V|--version
Print version information and help text.

-h|--help
Print help text.

-t|--timeout=<timeout in seconds>
Specify the timeout in seconds for calling of the other scripts (SNMP or CIM checks).
ATTENTION: This is not a timeout for this script!

[--ctimeout=<connection timeout in seconds>]
Specify the timeout for the connection test to the CIM services. The default is 30 seconds. All values above 30 will be ignored.
ATTENTION: This is used for calling the CIM script!

8.2.2 Select Host Options

-H|--host=<name-or-ip>
Enter the host address as a DNS name or IP address of the server.

[--onehost] | --ipv4-discovery | --hc|--hostcollection=<file>
| --csv=<svomcsv> [--show] [--nobmc]
| --xml=<svomxml> [--show] [--nobmc]

"onehost": Test only one host address specified with option -H. This is the default.

"ipv4-discovery":
Test for 256 servers for a given n.n.n. IPv4 address. (Be aware of the dot at the end.)
Test for a limited range of servers for a specified n.n.n.<firstn>-<lastn> IPv4 address.

"hostcollection":
Test a list of host addresses written to a file. – In this case option –H is ignored.
Format:
Specify one address or one "ipv4-discovery" range in each line

"csv":
Test a list of host addresses which are the "NetAddress" and "BmcAddress" part of an ServerView Operations Manager server list CSV file (The delimiter is ',')

"xml":
Test a list of host addresses which are the "NetAddress" and "BmcAddress"part of an ServerView Operations Manager server list XML file.

"show":
"show only mode" - Only show evaluations of found server information - there will be no discovery process.

nobmc: Use "nobmc" to prevent "BmcAddress" discovery.

For more about processing of multiple hosts, see chapter "Processing Loop Overview".

8.2.3 Select Usage Mode – SNMP or CIM-XML or WS-MAN or REST

[-U|--use={S|C|W|CW|R}]

Default: Try any connection abilities.

"S" Use only SNMP: This requires Perl Net::SNMP and uses tool_fujitsu_server.pl

"C" Use only the CIM-XML protocol. This requires wbemcli installation. The script tries to connect to SFCB or OpenPegasus. This uses tool_fujitsu_server_CIM.pl and check_fujitsu_server.pl

"W" Use only the WS-MAN protocol. This requires OpenWSMAN Perl binding. The script tries to connect to OpenWSMAN services or WinRM. This uses tool_fujitsu_server_CIM.pl and check_fujitsu_server.pl and fujitsu_server_wsman.pl

"CW" Try the CIM-CML and WS-MAN protocols.

"R" Try the REST protocol

8.2.4 Control Usage of SNMP community "public"

[--snmpfirstpublic | --snmplastpublic | --snmpnopublic]

"snmpfirstpublic": Try community "public" before any other community settings

"snmplastpublic": Try community "public" after any other community settings

"snmpnopublic": Try only specified community settings

8.2.5 Additional Authentication and Connection Options

-I|--inputfile=<filename> [--inputdir=<inputfiledir>] | --ic|--inputcollection=<dir>
The input option file will be used for the tool script calls.The files should contain options for these tools, e.g. credentials, port and transport type restrictions. The discovery script tries to analyze whether the content is meant for SNMP, CIM or REST calls.

"inputfiledir" - directory path of the input option file specified with -I

"inputcollection" - directory path of a collection of multiple input option files

RECOMMENDED: If these files are to be used for the Nagios monitoring use fully-qualified path names.

8.2.6 Output Options

[--config] | --txt
Store simple tool text output or store text output and generate the Nagios host definition configuration. The default is --config.

[-O|--outputdir=<dir>]
Specify the output directory for the resulting text and configuration files. The default is "svout".

8.2.7 Advanced Options for Output Files and Generated Nagios Host Name

For a description of the generated Nagios configuration, see chapter link "Nagios Configuration Files for Each Host".

Nagios UIs sort the hosts by the Nagios host name!

[--nozeroip]
For IPv4 addresses only:
Do not fill the last part of the address with zeros for name building of the output files and the Nagios host name. This is a sorting-relatedoption.

E.g. 172.17.48.87 results (since V3.10) in 172.17.48.087* files and Nagios host name.

With --nozeroip, 172.17.48.87 results in 172.17.48.87* files and Nagios host name, and because of this *.87 is sorted after *.100 as an example.

[--sortbyname]
As default of this script Nagios host names start with IP address before system name. To change this, use this option to start with system name before IP address.

8.3 Processing Loop Overview

Here is an overview of how the script handles multiple host specifications and multiple option input files. The description should help to understand how this script works.

ATTENTION:

Currently the script processes all actions step-by-step (in sync). This script can be called in parallel, but the number of resulting parallel socket connections must be taken into account by the caller!

The first loop level is for one or more specified host addresses.

For each host address there will be a loop for one or more specified option input files sorted for protocol usage and sorted (Perl sort()) by file names.

For SNMP: The default community "public" is tested and if failed each SNMP option input file is tested until a successful connection is registered.

This behavior can be influenced with additional options – see chapter link "Control Usage of SNMP community "public"".

For CIM or REST: The option input files are tested unless a successful connection is registered and "authentication error" occurs with no other reason for failure.

8.3.1 Multiple Hosts – Ipv4 Discovery

Use option -H<address range> --ipv4-discovery.

For testing all 256 servers, enter address range n.n.n. – be aware of the final dot.

Tests for a limited range of servers can be achieved with address range n.n.n.<firstn>-<lastn>

8.3.2 Multiple Hosts – Host Collection File

Use option –hc|--hostcollection=<file>

Test a list of host addresses written to a file.

Format:

Specify one host selection in one line.

A host selection can be an FQDN name, DNS name,IPv6 address,IPv4 address or IPv4 range. See address range in "IPv4 Discovery" above.

8.3.3 Multiple Hosts – ServerView Operations Manager Server List

Use option –csv=<csvfile>

Use option –xml=<xmlfile>

ServerView Operations Manager can export the server list in two standard formats:

CSV and XML

The resulting files can be read by the discovery script as a special host collection. If the discovery is successful, the host-assigned display name is used for the generated Nagios configuration file.

ATTENTION:

There is no way of exporting the "user/password" table of ServerView Operations Manager! It is therefore necessary that, for each host requiring such credentials for discovery, a corresponding option input file (readable only by the administrator and the script) is created by the user of this discovery script. For more on option input files, see chapter "Authentication and Credentials".

CSV - Before addresses are filtered, the first line will be checked to see if SVOM-specific column header names are available.

XML - Before addresses are filtered, the data will be checked to see if SVOM-specific XML namespaces and XML tag names are available.

An error message will be printed if the corresponding SVOM format could not be found.

Address information, type information, display name information and hints on the SNMP community will be read for each server if the SVOM format is discovered.

Some server types are ignored if they could not be monitored by the Plug-In scripts described in this document.

The addresses will be sorted for the discovery processing. Double IP addresses will be skipped.

8.3.3.1 Non-public SNMP Community

The discovery script generates an option input file

```
<outdir>/<hostaddress>_AUTH_SNMP.txt
```

if a non-public community is discovered on reading the SVOM server list. This will be used to test the corresponding host address. The file is only readable for the discovery script!

8.3.3.2 Ignore BMC Address Entry

The exported "Server List" contains NetAddress and BmcAddress entries. Both addresses will be tried by default. If it is known that the BmcAddress part does not rely on an iRMC S4/S5 address, it might be useful to omit the discovery trial of these addresses. Use option --nobmc to do so.

8.3.3.3 Show-Only Mode - Only Analysis, No Discovery

With the additional option --show, only the evaluation of the ServerView Operations Manager server list will be printed. This is to show which information is read and which entries will be used for discovery and which not.

Here are some examples of server node entries:

```
try: Address=n.n.n.72 BMC=n.n.n.90 Type=VMHost Mgmt=CIM
     SystemName="BX9-BX924S3-07.svsnet.qanet"
     DisplayName="BX9-BX924S3-07.svsnet.qanet-host"
     SuggestedName="BX9-BX924S3-07.svsnet.qanet-host"
```

COMMENT: Both IPs will be tried. For the CIM access of the address n.n.n.72, an additional input option file will be needed for the discovery check without "Show-Only Mode".

```
try: Address=n.n.n.30 Type=BladeServer Mgmt=SNMP
     SystemName="BX600-SM-GF"
     DisplayName="BX600-SM-GF"
     SuggestedName="BX600-SM-GF"
```

COMMENT: "BladeServer" is the type of the PRIMERGY Blade MMB;
"Blade" is the type of the Server Blade …
The data srtings are fetched from the exported server list!

```
try: Address=n.n.n.31 Type=Server Mgmt=SNMP
     SystemName=""
     DisplayName="HON-RX200S6"
     SuggestedName="HON-RX200S6"
     SpecialSNMPCommunity=qa
... generate svout/n.n.n.31_AUTH_SNMP.txt
```

COMMENT: This is an example where the SNMP community is not "public". The generate hint shows that an input option file is generated with corresponding information usable for the -I option of all scripts (for SNMP).

```
ign: Address=n.n.n.239 Type=SwitchBlade Mgmt=SNMP
     SystemName=""
     DisplayName="BX400S1em_044-Switch1"
     SuggestedName="BX400S1em_044-Switch1"
     SpecialSNMPCommunity=public17
```

COMMENT: This is a sample of an ignored server type – the Plug-In does not support Switch Blade monitoring.

```
try: Address=(N.A.) BMC=n.n.n.124 Type=Blade Mgmt=RMCP
     SystemName="pmblade2"
     DisplayName="BX900-3-02"
     SuggestedName="BX900-3-02"
```

COMMENT: In this case only the BMC address will be tried. This is also an example where the original "NetAddress" entry was empty – the "(N.A.)" value shows this.

8.3.4 Multiple Option Input Files

Each file should contain one set of credentials for CIM, REST or SNMP. For more about the individual files see chapter link "Authentication and Credentials".

8.4 Logging Information and Results

The discovery script writes logging information to STDOUT. Three additional files for each host are stored into the output directory. One is a log file, one is a text file if the connection was successful, and one is the configuration file if ServerView information is detected.

8.4.1 Central Logging

The information starts with the date and the directory name in which the output files are stored. At the beginning the option input files are checked and after that the loops for each host and option input file logs basic findings. This is followed by a summary section at the end.

See following descriptions of these parts.

8.4.1.1 Checks for the Option Input Files

At the beginning, the connection protocol for which the option input files can be used is logged. There will be ERROR hints if a file cannot be found or read, and there will be a WARNING hint if a file cannot be assigned to SNMP or CIM usage.

If the "inputcollection" directory is specified, only flat files within it will be checked!

ATTENTION

Unusable or not-existent files will be ignored!

