Dell OpenManage Plug-in Version 1.0 for Nagios Core
User's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your computer.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

2015- 01

Rev. A00

Contents

1

Introduction to Dell OpenManage Plug-in Version 1.0 for Nagios Core

This guide provides information about using the Dell OpenManage Plug-in Version 1.0 for Nagios Core and its various features such as discovering, monitoring, launching consoles, and troubleshooting of the supported Dell devices. The guide also provides details of the supported Dell devices and frequently asked questions by the customer.

The Dell OpenManage Plug-in Version 1.0 for Nagios Core provides capabilities to monitor 12th and later generations of Dell PowerEdge servers in the data center through an agent-free, out-of-band method using Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller (LC).

This plug-in provides features as mentioned in Table 1.

Table 1. Key features

Feature	Functionality
Device Discovery	Discovers 12th and later generations of Dell PowerEdge servers through iDRAC with LC using the agent-free method of monitoring. Once the discovery is complete, host and service definitions are created for each device. You can opt for either SNMP or WS-MAN protocol for device discovery based on your requirement.
Device Information	Displays information about the discovered device (service tag, server model, iDRAC firmware version, hostname, operating system name, operating system version, and so on) and its components (Fully Qualified Device Descriptor, and so on) after a device discovery is successful. You can view this information in the **Hosts** or the **Services** view in the Nagios Core console. For more information about the device information provided by the Plug-in, see Device Information.
Monitor overall health of Dell devices	Monitors the overall health of Dell devices in a scheduled or periodic manner.
Component level health of Dell devices	Monitors the health of server components (physical drives, virtual drives, fans, battery, server intrusion status, server network device status, and so on) and displays information about the Dell device component status at scheduled time intervals.
Monitor SNMP alerts	Monitors SNMP alerts for Dell devices. This feature displays only the last received SNMP alert.

Feature	Functionality
Launching iDRAC console	Launches the respective iDRAC console to further troubleshoot and manage the supported Dell devices.

2

Support matrix

Dell OpenManage Plug-in for Nagios Core supports the Dell devices listed in the following table.

Dell PowerEdge Servers

NOTE: In the PowerEdge server name format yxxx; y denotes alphabets, where M denotes Modular, R denotes Rack, T denotes Tower, and x denotes numbers.

yx2x Systems	yx3x Systems
PowerEdge M820	PowerEdge M630
PowerEdge M620	PowerEdge R730XD
PowerEdge M520	PowerEdge R730
PowerEdge M420	PowerEdge R630
PowerEdge R920	PowerEdge R530
PowerEdge R820	PowerEdge R430
PowerEdge R720xd	PowerEdge T630
PowerEdge R620	PowerEdge T430
PowerEdge R520	PowerEdge FC630
PowerEdge R420	
PowerEdge R320	
PowerEdge R220	
PowerEdge T620	
PowerEdge T420	
PowerEdge T320	
PowerEdge FM120x4	

3

Device Discovery and Inventory

About Device Discovery

You can discover 12th and later generations of Dell PowerEdge servers with the Plug-in using agent-free method of discovery. You can opt for SNMP or WS-MAN protocol.

At a time you can only discover a particular Dell device using SNMP or WS-MAN protocol and not both.

You must use **Dell Device Discovery Utility** to discover Dell devices. If the discovery is successful, then for the discovered devices, host and service definition files are created. For a device, it is recommended to have a unique host name and IP address. In Nagios Core, ensure that a host and service definition is not already present for a server that you want to discover.

You can discover devices using any of the following:

- Device's IP address or FQDN
- Subnet with mask
- File containing a list of device IP addresses or FQDNs

About Dell Device Discovery Utility

To run the **Dell Device Discovery Utility**; From the location: `<NAGIOS_HOME>/dell/scripts`, you must run the following PERL script:

```
perl dell_agent_free_server_discovery.pl
```

`<NAGIOS_HOME>` is the installed location of Nagios Core and by default, the location of `<NAGIOS_HOME>` is `/usr/local/nagios`.

When you run the PERL script, the following options are provided:

```
perl dell_oob_server_discovery.pl -H <host or IP Address> | -F <Ip Address list
file> | -S <subnet with mask> -P <protocol> [-c <protocol specific config file>]
[-t <service template file>] [-f] [-d]
```

Table 2. Dell Device Discovery Utility options

Options	Short Description	Description
`-h`	help	Use to view information about options.
`-H`	host	Use to input IP address or fully qualified domain name (FQDN) of the host device.
`-S`	subnet	Use to input subnet with mask.
`-F`	file	Use to input filename with absolute path. The file must contain a list of IP addresses or FQDN of host devices separated by a new line.
`-P`	protocol	Option for SNMP or WS-MAN protocol.
`-c`	configuration file	Use to configure protocol parameters. The default file is `.dell_device_comm_params.cfg`. For more information see About Protocol Parameters.
`-t`	template	Use to specify the services template file with absolute path. The default file is `dell_server_services_template.cfg`
`-f`	force	Use to overwrite an existing host configuration file.
`-d`	all services	Use to monitor all the services. If you run the utility without this option, then the basic three services are created. For more information, see **Table 3. Default services created based on selected protocol**.