Example of input collection option usage:

```
>>> read input option file AUTHQA3/A_Admin.txt
<<< OK - usable for CIM or REST calls
>>> read input option file AUTHQA3/A_LX_VAR.txt
<<< OK - usable for CIM or REST calls
>>> read input option file AUTHQA3/A_WIN_VAR.txt
<<< OK - usable for CIM or REST calls
>>> read input option file AUTHQA3/AuthentQA3.txt
<<< OK - usable for CIM or REST calls
>>> read input option file AUTHQA3/AuthentQA3Win.txt
<<< OK - usable for CIM or REST calls
>>> read input option file AUTHQA3/AuthentSNMP.txt
<<< OK - usable for SNMP calls
```

8.4.1.2 Central Process Logging for Each Host

The middle part of the central logging is the process log for each host and option input file.
For SNMP each option input file will be checked unless a successful connection is registered. For CIM or REST calls, multiple option input files are only checked if an authentication error is discovered.

Example of an inaccessible host:

```
>>> nnn.nnn.nnn.0
... try Community public
... try CIM AUTHQA3/AuthentSNMP.txt
... try CIM AUTHQA3/A_Admin.txt
... try REST AUTHQA3/AuthentSNMP.txt
... try REST AUTHQA3/A_Admin.txt
<<< nnn.nnn.nnn.0 3
```

Key:

The number after "<<< address" shows 0 for connection OK, 3 for connection UNKOWN.

Example of an SNMP connectable host:

```
>>> nnn.nnn.nnn.6
... try Community public
... SNMP connection OK
... no ServerView SNMP Agent information
... try AUTHQA3/A_LX_VAR.txt
<<< nnn.nnn.nnn.6 0
```

Example of detected CIM authentication errors:

```
>>> nnn.nnn.nnn.54
... try Community public
... SNMP connection OK
... SNMP ServerView information OK
... try CIM AUTHQA3/A_admin.txt
... CIM AUTHENTICATION ERROR
... try CIM AUTHQA3/A_LX_VAR.txt
... CIM AUTHENTICATION ERROR
...
<<< nnn.nnn.nnn.54 *
```

8.4.1.3 Summary Information

The summary part contains the result collections for "Timeout", "Authentication errors", "Connection is OK but no ServerView information is found" and detected host names.

For each detected host name a collection of found address hints is printed.

"address hints" are <address>|{SNMP,CIM,REST}[|{SV,SViRMC,iRMCReport,iRMCRedfish}]

- The first part is the tested address
- The second part indicates the connection protocol
- The third indicates whether ServerView Agent "SV" or ServerView iRMC information "SViRMC" is detected.
  In case of REST and existing iRMC Report or iRMC Redfish service, this is shortened as "iRMCReport" resp. "iRMCRedfish" because there exist two different REST interfaces for iRMC.

Any host which is definitely not reachable is omitted from the summary.

Example extract:

```
SUMMARY:
TIMEOUT
        nnn.nnn.nnn.4|CIM + nnn.nnn.nnn.11|CIM + ...
AUTHENTICATION ERROR
        nnn.nnn.nnn.10|CIM + ...
CONNECTION OK - NO SERVERVIEW
        nnn.nnn.nnn.6|CIM + nnn.nnn.nnn.28|CIM
CLIENT_TX120
        nnn.nnn.nnn.49|SNMP|SV
...
MX130-S22
        nnn.nnn.nnn.99|SNMP|SV
RX100S42
        nnn.nnn.nnn.26|SNMP|SV
...
RX200-S82
        nnn.nnn.nnn.144|SNMP|SV

...
```

8.4.2 Logging for Each Host Discovery

File name: <outputdir>/<address>.log

NOTE: This file is opened in append mode.

Each test log sequence is begins and ends with the current date and time. Inbetween is information on the tested protocol, script call and its output data (regardless on success) and the resulting connection status.

Example svout/nnn.nnn.nnn.10.log

```
START DATE:     Wed Apr 23 13:48:51 2014
ADDRESS:        nnn.nnn.nnn.10
>>> SNMP
... call: ./tool_fujitsu_server.pl -H nnn.nnn.nnn.10 --typetest --nopp -e
OK
    Protocol    = SNMP
    Name        = RX200S52
    Components  = Environment PowerSupply MassStorage Systemboard Network
DrvMonitor
    OS          = Windows Server 2008 Standard Service Pack 2
    FQDN        = RX200S52
    Type        = PRIMERGY with SV SNMP Agent
    Model       = PRIMERGY RX200 S5
    AdminURL    = http://nnn.nnn.nnn.11:80
    UpdateAgent = Status(UNKNOWN) SNMP-Monitoring=available
<<< OK
END DATE:       Wed Apr 23 13:48:53 2014
START DATE:     Wed Apr 23 13:48:53 2014
ADDRESS:        nnn.nnn.nnn.10
```

```
INFILE:         AUTHQA3/A_Admin.txt
>>> CIM
... call: ./tool_fujitsu_server_CIM.pl -H nnn.nnn.nnn.10 -I
AUTHQA3/A_Admin.txt --typetest –nopp -e
UNKNOWN  - AUTHENTICATION FAILED
    InAddress   = nnn.nnn.nnn.10

<<< AUTHENTICATION ERROR
END DATE:       Wed Apr 23 13:48:55 2014
...
```

8.4.3 Text Information for Each Host

File name: <outputdir>/<address>_<protocol>.txt

This file will only be created if the connection test is successful. The file contains the output information of the tool script.

Example svout/nnn.nnn.nnn.10_**SNMP**.txt:

```
OK
    Protocol    = SNMP
    Name        = RX200S52
    Components  = Environment PowerSupply MassStorage Systemboard Network
DrvMonitor
    OS          = Windows Server 2008 Standard Service Pack 2
    FQDN        = RX200S52
    Type        = PRIMERGY with SV SNMP Agent
    Model       = PRIMERGY RX200 S5
    AdminURL    = http://nnn.nnn.nnn.11:80
    UpdateAgent = Status(UNKNOWN) SNMP-Monitoring=available
```

Example svout/nnn.nnn.nnn.nnn_**CIM**.txt

```
OK
    Protocol    = WS-MAN
    Port        = 5985
    TransType   = http
    ServiceType = Windows
    OptionFile  = AUTHQA3/AuthentQA3Win.txt

    Name        = RX100S7-89
    Model       = PRIMERGY RX100 S7
    AdminURL    = http://nnn.nnn.nnn.104:80
    OS          = "Windows Server 2008 R2 Datacenter (x64)"
    Components  = Environment Power MassStorage Systemboard Network
DriverMonitor
    UpdateAgent = Status(UNKNOWN) Monitoring=available
```

Example svout/nnn.nnn.nnn.nnn_**REST**.txt

```
OK
    Protocol    = REST-Server-Control
    Port        = <default>
    TransType   = <default>
    OptionFile  = AUTH/ABG/IRMC0.txt

    Name        = H49003-RX300S8
    NodeType    = Windows
    Model       = PRIMERGY RX300 S8
    AdminURL    = http://nnn.nnn.nnn.103:80
    OS          = "Windows Server 2012 Datacenter"
    Agent       = SrvView Agent Server Control
    AgentVersion= 7.20.09.08
```

```
    Components  = Environment PowerSupply MassStorage Systemboard Network
    UpdateAgent = Status(unknown)
```

8.4.4 Nagios Configuration Files for Each Host

File name: <outputdir>/<address>_<protocol>_<hostname>.cfg

These files are only written if ServerView information is available (and readable). The format is meant for Nagios.

Example svout/nnn.nnn.nnn.010_SNMP_RX200S52.cfg

```
define host {
        host_name       nnn.nnn.nnn.010_RX200S52_SNMP
        display_name    RX200S52
        address         nnn.nnn.nnn.10
        hostgroups      primergy-servers,primergy-update-monitor
        use             windows-server,fj_server_icon
        notes_url       http://nnn.nnn.nnn.11:80
        register        1
}
```

Example svout/nnn.nnn.nnn.103_CIM_RX100S789.cfg

```
define host {
        host_name       nnn.nnn.nnn.103_RX100S789_CIM
        display_name    RX100S789
        address         nnn.nnn.nnn.103
        hostgroups      primergy-servers-CIM
        use             linux-server
        _SV_CIM_OPTIONS -UW -P5985 -Thttp  -SW -I
AUTHQA3/AuthentQA3Win.txt
        notes_url       http://nnn.nnn.nnn.104:80
        register        1
}
```

Example svout/nnn.nnn.nnn.003_REST_ H49003-RX300S8.cfg

```
define host {
        host_name       172.17.49.003_H49003-RX300S8_REST
        display_name    H49003-RX300S8
        address         172.17.49.3
        hostgroups      primergy-servers-REST,primergy-servers-REST-
update-monitor
        use             linux-server
        _SV_REST_OPTIONS        -SA -I AUTH/ABG/IRMC0.txt
        notes_url       http://nnn.nnn.nnn.103:80
        register        1
}
```

NOTES:

This configuration file can be used as-is, but the generated Nagios host name "host_name" within it is meant to be unique but may not be the ideal one.

The Nagios host name is created with address, host name and protocol because it might happen that one host has multiple addresses or in the worst case that multiple hosts have the same internal host name. It may also happen that one host is reachable via SNMP, CIM and REST protocol. In this case there will be multiple configuration files for one server!

Check the summary information in the central log file and check the files in the output directory.

The names of the output files and the generated Nagios host name can be influenced with additional options. For more about these, see chapter link "Advanced Options for Output Files and Generated Nagios Host Name".

9 Inventory – Get Information Unscheduled

Some server information does not need a scheduled call or does not contain status or performance values. This information data is a kind of "inventory" data.

The ServerView Plug-ins support a script whose name starts with **inventory_fujitsu_server.** Some of the information is server type and agent version-dependent.

The following data can be obtained with this:

- Enhanced system information
  (more detailed relative to the information fetched by the check or tool scripts)
- Network configuration information
- Firmware or software information
- Special unit information for PRIMEQUEST MMB (SNMP)
- Information about running processes

This script can be called stand-alone. At the end of this chapter is a description of how the "Enhanced system information" can be used as a non-scheduled Nagios service, so that corresponding information can be read in the Nagios user interfaces.

9.1 Fujitsu SNMP Server Inventory Tool

9.1.1 Script Name

Name of the script
inventory_fujitsu_server.pl

This is a Perl script which uses Net::SNMP calls.

It checks a FUJITSU server using SNMP. Currently this script is able to check PRIMERGY servers (meaning any server where ServerView SNMP Agent is installed and running), PRIMERGY Blade Servers (BX series) and PRIMEQUEST servers, as well as PRIMERGY Multi-Node servers (e.g.: CX400), and iRMC nodes where SNMP is enabled.

9.1.2 Text Rules for Automatic Scanning of Printouts

The print rules for inventory are similar but not identical to the ones for the check scripts.

The differences are as follows:

- 1st line – (the SERVER_OUTPUT line)
  - Starts with INVENTORY and contains the host address set by the calling options.
- Key-Value-Pair print:
  …indented <field><spacesortab>= <value>[<unit>] and each in a separate line
- Value print
  Values may or may not have quotation.
- For multi-line-unit prints - Rows
  … indented *** <item>['<index']] and each in a separate line

9.1.3 Enhanced System Information

HINT: The best way to show what information is fetched is to add here examples for each server type.

First the inventory script reads standard information available for all systems with enabled SNMP. This is data found in RFC1213.mib

- SNMP uptime
- System name, description, contact and location

9.1.3.1 Option

--inventory

This is the default option of the script. Gets the system information.

9.1.3.2 Server with ServerView SNMP Agent Installed (PRIMERGY)

The following information is fetched:

- Information about the ServerView Agent itself
- Agent information about the system
  - Start time
  - Serial number, UUID
  - Available hardware component groups
  - Operating system information
  - FQDN
  - System model and housing
  - Administrative URL
  - Multi-node information or parent MMB information if available
  - System memory
  - BIOS, VIOM and cluster information
- System board data
- System processor data
- TPM – Trusted Platform Module information

Example data:

```
 INVENTORY DATA FOR HOST = xxx.xxx.xxx.43
 * Standard System Information
     SNMP Uptime ="7 days, 04:46:05.38"
     Name        = H50043-Lovissa.nnn.nnn.nnn.net
     Description ="Hardware: Intel64 Family 6 Model 23 Stepping 10 AT/AT
 COMPATIBLE - Software: Windows Version 6.2 (Build 9200 Multiprocessor
 Free)"
     Location    = ABG
     Contact     ="…"
 * Used Agent
     Type        ="ServerView Agent"
     Company     = Fujitsu
     Version     = 7.01.10.06
 * Agent Information about the System
     OnTime      ="Thu Mar 12 07:32:06 2015"
     ID          = YK8B057639
     UUID        = 06BA5017-2C5B-11DF-A847-00199977DC05
```

```
    Components  ="Environment PowerSupply MassStorage Systemboard Network
DrvMonitor"
    OS          ="Windows Server 2012 Standard"
    OS-Revision ="6.2 Build 9200 "
    FQDN        = H50043-Lovissa.nnn.nnn.nnn.net
    Model       ="PRIMERGY TX150 S6"
    Housing     = TX150S6F
    AdminURL    = http://xxx.xxx.xxx.143:80
    Memory      = 8192MB
    BIOS        ="6.00 R1.15.2559.A1"
    VIOM        = disabled
    VIOM Bios   = disabled
    InCluster   = false
* Agent System Board Table
    *** SystemBoard[1.1]
        Name    ="SB#0"
        ID      = 32722778
        Product ="S26361-D2559-A12"
* Agent Management Processor Table
    *** Processor[1]
        Model           ="iRMC S2"
        FV-Version      ="3.10.054B0041"
* Agent Trusted Platform Module Table
    *** false: tpm[1]
        HardwareAvailable       = true
        BiosEnabled     = true
        Activated       = false
        Qwnership       = false
```

9.1.3.3 iRMC S4/S5 SNMP

This is similar to the above fetched data. The iRMC is dependent on whether an agent service is installed on the base server system and, if so, which one.

The following information is sought:

- Information about the firmware itself
- Information as to whether an agent service is installed on the base server system and, if so, which one.
- Agent information about the base server system
    - Start time
    - Serial number, UUID
    - Available hardware component groups
    - Operating system information
    - FQDN
    - System model and housing
    - Administrative URL
    - Multi-node information or parent MMB information if available
    - System memory
    - BIOS, VIOM and cluster information
- System board data
- System processor data

- TPM – Trusted Platform Module information

Example data – "No Agent", meaning no Agentless Service or no ServerView SNMP Agent installed

```
INVENTORY DATA FOR HOST = n.n.n.16
* Standard System Information
    SNMP Uptime ="41 days, 01:38:06.41"
    Name        = iRMC523685
    Description ="Primergy iRMC S4 #1 Fri Sep 26 15:19:12 CEST 2014"
    Location    = Unknown
    Contact     = root@localhost
* Used Firmware
    Type        ="iRMC Firmware"
    Company     = Fujitsu
    Version     ="Build: 7.69.F"
* Used Agent
    Agent       ="No Agent"
* Agent Information about the System
    ID          = S#1250123
    UUID        = 63B231E9-40B0-11E4-A3E5-901B0E5230D0
    Components  ="Environment PowerSupply Systemboard AgentStatus"
    Model       ="PRIMERGY BX2580 M1"
    Housing     = BX2580M1
    AdminURL    = http://n.n.n.16:80
    Memory      = 16384MB
    BIOS        ="V5.0.0.9 R1.15.0 for D3321-A1x"
    VIOM        = disabled
    VIOM Bios   = disabled
* Agent System Board Table
    *** SystemBoard[1.1]
        Name    ="SB#0"
        ID      = SQ1438MA00067
```

Example data – Agentless Service installed

```
INVENTORY DATA FOR HOST = n.n.n.161
* Standard System Information
    SNMP Uptime ="41 days, 19:49:08.26"
    Name        = iRMC3FB5C1
    Description ="Primergy iRMC S4"
    Location    ="- unknown -"
    Contact     ="- unknown -"
* Used Firmware
    Type        ="iRMC Firmware"
    Company     = Fujitsu
    Version     ="Build: 7.69.F"
* Used Agent
    Agent       ="Agentless Service"
    Version     = 7.01.16.04
* Agent Information about the System
    OnTime      ="Tue Mar 17 11:47:27 2015"
    ID          = YM2U000999
    UUID        = 66198855-85E8-48A2-A934-094C729C0E07
    Components  ="Environment PowerSupply Systemboard MassStorage
Network DrvMonitor AgentStatus"
    OS          ="Windows Server 2012 R2 Standard"
    OS-Revision ="6.3 Build 9600 "
    FQDN        = SW1-CC740
    Model       ="CELSIUS C740"
    Housing     ="CELSIUS C740"
    AdminURL    = http://n.n.n.161:80
```

```
    Memory      = 16384MB
    BIOS        ="V5.0.0.9 R0.91.0 for D3288-A1x"
    VIOM        = disabled
    VIOM Bios   = disabled
    InCluster   = false
  * Agent System Board Table
    *** SystemBoard[1.1]
        Name    ="SB#0"
        ID      = 45680453
        Product ="S26361-D3288-A10"
  * Agent Management Processor Table
    *** Processor[1]
        Model           ="iRMC S4"
        FV-Version      ="7.69F"
  * Agent Trusted Platform Module Table
    *** true: tpm[1]
        HardwareAvailable       = true
        BiosEnabled     = true
        Activated       = true
        Qwnership       = true
```

Example data – ServerView SNMP Agent installed

```
  INVENTORY DATA FOR HOST = n.n.n.159
  * Standard System Information
    SNMP Uptime ="19 days, 00:07:02.84"
    Name        = iRMC240226
    Description ="Primergy iRMC S4 #1 Fri Sep 26 15:19:12 CEST 2014"
    Location    = Unknown
    Contact     = root@localhost
  * Used Firmware
    Type        ="iRMC Firmware"
    Company     = Fujitsu
    Version     ="Build: 7.69.F"
  * Used Agent
    Agent       ="Mgmt. Agent"
    Version     = 7.01.20
  * Agent Information about the System
    OnTime      ="Wed Mar  4 09:45:20 2015"
    ID          = S#1250058
    UUID        = 00020003-0004-0005-0006-000700080009
    Components  ="Environment PowerSupply Systemboard MassStorage
  Network DrvMonitor AgentStatus"
    OS          ="Windows Server 2012 R2 Standard"
    OS-Revision ="6.3 Build 9600 "
    FQDN        = H49059-BX2580M1N.servware.abg.fsc.net
    Model       ="PRIMERGY BX2580 M1"
    Housing     = BX2580M1
    AdminURL    = http://n.n.n.159:80
    Memory      = 8192MB
    BIOS        ="V5.0.0.9 R1.7.0 for D3321-A1x"
    VIOM        = disabled
    VIOM Bios   = disabled
  * Agent System Board Table
    *** SystemBoard[1.1]
        Name    ="SB#0"
        ID      = SQ1411MA00036
  * Agent Trusted Platform Module Table
    *** unknown: tpm[1]
        HardwareAvailable       = false
        BiosEnabled     = unknown
```

```
        Activated       = unknown
        Qwnership       = unknown
```

9.1.3.4 PRIMERGY Blade MMB

The following information is sought:

- Type of firmware agent used
- Agent information about the base server system
  - Serial number
  - Local time of the MMB
  - Administrative URL
  - System housing
  - Multi-node information or parent MMB information if available
  - VIOM
  - Type and number of blades controlled with this MMB
- MMB data including version
- System control counters

Example data:

```
  INVENTORY DATA FOR HOST = n.n.n.232
  * Standard System Information
      SNMP Uptime="2 days, 20:47:37.91"
      Name       = BX900-2
      Description="PRIMERGY BX900 A3C4096526"
      Location   ="ABG"
      Contact    ="..."
  * Used Agent
      Type       ="PRIMERGY Management Blade Agent"
  * Agent Information about the System
      ID         = QTFCQK8240035
      Name       = BX900-2
      LocalTime   ="03/19/2015 12:46:34"
      IP         = n.n.n.232
      AdminURL   = http://n.n.n.232:80
      HousingType= BX900
      VIOM       = managed
      Sub-Blades ="ServerBlades(9) Switch(7) Storage(1)"
  * Management Blade Table
      *** ok: MMB[1]
          ID     = SQ1347MI00008
          Product="PRIMERGY BX900 Management Blade S1"
          MAC    = 90:1B:0E:22:BA:6D
          RunMode= master
          Maunfacturer   = FUJITSU
          HW-Version     = 04
          FW-Version     = 5.44
      *** standby: MMB[2]
          ID     = SQ1347MI00187
          Product="PRIMERGY BX900 Management Blade S1"
          MAC    = 90:1B:0E:22:BB:DF
          RunMode= slave
          Maunfacturer   = FUJITSU
          HW-Version     = 04
          FW-Version     = 5.44
```

```
 * Agent System Control Counter
     Fans               = 48
     TemperaturSensors  = 22
     PowerSupplyUnits   = 4
     PSURedundancy      = 0
     UPS                = 0
```

9.1.3.5 PRIMEQUEST MMB

The following information is sought:

- Type of firmware agent used
- Agent information about the base server system
  - Serial number, MMB internal name
  - Model information
  - Administrative URL
- MMB processor data including version
- Management node table including MAC
- Server table
- System board information
- TPM – Trusted Platform Module information

Example data:

```
INVENTORY DATA FOR HOST = xxx.xxx.xxx.222
* Standard System Information
    SNMP Uptime ="1 day, 20:22:11.67"
    Name        = PRIMEQUESTFTS7
    Description ="PRIMEQUEST Management Board"
    Location    ="…"
    Contact     ="…"
* Used Agent
    Type        ="PRIMEQUEST Agent"
* Agent Information about the System
    ID          = 1541329002
    Name        = MCF3AC111
    Model       ="PRIMEQUEST 2800E"
    AdminURL    = http://172.17.55.222:8081
* Agent Management Processor Table
    *** Processor[136.1]
        Model   ="MMB"
        FW-Version      = 2.22
    *** Processor[137.1]
        Model   ="MMB"
        FW-Version      = 2.22
* Management Node Table
    *** Node[136.1]
        MAC     = 2C:D4:44:F0:8E:FC
        Class   = secondary-management-blade
    *** Node[136.2]
        MAC     = 2C:D4:44:F0:8E:FC
        Class   = secondary-management-blade
    *** Node[137.1]
        Name    ="PRIMEQUEST1541329002"
        Address = xxx.xxx.xxx.222
        MAC     = 2C:D4:44:F0:8F:00
```

```
        Class   = management-blade
    *** Node[137.2]
        MAC     = 2C:D4:44:F0:8F:00
        Class   = management-blade
    *** Node[137.3]
        Name    ="PRIMEQUEST1541329002"
        Address = ::
        MAC     = 2C:D4:44:F0:8F:00
        Class   = management-blade
    *** Node[137.4]
        MAC     = 2C:D4:44:F0:8F:00
        Class   = management-blade
* Server Table
    *** Server[2]
        Partition       = 0
        BootStatus      = ..unexpected..
        ManagementIP    = xxx.xxx.xxx.142
        UUID            = 9AB0C000-F668-11DE-8000-2CD444F11800
    *** Server[3]
        Partition       = 1
        BootStatus      = os-running
        ManagementIP    = xxx.xxx.xxx.141
        UUID            = 9AB0C000-F668-11DE-8100-2CD444F11801
    *** Server[5]
        Partition       = 3
        BootStatus      = os-running
        ManagementIP    = xxx.xxx.xxx.143
        UUID            = 9AB0C000-F668-11DE-8300-2CD444F11803
    *** Server[6]
        Partition       = 4
        BootStatus      = os-running
        UUID            = 9AB0C000-F668-11DE-8400-2CD444F11800
    *** Server[7]
        Partition       = 5
        BootStatus      = reset
        UUID            = 9AB0C000-F668-11DE-8500-2CD444F11800
* System Board Table
    *** SystemBoard[19]
        ID      = PP132801WF
        Product ="FUJITSU LIMITED"
        Model   ="SB"
        Revision= CA07603-D003 A1
    *** SystemBoard[20]
        ID      = PP132702ZY
        Product ="FUJITSU LIMITED"
        Model   ="SB"
        Revision= CA07603-D003 A1
    *** SystemBoard[21]
        ID      = PP13280189
        Product ="FUJITSU LIMITED"
        Model   ="SB"
        Revision= CA07603-D003 A1
    *** SystemBoard[22]
        ID      = PP1328018B
        Product ="FUJITSU LIMITED"
        Model   ="SB"
        Revision= CA07603-D003 A1
* Trusted Platform Module Table
    *** TPM[2]
        Enabled                 = unknown
```

```
      Activated              = unknown
   *** TPM[3]
      Enabled                = unknown
      Activated              = unknown
   *** TPM[5]
      Enabled                = unknown
      Activated              = unknown
```

9.1.4 Network Configuration Information (IP, MAC)

HINT: The best way to show what information is fetched is to add here examples for each server type.

There is no additional network configuration information for the following types:

- iRMC S4/S5 and no agent service installed on the base server system

9.1.4.1 Option

--invnet

Search for configured network addresses

9.1.4.2 Server with ServerView SNMP Agent Installed (PRIMERGY)

Example data:

```
* Agent Management Nodes
   *** Node[1]
       IP      = xxx.xxx.xxx.43
       MAC     = 00:19:99:77:DC:05
   *** Node[2]
       IP      = fe80::…:76bc
       MAC     = 00:19:99:77:DC:05
   *** Node[3]
       IP      = xxx.xxx.xxx.1
       MAC     = 00:50:56:C0:00:01
   *** Node[4]
       IP      = fe80::…:16f0
       MAC     = 00:50:56:C0:00:01
   *** Node[5]
       IP      = xxx.xxx.xxx.1
       MAC     = 00:50:56:C0:00:08
   *** Node[6]
       IP      = fe80::…:4d87
       MAC     = 00:50:56:C0:00:08
   *** Node[7]
       IP      = xxx.xxx.xxx.143
       ControllerType  ="iRMC S2"
       Class   = baseboard-controller
       MAC     = 00:19:99:79:E0:AC
   *** Node[8]
       IP      = fe80::…:e0ac
       ControllerType  ="iRMC S2"
       Class   = baseboard-controller
       MAC     = 00:19:99:79:E0:AC
```

9.1.4.3 iRMC S4/S5 SNMP

Example data – Agentless Service or ServerView SNMP Agent installed

```
* Agent Management Nodes
   *** Node[1]
       IP      = xxx.xxx.xxx.169
       MAC     = 90:1B:0E:3F:B2:13
   *** Node[2]
```

```
        IP      = fe80::…:68c6
        MAC     = 90:1B:0E:3F:B2:13
    *** Node[3]
        IP      = xxx.xxx.xxx.162
        MAC     = 90:1B:0E:43:0C:5F
    *** Node[4]
        IP      = fe80::…:a40d
        MAC     = 90:1B:0E:43:0C:5F
    *** Node[5]
        IP      = xxx.xxx.xxx.161
        ControllerType  ="iRMC S4"
        Class   = baseboard-controller
        MAC     = 90:1B:0E:3F:B5:C1
```

9.1.4.4 PRIMERGY Blade MMB

Example data

```
* Agent Information around Network
    Gateway     = xxx.xxx.xxx.1
    DNS         = enable
    DNS IP      = xxx.xxx.xxx.99
    DNS IP      = xxx.xxx.xxx.98
```

9.1.4.5 PRIMEQUEST MMB

Example data:

```
* Lan Interface Table
    *** LanIF[2.0]
        MAC     = 2C:D4:44:F1:45:46
    *** LanIF[2.1]
        MAC     = 2C:D4:44:F1:45:47
    *** LanIF[3.4]
        MAC     = 2C:D4:44:F0:00:6E
    *** LanIF[3.5]
        MAC     = 2C:D4:44:F0:00:6F
    *** LanIF[5.2]
        MAC     = 2C:D4:44:F1:45:58
    *** LanIF[5.3]
        MAC     = 2C:D4:44:F1:45:59
    *** LanIF[6.0]
        MAC     = 2C:D4:44:F1:45:46
    *** LanIF[6.1]
        MAC     = 2C:D4:44:F1:45:47
```

9.1.5 Firmware Information

HINT: The best way to show what information is fetched is to add here examples for each server type.

There is no information for following the types:

- iRMC S4/S5
- PRIMERGY Blade MMB

9.1.5.1 Option

--invfw

Print firmware table resp. print component version table including firmware information

9.1.5.2 Server with ServerView SNMP Agent Installed (PRIMERGY)

Example data:

```
 * VersionView Component Table
```

```
        *** Component[1]
            Name            ="H50043-LOVISSA"
            Description     ="Computer Name"
        *** Component[2]
            Name            ="H50043-Lovissa.nnn.nnn.nnn.net"
            Description     ="Full qualified DNS Name"
            Version         ="DNS"
        *** Component[3]
            Name            ="PRIMERGY TX150 S6"
            Description     ="Cabinet"
            Version         ="GS01"
            SerialID        ="YK8B057639"
            Vendor          ="FUJITSU"
        *** Component[4]
            Name            ="TX150S6F"
            Description     ="Chassis"
            Version         ="GS01"
            SerialID        ="YK8B057639"
            Vendor          ="FUJITSU"
        *** Component[5]
            Name            ="POWERSUPPLY 350W"
            Description     ="Power Supply"
            Version         ="GS01"
            Vendor          ="HIPRO"
    . . .
        *** Component[244]
            Name            ="WDC WD7502ABYS-50A6B0 03.00C07"
            Description     ="IDE direct access"
            Version         ="03.00C07"
            SerialID        ="WD-WMATW0322329"
        *** Component[245]
            Name            ="WDC WD7502ABYS-50A6B0 03.00C07"
            Description     ="IDE direct access"
            Version         ="03.00C07"
            SerialID        ="WD-WMATW0322612"
        *** Component[246]
            Name            ="WDC WD7502ABYS-50A6B0 03.00C07"
            Description     ="IDE direct access"
            Version         ="03.00C07"
            SerialID        ="WD-WMATW0322621"
        *** Component[247]
            Name            ="DVD RW AD-7700S 1.44"
            Description     ="IDE CD_ROM"
            Version         ="1.44"
            Vendor          ="Opti"
```

9.1.5.3 PRIMEQUEST MMB

Example data:

```
   * Firmware Version Table
     *** Firmware[1]
         Unit    = Chassis
         Type    = total
         Model   ="Unified Firmware Version"
         Version = BA14113
     *** Firmware[19]
         Unit    = SystemBoard
         Type    = bios
         Model   ="BIOS"
         Version = 1.77
```

```
    *** Firmware[19]
        Unit    = SystemBoard
        Type    = baseboard-management-controller
        Model   ="BMC"
        Version = 1.29F
    *** Firmware[20]
        Unit    = SystemBoard
        Type    = bios
        Model   ="BIOS"
        Version = 1.77
    *** Firmware[20]
        Unit    = SystemBoard
        Type    = baseboard-management-controller
        Model   ="BMC"
        Version = 1.29F
    *** Firmware[21]
        Unit    = SystemBoard
        Type    = bios
        Model   ="BIOS"
        Version = 1.77
    *** Firmware[21]
        Unit    = SystemBoard
        Type    = baseboard-management-controller
        Model   ="BMC"
        Version = 1.29F
    *** Firmware[22]
        Unit    = SystemBoard
        Type    = bios
        Model   ="BIOS"
        Version = 1.77
    *** Firmware[22]
        Unit    = SystemBoard
        Type    = baseboard-management-controller
        Model   ="BMC"
        Version = 1.29F
    *** Firmware[136]
        Unit    = MMB
        Type    = management-controller
        Model   ="MMB"
        Version = 2.22
    *** Firmware[137]
        Unit    = MMB
        Type    = management-controller
        Model   ="MMB"
        Version = 2.22
```

9.1.6 PRIMEQUEST MMB - Unit Table Information

HINT: The best way to show what information is fetched is to add examples here.