Based on the options you selected during discovery, the following services are run:

- If you run `perl dell_agent_free_server_discovery.pl` without the `-d` option, then the following services are created by default and displayed in the user interface under **Services**:
  - Dell Server Information
  - Dell Server Overall Health Status
  - Dell Server Traps
- If you run `perl dell_agent_free_server_discovery.pl` with the `-d` option, depending on the protocol you selected, the following services are created by default and are displayed in the user interface under **Services**:

Table 3. Default services created based on selected protocol

Services	SNMP	WS-MAN Protocol
Basic Services		
Dell Server Overall Health Status	√	√
Dell Server Information	√	√
Dell Server Traps (If SNMPTT integration is configured for Dell plug-in.)	√	√
Detailed Services		
Dell Server Physical Disk Status	√	√
Dell Server Virtual Disk Status	√	√
Dell Server Fan Status	√	√
Dell Server Battery Status	√	√
Dell Server Intrusion Status	√	√
Dell Server Network Device Status	√	√
Dell Server CPU Status	√	X
Dell Server Power Supply Status	√	X
Dell Server Temperature Probe Status	√	X
Dell Server Voltage Probe Status	√	X
Dell Server Controller Status	√	X
Dell Server Amperage Status	√	X
Dell Server SD Card Status	X	√

About Protocol Parameters

During discovery, depending on the protocol you have selected, SNMP or WS-MAN, you can set values for the protocol in the parameters file, `.dell_device_comm_params.cfg`.

The `.dell_device_comm_params.cfg` file is present at the following location:**<NAGIOS_HOME>/dell/scripts**. The options provided are:

Table 4. Parameters File

Protocol Communication Parameters	Description
SNMP	
snmp.version	Use to input the SNMP version. Default version is 2.
snmp.community	Use to input the user macro for SNMP community string.
snmp.retries	Use to input the number of times an SNMP request must be sent when a timeout occurs . Default retry value is 1.
snmp.timeout	Use to input SNMP timeout value in seconds. Default timeout value is 3 seconds.
snmp.port	Use to input the SNMP port value. Default SNMP port value is 161.
WS-MAN	
wsman.username	Use to input the user macro for WS-MAN service account user name.
wsman.password	Use to input the user macro for WS-MAN service account password.
wsman.port	Use to input the WS-MAN port value. Default value is 443.
wsman.timeout	Use to input WS-MAN timeout value in seconds. Default timeout value is 60 seconds.
wsman.retries	Use to input the number of times a WS-MAN request must be sent when a timeout occurs. Default retry value is 2.

NOTE:
You can configure the user macros, snmp.community, wsman.username, and wsman.password in the file dell_resources.cfg available at the location: **<Nagios_Home>/dell/resources/**.

Discovering Dell Servers

You can discover 12th and later generations of Dell PowerEdge servers using Dell plug-in.

Prerequisites:

- If you are using SNMP protocol for discovery, ensure that SNMP version 1 or SNMP version 2c are enabled, community string is set and configured in iDRAC. For more information see Appendix.
- A secured network connectivity is established between Nagios Core and the iDRAC with LC.
- (Recommended) An iDRAC device must have a resolvable FQDN.
- If you are using WS-MAN protocol, it is recommended that you use a WS-MAN service account other than the default service account for WS-MAN communication.

To discover Dell servers:

1. Log in to Nagios Core with Nagios administrator privileges.
2. Navigate to the directory `<NAGIOS_HOME>/dell/scripts`.
3. Run the Dell Server Discovery Utility with options: `perl dell_agent_free_server_discovery.pl` or `perl dell_agent_free_server_discovery.pl -h`

   The script syntax and information on options are displayed. For more information see About Dell Discovery Utility.

   Based on your requirement do the following:

   NOTE: Before running the utility, ensure that you have updated protocol related information, for more information see About Protocol Parameters.