9.1.6.1 Option

--invunit

Print complete unit table of the MMB

9.1.6.2 PRIMEQUEST MMB

Example data:

```
    * Unit Table
        *** Unit[1]
            ID      = 1541329002
```

```
            Class   = chassis
            Name    ="MCF3AC111"
            Location="…"
            Contact ="…"
            AdminURL=http://xxx.xxx.xxx.222:8081
            Model   ="PRIMEQUEST 2800E"
        *** Unit[19]
            ID      = PP132801WF
            Class   = sb
            Name    ="SB#0"
            Model   ="SB"
        *** Unit[20]
            ID      = PP132702ZY
            Class   = sb
            Name    ="SB#1"
            Model   ="SB"
        *** Unit[21]
            ID      = PP13280189
            Class   = sb
            Name    ="SB#2"
            Model   ="SB"
. . .
        *** Unit[167]
            ID      = SQ1310MK00029
            Class   = du
            Name    ="DU#1"
        *** Unit[180]
            ID      = G743LE0047AEF
            Class   = psu
            Name    ="PSU#0"
            Model   ="AA25370L"
        *** Unit[182]
            ID      = G743LE004VAEF
            Class   = psu
            Name    ="PSU#2"
            Model   ="AA25370L"
        *** Unit[183]
            ID      = G743LD009DAEF
            Class   = psu
            Name    ="PSU#3"
            Model   ="AA25370L"
        *** Unit[185]
            ID      = G743LD00AZAEF
            Class   = psu
            Name    ="PSU#5"
            Model   ="AA25370L"
```

9.1.7 Process Information

HINT: The best way to show what information is fetched is to add examples here.

The data from running processes is non-permanent!

There is no process information for the following types:

- iRMC S4/S5
- PRIMERGY Blade MMB
- PRIMEQUEST

9.1.7.1 Option

--invproc

Print process table

9.1.7.2 Server with ServerView SNMP Agent Installed (PRIMERGY)

HINT:

The printed information and the format are dependent on the ServerView Agent version. Here is a sample from version 7 or higher.

Example data:

```
   * Process Table
       *** Process[0]
           Name            = System Idle Process
           CPU             = 94 %
       *** Process[4]
           Name            = System
       *** Process[296]
           Name            = smss.exe
           Path            = C:\Windows\System32\smss.exe
           Description     = Windows Session Manager
           Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
       *** Process[376]
           Name            = dwm.exe
           Path            = C:\Windows\system32\dwm.exe
           Description     = Desktop Window Manager
           Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
       *** Process[456]
           Name            = svchost.exe
           Path            = C:\Windows\system32\svchost.exe
           Description     = Host Process for Windows Services
           Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
       *** Process[484]
           Name            = csrss.exe
           Path            = C:\Windows\system32\csrss.exe
           Description     = Client Server Runtime Process
           Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
   . . .
       *** Process[2948]
           Name            = wmiprvse.exe
           Path            = C:\Windows\system32\wbem\wmiprvse.exe
           Description     = WMI Provider Host
           Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
       *** Process[3220]
           Name            = CNTAoSMgr.exe
           Path            = C:\Program Files (x86)\OfficeScan
   NT\CNTAoSMgr.exe
           Description     = Trend Micro OfficeScan Client Plug-in Service
   Manager
           Version         = 2.0.0.1249
       *** Process[3228]
           Name            = conhost.exe
           Path            = C:\Windows\system32\conhost.exe
           Description     = Console Window Host
           Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
       *** Process[3232]
       *** Process[3364]
       *** Process[3568]
       *** Process[3820]
           Name            = csrss.exe
           Path            = C:\Windows\system32\csrss.exe
```

```
        Description     = Client Server Runtime Process
        Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
    *** Process[3876]
        Name            = winlogon.exe
        Path            = C:\Windows\system32\winlogon.exe
        Description     = Windows Logon Application
        Version         = 6.2.9200.16384 (win8_rtm.120725-1247)
```

9.1.8 Sample Nagios Configuration

Example file **serverview_inventory.cfg_**

In this file, all ServerView SNMP Nagios host groups are referenced! Because of this, an underscore '_' is appended to the file name so that it is not automatically used by Nagios. Read this file and change it if necessary, then remove the trailing underscore.

Command Definition

```
define command {
      command_name      inventory_fujitsu_server
      command_line      $USER1$/inventory_fujitsu_server.pl -H
$HOSTADDRESS$ $_HOSTSV_OPTIONS$ $ARG1$
      register          1
}
```

Expected: **$USER1$** must hint on the plugin directory path (see resources.cfg of the Nagios scheduler)

Service Definition

```
define service {
      hostgroup_name          all-fujitsu-servers,all-fujitsu-servers-
iRMC-SNMP
      service_description     SV System Inventory
      servicegroups           serverview
      use                     generic-service
      check_command           inventory_fujitsu_server!--inventory
      active_checks_enabled   1
      passive_checks_enabled  0
      check_period            none
      register                1
}

define servicedependency {
    dependent_service_description   SV System Inventory
    hostgroup_name                  all-fujitsu-servers,all-fujitsu-
servers-iRMC-SNMP
    service_description             SV SNMP Uptime
    execution_failure_criteria      w,u,c
    notification_failure_criteria   w,u,c
    inherits_parent                 1
}
```

The service will never be called (scheduled) because of the check_period "none". The Nagios Administrator user can **force** the call at a time where the server is powerd on. The Nagios user interfaces support an interface for this.

The service should not be called if SNMP is not up at calling time – the service dependency forces this.

Advantage of check_period "none":

- If successful, the script returns a large amount of data. To prevent it being stored in Nagios databases, check_period "none" can be used.
- The administrator can check that the script is only called if the system is up. Otherwise the data will be lost until the system is reachable again.

10 Managing and Administration of Fujitsu Servers

10.1 Fujitsu Update Management Tool

For CIM:
This feature is currently only available "in-band" for Linux and Windows and is based on the CIM-Provider of ServerView Agent 7.10.18 (or higher).
For REST:
Available for (in-band) ServerView Agent V7.10 and the Server Control service

10.1.1 Script Names

Name of the scripts

updmanag_fujitsu_server_CIM.pl

This is a Perl script which uses wbemcli or fujitsu_server_wsman.pl calls.

updmanag_fujitsu_server_REST.pl

This is a Perl script which uses curl command calls.

This is a script for managing features around ServerView Update Management as-far-as possible.

For CIM:

The managing script uses wbemcli calls (for the CIM-XML protocol) or fujitsu_server_wsman.pl calls for the WS-MAN protocol. For WS-MAN usage, the wsman script must be placed parallel to the management script.

The wsman script needs a special Perl class. See other descriptions of fuitsu_server_wsman.pl.

10.1.2 Requirements for wbemcli or OpenWSMan

For the managing operations, "methods" of CIM classes must be "invoked". Tests have shown that this requires special versions of the above-mentioned tools:

OpenWSMan

Invoking of methods via the OpenWSMan API requires V2.4.8 or higher - there have been errors in older versions.

wbemcli V1.6.3

There is a known bug in this version.
Patch: http://sourceforge.net/p/sblim/bugs/2743/
Error message "`* wbemcli: Http Exception: HTTP response code said error`":

10.1.3 Update Status – Host, Update Check and Update Job

Besides the central host update status value which is also read by the check_fujitsu scripts above, there are two more status values. One is the status of "Update Checks" – the process to find out whether updates are needed or not. The other is the status of "Update Jobs" – the real update process.

Option overview:
--status

Print all status values. "status" is the default option of the script.

This can be split into three actions:

{ --updstatus | --updcheckstatus | --updjobstatus }

The values:
In this case the status values are more or less self-explanatory. A single status value can be fetched using the corresponding option --upd* above instead of --status.

If all status values are to be fetched or if only the host status value is wanted (--updstatus), then the host update status is mapped to the Nagios return codes.

--updstatus

The host update status is the same as the one described for the check scripts.

--updcheckstatus:

Additional information will be printed in addition to the status if available. If only updcheckstatus is selected, the check status values will be mapped to Nagios return codes.

Example:

```
OK - UpdateCheckStatus(Done - OK)
Update Check: LastCheckTime="Tue Apr 14 13:36:12 2015"
```

Status strings:	"Done - OK",	"Done - Error",	"Downloading",	"Checking"
Return codes:	OK	WARNING,	UNKNOWN	UNKNOWN

--updjobstatus:

Additional information will be printed in addition to the status value if available. If only updjobstatus is selected, the job status values will be mapped to Nagios return codes.

Example:

```
WARNING - UpdateJobStatus(Done - Error)
Update Job: UpdateJobStartTime="Fri Apr 24 11:23:44 2015"
LogFile="C:/Program Files/Fujitsu/ServerView
Suite/Agents/Server
Control/Data/EM_UPDATE/UpdateJob/Logs\job_1_log.xml"
```

Status strings: "Waiting", "Downloading", "Downloaded", "Updating", "Updated", "Done - OK", "Done - Error"

Return codes: OK for "Done – OK", WARNING for "DONE - Error", all others to UNKNOWN

10.1.4 Update Configuration – Get and Set

Option overview:
--getconfig [-O|--outputdir=<dir>] |
--setconfig=<file> |
--setconfigarg --arguments=<keyvalue-list>

10.1.4.1 Get the Update Configuration Settings

Get "Update Configuration" information. This will be printed with the exception of the repository password. If outputdir is specified, all information (including password) will be printed in a key=value formatted file.

The file name is <dir>/<hostaddress without special signs>_CFG.txt.

This file also contains a short description as comments of the available values and their data types (comments are lines starting with #).

Short description of the values (written in the file):

```
#       UpdAlertJobFinished (uint16) - (0=disable,1=enable)
#       UpdAlertNewUpdates (uint16) - (0=disable,1=enable)
#       UpdAutomaticInstall (boolean)
#       UpdDeleteBinaryAfterUpdate (boolean)
#       UpdDownloadMode (uint16) - (0=no,1=aftercheck)
#       UpdDownloadProtocol (uint16) - (0=http,1=https)
#       UpdDownloadRepositoryPath (string)
#       UpdDownloadServerAddress (string)
#       UpdRepositoryAccess (uint16) -
(0=local_RO,1=local_RW,2=remote_RO,3=iRMC_RO)
#       UpdRepositoryPassword (string)
#       UpdRepositoryPath (string)
#       UpdRepositoryUserId (string)
#       UpdScheduleDate (uint64) - (time_t)
#       UpdScheduleFrequency (uint64) - number of days
#       UpdUpdateCheckMode (uint16) -
(0=manually,1=aftermodification,2=scheduler)
#       ConfHttpProxyServerUsage (uint16) -
(0=no,1=systemconfig,2=userconfig)
#       ConfHttpProxyServerPort (uint32)
#       ConfHttpProxyServerAddress (string)
#       ConfHttpProxyServerId (string)
#       ConfHttpProxyServerPasswd (string)
```

10.1.4.2 Set the Update Configuration Settings

This operation needs configuration properties as input. These can be specified in a file in the format of the “Get Configuration Output File” (see above) – a collection of simple key=value lines or they can be specified via arguments (usable for single property settings).

"OK" will be printed on successful start.

Call script with --getconfig to check the results.

10.1.5 Update Check Process – Start and Get Log File

Option overview:

--startcheck | --getchecklog

10.1.5.1 Start the Update Check

This operation needs no additional information. "OK" will be printed on successful start.

Call the script with --updcheckstatus or --getchecklog to get more information about the results of the check itself.

10.1.5.2 Get the Update Check Log File

The ServerView Update Manager returns the contents of the update check log file. The script prints the content if sucessful.

The format of the content is specified by the ServerView Update Manager itself.

10.1.6 Components to be Updated, Installed Components and Release Notes

The update scripts and the already described check scripts know options to get the "Update Difference List" and the "Installed Component List".

The update scripts enable the information to be written to files. The update difference list can be used as an input file for Update Jobs. If components are removed or commented in this file they will not be updated.

With the Update Manager scripts, additional release notes can be fetched for the components in addition to these two lists.

Option overview:

--difflist [-O|--outputdir=<dir>] |

--instlist [-O|--outputdir=<dir>] |

--getreleasenotes | --getdiffreleasenotes | --getonereleasenote=<comppath>

10.1.6.1 Get Update Installed Component List

This list contains all software components that can be updated at some time by the ServerView Update Manager.

This list is only available after a successful "Update Check".

For more on this see chapter link "Start the Update Check".

10.1.6.2 Get Update Component Difference List

This list contains all software components that can be updated at some time by the ServerView Update Manager.

This list is only available after a successful "Update Check".

For more on this see chapter link "Start the Update Check".

10.1.6.3 Get Release Notes

With the **getreleasenotes** option, all available release notes will be fetched. With **getdiffreleasenotes,** only the release notes of the components in the update difference list will be read. With **getonereleasenote** a single relase note is fetched.

This data is only available after a successful "Update Check".

The format of each release note depends on the component.

If a single release note is to be fetched, only the contents of this release note are printed.

For multiple release notes the following data is printed:

On success, the first printed line is "OK - - Found release notes".

For each component for which a release note exists, the following text block is printed:

```
AVAILABLE: … the component path name …
<ReleaseNotes>
… the corresponding release note …
</ReleaseNotes>
…new line…
```

If there is no release note for a component, no "<ReleaseNotes>" part and status "UNKNOWN" instead of "AVAILABLE" is printed.

10.1.7 Update Job Process – Start and Cancel and Log Information

Option overview:
{ { --startjoball | --startjob=<file>] [--jobstarttime=<timestampinseconds>] }
| --canceljob
| --getjobcomponentlog | --getjoblogfile } }

10.1.7.1 Start the Update Job

The operation for --startjoball requires no additional parameter. All component paths (see "Update Difference List") will be updated. The operations behind startjob=<file> require a file with component path lines - see format of the "Update Difference List". All uncommented lines will be used.

Use jobstarttime to schedule the start of the update job. Use time in seconds since 1.1.1970 and specify the local time for the addressed system.

NOTE:

There will be warning if one or more component paths already exist in the component collection or if a component path is wrong. If no component could be successfully added to the component collection, the whole operation is stopped.

"OK" and "UpdateJob(Started)" will be printed on successful start.

Call the script with --updjobstatus to get the job status information.

10.1.7.2 Cancel the Update Job

There is not much to say about canceling update jobs. The script returns "OK - -CancelUpdateJob(Started)" if the cancel action can be called.

10.1.7.3 Logging Information of the Update Job

There are two logging formats.

Options:

getjobcomponentlog

The first format contains information for each updated component.

getjoblogfile

The second format is an XML file transferred from the target system with all results for all components.

Information for each updated component:

The script exit code and the first line print contains "OK" if a component log can be fetched.

The sample output shows the printed information parts.

For each component:

One line with the update status followed by ':' and the component path name as the identifier of the corresponding log data.

The lines below starting with hash '#' belong to this component and show some details.

Sample output for the update of one component:

```
OK
Done - Error: ComponentLog[PrimSupportPack-Win\FSC_SCAN\V06.80]
# ReturnCode=31
# StartTime="Thu Jul 30 12:47:47 2015" EndTime="Thu Jul 30 12:48:08 2015"
# LogText="command 'PRIMEUP' returned exit code: 008 = \"PSP not installed\""
```

XML file:

In the original path of the XML log file (see extended status information) is an XSL file. This XSL file can be used to present XML file of the update job process in the best way any.

Use getjoblogfile to fetch the XML log file and copy it and the XSL file into one directory to view the results in a browser.

10.1.8 Sample Nagios Configuration

CIM example file **cfg/UpdManagCIM/serverview_updatemanagement_CIM.cfg**

REST example file **cfg/UpdManagREST/serverview_updatemanagement_REST.cfg**

The tool for managing updates starts actions which result in a large amount of data. This cannot be viewed directly in the Nagios-based front-ends. There are some actions which require the editing of files and this cannot be integrated in the front-ends. Therefore only some actions of the update management are added into the above-named configuration for Nagios.

10.1.8.1 Not-Supported Update Management Actions

Update configuration:

Setting the configuration is best done by editing a file in which the current configuration is stored. The modification of the configuration must be executed once for each server to be managed.
Because of this, no Nagios service is defined in the example configuration.

Update check log file:

This log file might exceed the size limit for Nagios services.
Because of this, no Nagios service is defined in the example configuration.

Update Release Files

The release files exceed the size limit for Nagios services.

Selection of component to be installed

The complete list of components to be installed might exceed the size limit for Nagios services. This list of components could not be edited in the Nagios front-ends.
Because of this, no Nagios service is defined in the example configuration.

Update job log file or information:

This data might exceed the size limit for Nagios services.
Because of this, no Nagios service is defined in the example configuration.

10.1.8.2 Supported Update Management Actions

The following actions can be integrated:

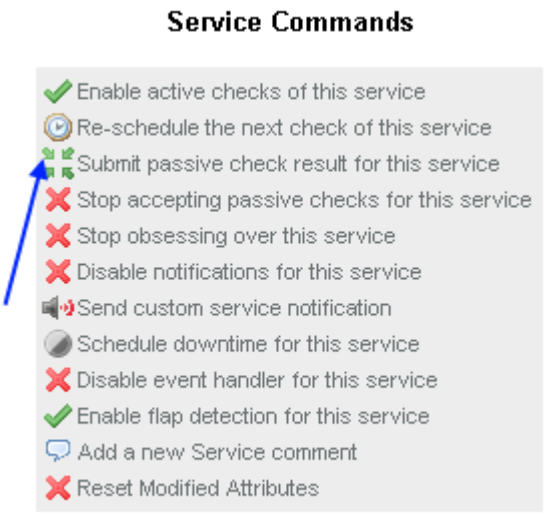
- Get all status values for host, update check and update job - get this information scheduled
- Start update check - defined as an unscheduled call - the administrator user can force the call in the front-end
- Set parameters for update job - set selection list file if wanted
  These are so-called "passive checks", where the administrator user can set data in the front-end
- Start update job for all components or start job for a selected list - defined as an unscheduled call - the administrator user can force the call in the front-end

10.1.8.3 Set Update Job File Parameter - How to Handle a Passive Nagios Service

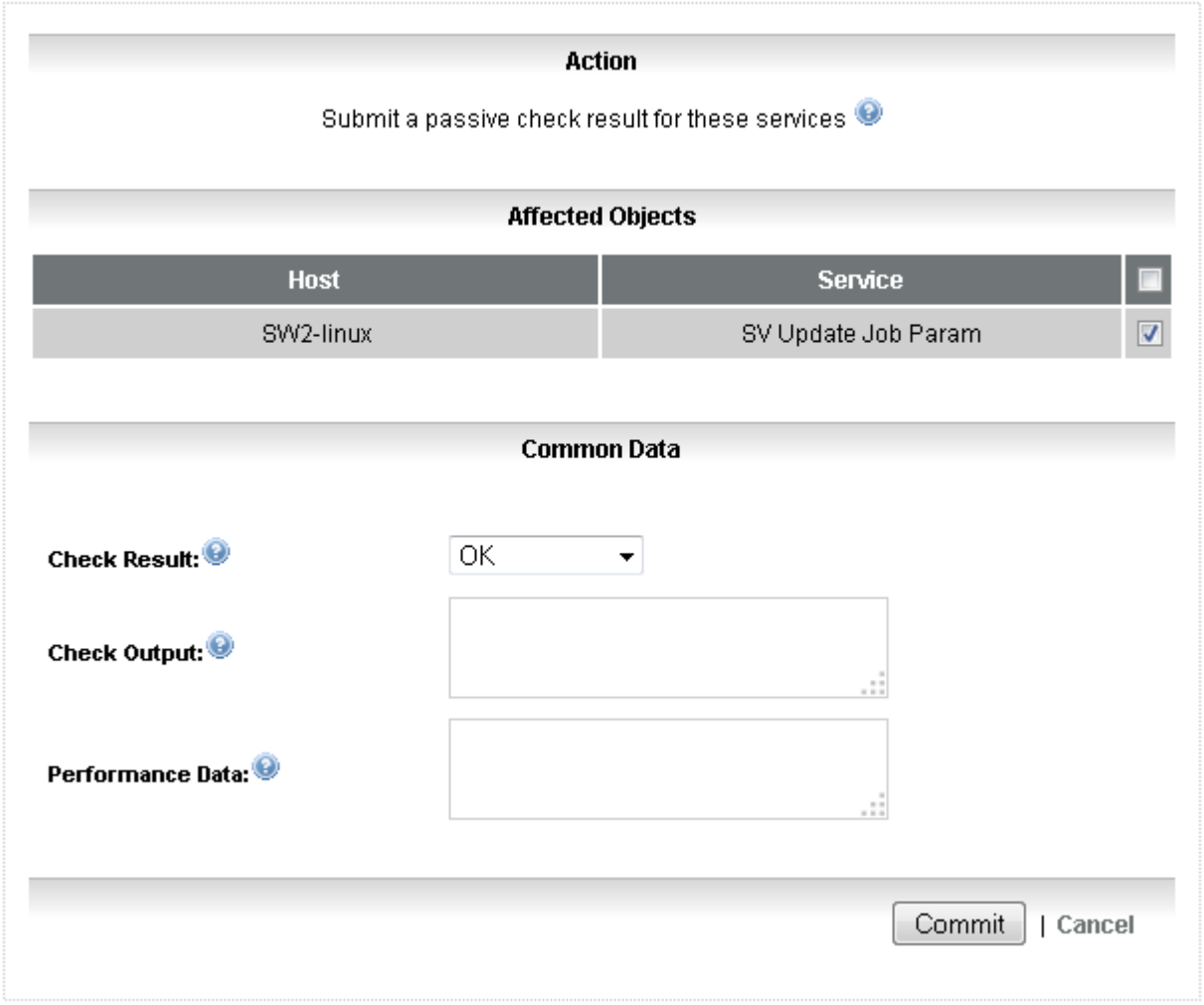
Select the passive service

At the beginning these passive services have no "Pending" status.

Below is an Icinga sample showing how to submit result data to a passive service. Select the corresponding service command.



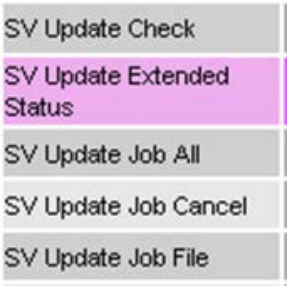
Enter the file name (fully qualified) as "Check Output" and use "Commit".



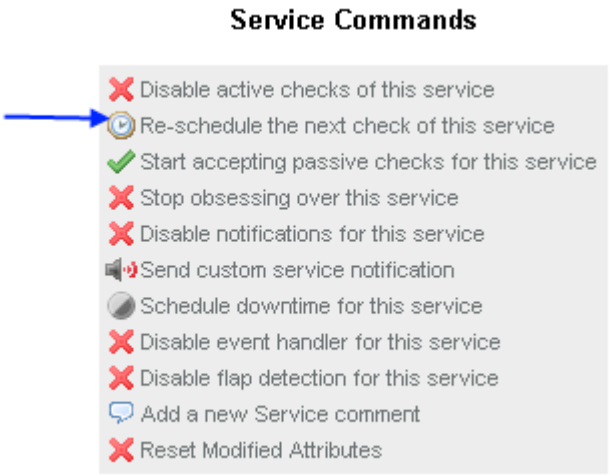
The entered string will appear as "result" after the next refresh of the service data.

10.1.8.4 Starting Update Actions - How to Start Unscheduled Nagios Services

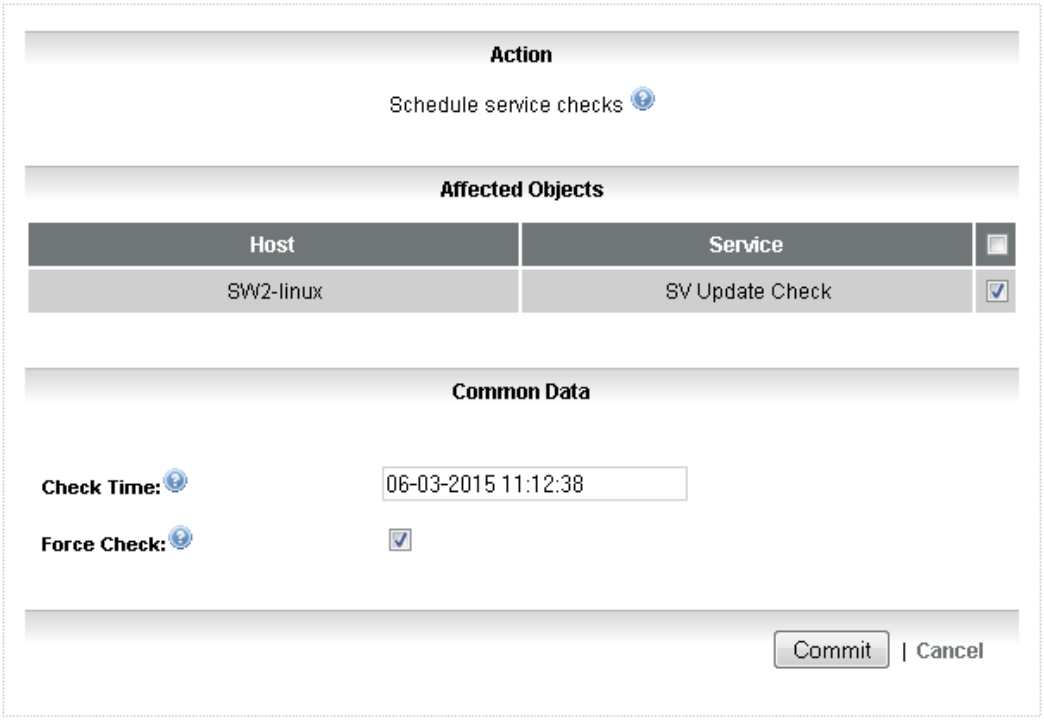
Select an unscheduled service - here SV Update Check, SV Update Job All, SV Update Job File or SV Update Job Cancel.



Force a call of this service:



Select the start time of the action in the new dialog and use "Commit" to start this Nagios service.



10.1.8.5 Command Definition

```
define command {
        command_name            check_fujitsu_server_update_CIM
        command_line            $USER1$/updmanag_fujitsu_server_CIM.pl -H
$HOSTADDRESS$ $_HOSTSV_CIM_OPTIONS$ $ARG1$
        register                1
}
```

$USER1$ is set to the plugin directory path (see resources.cfg of the Nagios scheduler)

10.1.8.6 Hostgroup Definition

```
define hostgroup {
        hostgroup_name          primergy-update-manage-servers-CIM
        alias                   Fujitsu Servers - Update Management (CIM)
        register                1
}
```

NOTE: In the sample config files, this host group is not added to the overall CIM or Fujitsu host group definitions. Add it if this hostgroup is assigned to at least one host.

10.1.8.7 Service Definition

In the following it is expected that the **generic-service** template is predefined and the timeout period is **none**.

```
define service {
        hostgroup_name          primergy-update-manage-servers-CIM
        service_description     SV Update Extended Status
        servicegroups           serverview
        use                     generic-service
        check_interval          60
        check_command           check_fujitsu_server_update_CIM
        flap_detection_enabled  0
        register                1
}

define service {
        hostgroup_name          primergy-update-manage-servers-CIM
        service_description     SV Update Check
        servicegroups           serverview
        use                     generic-service
        initial_state           u
        passive_checks_enabled  0
        check_command           check_fujitsu_server_update_CIM!--
startcheck
        active_checks_enabled   1
        passive_checks_enabled  0
        check_period            none
        register                1
}

define service {
        hostgroup_name          primergy-update-manage-servers-CIM
        service_description     SV Update Job File Param
        servicegroups           serverview
        use                     generic-service
        active_checks_enabled   0
        passive_checks_enabled  1
        initial_state           u
        check_period            none
        check_command           check_fujitsu_server_update_CIM
        flap_detection_enabled  0
```

```
        register                1
}

define service {
        hostgroup_name          primergy-update-manage-servers-CIM
        service_description     SV Update Job All
        servicegroups           serverview
        use                     generic-service
        passive_checks_enabled  0
        initial_state           u
        check_period            none
        check_command           check_fujitsu_server_update_CIM!--
startjoball
        register                1
}

define service {
        hostgroup_name          primergy-update-manage-servers-CIM
        service_description     SV Update Job File
        servicegroups           serverview
        use                     generic-service
        passive_checks_enabled  0
        initial_state           u
        check_period            none
        check_command           check_fujitsu_server_update_CIM!--
startjob=$SERVICEOUTPUT::SV Update Job File$
        register                1
}

define service {
        hostgroup_name          primergy-update-manage-servers-CIM
        service_description     SV Update Job Cancel
        servicegroups           serverview
        use                     generic-service
        passive_checks_enabled  0
        initial_state           u
        check_period            none
        check_command           check_fujitsu_server_update_CIM!--
canceljob
        register                1
}
```

11 Fujitsu SNMP Trap Configuration Files

The status change of a host is only seen when the Nagios scheduler calls the corresponding Nagios Plugin. An additional notification chain could be started only with receiving SNMP traps.

11.1 Standards

snmptrapd is a listener for receiving SNMP traps in LINUX. This program supports configurable follow-up actions. One of these actions could be a tool named **snmptt.**

The trap data received via snmptrapd includes:

- Sender IP Address
  ATTENTION: This is not the origin of the trap if forwarded traps are received!
- Timestamp information
- Trap SNMP OID
- One Origin Hostname
- Optional Trap Arguments
- One Origin IP Address

Severity and message texts are no part of this.

snmptrapd enables **the first opportunity** for notifications, storage and filtering.

snmptt enables **the second opportunity** for notifications, storage and filtering if triggered by snmptrapd.

ATTENTION:

There is a particular problem around sent IP addresses and host names:

- The sender IP address is one of multiple potential IP addresses of the sender and this is NOT the IP address of the origin of traps in the case of forwarded traps! Even if origin and sender are identical the IP addresses might differ!
- The host name is one of multiple potential host names of the originator
- The origin IP address is one of multiple potential IP addresses of the sender – this might even be a link-local address!

Because of this, the association of sent address information with a Nagios "host" is a problem that can only be solved by the administrators of each Nagios system.

11.2 Plugin Support

With the ServerView Nagios Plugin, configuration files in two formats will be supported.

- One is in a separate format – easy to scan for tools written by any user and usable by user-specific snmptrapd handlers
- The second is the **snmptt** format usable as-is for snmptt configurations and extendable for snmptt EXEC directives

These configuration files contain information for associating the SNMP OID with regard to severities and texts, and how to insert the sent arguments into texts!

Path:

fujitsu/ServerViewSuite/nagios/trap

Subdirectories:

- **trapconf** (own format)
- **snmpttconf** (snmptt format)

11.3 Helpful Hints around SNMPTT

URL: http://www.snmptt.org/

Suggested snmptrap.conf configuration:

```
traphandle default /usr/local/sbin/snmptt
```

The traps can be stored in an snmptt database which might be interpreted by already implemented Nagios Plugins and other user interfaces.

A "How-To" description for snmptt is available at http://www.snmptt.org/docs/snmptt.shtml .

NOTE ON IP AND HOST NAME:

snmptt expects the host name specified for Nagios to be identical with the one that snmptrapd can compute for the sender IP address!

ATTENTION: This does not work for forwarded traps!

Integration of snmptt configuration files:

Quote on snmptt main configuration from the above mentioned "How-To" description:

"

Add the file names to the snmptt_conf_files section in the snmptt.ini file.

For example:

snmptt_conf_files = <<END
/etc/snmp/snmptt.conf.generic
/etc/snmp/snmptt.conf.compaq
/etc/snmp/snmptt.conf.cisco
/etc/snmp/snmptt.conf.hp
/etc/snmp/snmptt.conf.3com
END

"

12 Fujitsu ServerView CIM Indications

Similar to SNMP traps, the ServerView CIM Provider might send so-called "CIM indications". This chapter explains how to subscribe to these indications and how to receive and them.

Within the FUJITSU Server Plug-ins is a directory named "cimindication" with tools for this.

Since CIM indications should be handled parallel to SNMP traps in the Nagios environment, these indications will be converted into special "SNMP traps" and **snmptt** (default) will be used for further administration abilities.

There are three supported functionalities:

- One "Listener" to receive ServerView CIM indications and convert them into SNMP traps. This listener is a similar listener to **snmptrapd'**
- Subscribe, list or unsubscribe from the local "Listener" into a server node (to be monitored) to receive ServerView CIM indications
- Special SNMP Trap Indication configuration files

ATTENTION: The subscription tool requires the CIM provider of ServerView Agent 7.10.18 (or higher) for Windows. For Linux and ESXi, V7.20 is the minimum version.

12.1 Receiving ServerView CIM Indications - Listener

Directory: **cimindication/listener**

12.1.1 Listener Requirements

The listener daemon is a Perl script. It uses several Perl classes which must be available on the system.

Requirements:

- perl-IO-Socket-INET6
- perl-NetAddr-IP
- perl-IO-Socket-SSL
- perl-Net-SSLeay
- perl-XML-Twig
- perl-Time-HiRes
- SNMP Trap Handler - Default "snmptt"

ATTENTION:

Some distributions supply older versions of the perl-Net-SSLeay module, which was not thread-safe up to version 1.43. Having these versions will cause the listener to fail when using SSL connections. To fix this, you should update Net::SSLeay to a more recent version using your distribution package manager, or from CPAN.

Version 1.58 (the latest at the time of this writing) was used for tests.

12.1.2 Security

The listener uses port 3169 (default) to receive SSL and Non-SSL requests.

Whether or not "http" or "https" can be used or subscribed depends on the indication-sending service.

FUJITSU ServerView Plug-ins contain a simple server certificate "server.crt" without any host name or host address references. This can be replaced by customer specific certificates as long as they are in PEM format and allow the processing of requests.

The path of the certificate can be specified in the central configuration file of the listener.

The archive also contains a file named "cacert.crt", which might be distributed to indication-sending services for verifications of "server.crt" if needed.

12.1.3 Stabilization / Availability

The listener is based on Perl module IO::SOCKET or IO::SOCKET::SSL. The stability is based on these modules.

The signals INT and TERM are redirected to finalize the listener.

12.1.4 Central Configuration of the Listener

The listener searches for /etc/<listenername>.conf by default.

In this central configuration file are several defaults which can be changed if necessary. In the configuration file are comments for each entry.

12.1.4.1 Address and Port Usage

- ADDRESS
  The default is ::, meaning any IPv4 and any IPv6 address
- If IPv6 is prohibited in a system, add 0.0.0.0 for "any IPv4" address. If the listener is only to listen for one address, add this address into this configuration
- PORT
  The default is 3169 (IANA reserved for ServerView services)

  If ServerView Operations Manager is installed on the same system, this port number must be changed!

  ATTENTION: A changed port number must be used as the parameter for subscriptions.

12.1.4.2 Debug Logging

The listener writes "events" into central /var/log/messages. By default, only start and end logs are stored in /var/log/fujitsu/svcimlistener/<listnername>.log.

If a problem occurs and is reproducible, it might be helpful to set DEBUG_LEVEL and send the resulting files along with an error report.

12.1.4.3 SSL Settings

Here are the central configuration keys to enable SSL and set certificate file parameters:

- VERIFY_SSL 1 - enable SSL (parallel to Non-SSL)
- SSL_CERT [SSL_KEY]
  Default: /etc/svcimlistenerd/server.crt

  This might be replaced with customer or host-specific certificates.
- SSL_PASSWD
  Unset as default. server.crt does not need a password.

  This must be specified if server.crt is not used and the new certificate needs a password for use.

  ATTENTION: If a password is added, make sure the configuration file is only readable for the listener process and the administrator.
- CA_PATH
  Default: /etc/ssl/certs

12.1.4.4 SSL Settings for Experts

There are some SSL parameters around IO::SOCKET::SSL which can be specified in the central configuration.

Be aware that these might affect the communication ability. Therefore this is for experts only - see descriptions for above-named Perl class.

- SSL_PROTOCOL
  See "SSL_version" parameter
- SSL_CIPHERS
  See "SSL_cipher_list" parameter
- SSL_DH_FILE
  See "SSL_dh_file" parameter"

ATTENTION:

The SSL_PROTOCOL setting depends very much on the ability of the installed IO::SOCKET::SSL version!

The parameter defaults depend on the IO::SOCKET::SSL version!

Here is a link to the latest SSL.pm description (as at 2015 - the address might change in the future):
http://search.cpan.org/~sullr/IO-Socket-SSL/

12.1.4.5 SNMP Trap Handler - SNMPTT

Check the path in SNMPTT_EXE for the usage of SNMPTT.

Add an alternative trap handler if an alternative handler is to be used instead.

12.1.5 Install Script

The listener installation helper shell script “sv_install.sh” is intended for an installation on RHEL-like distributions. For other distributions this script can be modified by Nagios administrators.

12.1.5.1 Basic functions

- Check for appropriate user permission
- Check for an existing ServerView Operations Manager installation that also uses the default port 3169
- Check prerequisites (Perl classes and SNMP Trap Handler) as already described above
- Copy the necessary files to default locations. For detailed information see:
  - sv_install.sh script
    section: “svcimlistenerd default installation settings”
  - svcimlistenerd.conf
- Configure the listener daemon to be started at system boot time and stopped at the beginning of shutdown
- Start the listener after installation
- Provide log files. The default location is “/var/log/fujitsu/svcimlistener”

12.1.5.2 Options

-h|--help
Print help text.

-e|--erase|--uninstall
Start daemon unregistration and uninstallation.

-n|--noprereq
Do not check for prerequisites.

-s|--silent

Allow an unattended installation. Use -s and -n to omit any interactive questions.

12.1.6 Starter Script

The listener daemons starter script “sv_cimlistenerd” is written for RHEL-like distributions. For other distributions this script can be modified by Nagios administrators.

If the listener installation has been performed with the helper script “sv_install.sh”, then:

- The listener daemon can be maintained by the starter script.
- The starter script can be used in the following manner:
  - service sv_cimlistenerd “option”
  - /etc/init_d/sv_cimlistenerd “option”

12.1.6.1 Options

status
Displays the listener status, e.g:
Checking status of CIM listener daemon (pid 14786) : running.

start
Starts listener daemon

stop
Stops listener daemon

restart
Stops and then starts listener daemon

A check for appropriate user permission is done before execution of “start, stop and restart”.

12.2 Subscriptions to Receive ServerView CIM Indications

The listener will only get CIM indications if the address (URL) of the listener is "subscribed" to the CIM Service that sends indications.

Within FUJITSU ServerView Plug-ins is a tool to subscribe, unsubscribe and list all ServerView CIM indication subscriptions (sometimes also called "Registrations").

ATTENTION: This feature is currently only available "in-band" and is based on the CIM provider of ServerView Agent 7.10.18 (or higher) for Linux and Windows and CIM Provider 7.20.01 (or higher) for ESXi.

12.2.1 Script Name

Name of the script
subscribe/svindication_subscribe.pl

This is a Perl script which uses wbemcli or fujitsu_server_wsman.pl calls.

It is a script to manage all features around ServerView CIM indication subscriptions.

12.2.2 Requirements for wbemcli or OpenWSMan

This is the same as described for Upate Management, see chapter link "Requirements for wbemcli or OpenWSMan".

12.2.3 Add - Subscribe to ServerView CIM Indications

Option:

--add=<listenerhost> [--listport=<listenerport>] [--listttransport=<listenertype>]

For subscriptions the remote CIM service needs an address for contacting the listener.

The address might be an IP address or a DNS (FQDN) name.

ATTENTION: This address must be resolvable by the remote server!

A URL will be built from <listenertype>://<listenerhost>:<listenerport>.

Default listener type is "https".

Default listener port is 3169.

The script returns "OK - Successful registration" on success.

A "Tag" name will be built for this subscription to identify it in the list of subscriptions. The name is built from "SvNagios-<listenerhost>-<listenerport>".

12.2.4 List - List all Subscriptions to ServerView CIM Indications

Option:

[--list]

The "list" action will be called if the script is called without the action options --add or --remove. Option --list is the default action.

For each registration the "Tag" name and a filter name will be printed.

With verbose level 2 the full handle is printed. This is a complex multi-quoted stream. It is the registration handle of the WS-Eventing standard. The syntax and contents depend on the operating system type and CIM service of the server to be monitored.

Sample output:

```
OK

Registration[0] - Tag=BLTest5 FilterName="SVS:Filter#TBLTest5T#_11"
ListenerURL="…"

Registration[1] - Tag=BLTest5 FilterName="SVS:Filter#TBLTest5T#_12"
ListenerURL="…"

Registration[2] - Tag=SvNagios-nnn.nnn.nnn.nnn-3169
FilterName="SVS:Filter#TSvNagios-nnn.nnn.nnn.nnn-3169T#_13"
ListenerURL="https://nnn.nnn.nnn.nnn:3169"
```

12.2.5 Remove - Unsubscribe from ServerView CIM Indications

Option:

--remove=<listenerhost> [--listport=<listenerport>]

Removes a subscription using the tag name "SvNagios-<listenerhost>-<listenerport>"

The default listener port is 3169.

12.3 About SNMP Trap Configurations for CIM Indications

The listener transforms ServerView "logMessage" indications into traps. The archive (tgz) contains an snmptt configuration file to handle these indication traps.

Directory: **cimindication/snmptt/**

ATTENTION:

In the indications is a "host address" showing which server is the origin of the indication. This might be an FQDN or other host name or, if no host name is available, an IP address.

This address is added to the indication trap

Snmptt-Nagios Plug-ins expect the host name specified for Nagios to be identical with the one that is part of the trap!

The chapter on SNMP Traps explains how to integrate snmptt configuration files for snmptt usage. For more about this, see chapter link "Helpful Hints around SNMPTT".