   To discover a device using an IP address or FQDN:

   - `perl dell_agent_free_server_discovery.pl -H <IP address or FQDN name> -P <protocol>`

   To discover using subnet with mask:

   - `perl dell_agent_free_server_discovery.pl -S <subnet with mask> -P <protocol>`

     An example format for subnet with mask: 11.98.149.0/24

   To do discover using a list of IP addresses present in a file:

   - `perl dell_agent_free_server_discovery.pl -F <Ip Address list file> –P <protocol>`
   - For the `-P` option, Opt for a protocol:
     - For SNMP, the value is 1.
     - For WS-MAN, the value is 2.
4. Once the discovery utility script is run, verify the Nagios configuration by running the command `<NAGIOS_HOME>/bin/nagios -v /usr/local/nagios/etc/nagios.cfg`.
5. Ensure that no errors are present and then restart Nagios Core by running the command `service nagios restart`.
6. You can view the logged information in the Log file path: `<NAGIOS_HOME>/var/dell/discovery_<yyyymmddhhmiss>.dbg.`.

   In the filename, `<yyyymmddhhmiss>` pertains to the time when the log information was gathered; `yyyy` is the calendar year, `mm` is month, `dd` is date, `hh` is hour of the day, `mi` is minutes, and `ss` is seconds.

After Completion of Discovery:

- Dell server Host definition and its service definitions are created in the Nagios server and this is subsequently used for monitoring the Dell servers.

  The discovered Dell servers and its services are displayed in the **Host** view and the **Services** view in the Nagios console. Wait for the scheduled service to complete for the service details to be displayed.

- The discovered Dell servers are displayed in the **Map** view in the Nagios Core console.

Device Information

About Device Information

The dell server information service provides the basic information about the system. By default this service is polled once a day.

Table 5. Device Information

Service	Status	Description	Attributes Displayed when using SNMP or WS-MAN
Dell Server Information	The following states are possible: • **OK** • **Unknown** • **Critical**	This service provides the basic device inventory information. **NOTE:** Chassis Tag is applicable only for modular servers and Node ID is applicable only for PowerEdge FC120x4	• Server Host FQDN • Model Name • Device Type (iDRAC7 or iDRAC8) • Service Tag • Product Type (monolithic or modular) • Chassis Tag • iDRAC Firmware Version • OS Name • OS Version • Console URL This is iDRAC web console URL. • Node Id

For attributes information on various components, see About Monitoring Component Health of Dell Devices.

Viewing Device Information

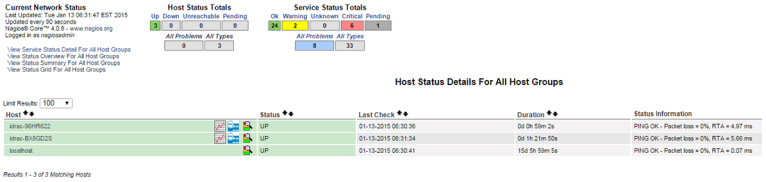
To view the information on devices once the **Dell Server Information** service is run:

In Nagios Core console, under **Current Status**, select **Services**.

Viewing Dell Devices in the Nagios Core Console

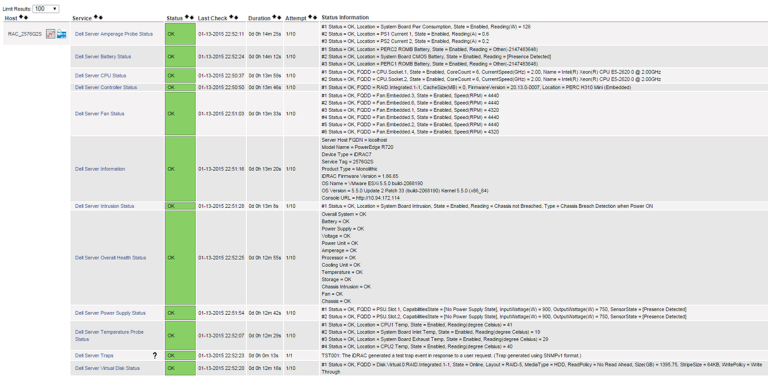
Prerequisites: The Dell devices are discovered and inventoried in Nagios Core.
You can view the discovered Dell devices in Nagios Core in the **Hosts** or the **Services** view:

1. To view the hosts in the Nagios Core, select **Hosts** under **Current Status**.
   The hosts are displayed in the right pane.



2. To view the services associated with the hosts in the Nagios Core, select **Services** under **Current Status**.

   The services are displayed in the right pane.



4

Monitor Dell Devices

Yon can monitor the following aspects of Dell devices.

Overall Health

You can monitor the Dell devices for their overall health status.

About Overall Health

Overall health status is an aggregate status of the components of the Dell devices.

Overall health status of a device is polled periodically based on the configured interval. By default, the **Dell Server Overall Health Status** service is scheduled once an hour.

Table 6. Overall Health Information

Service	Status	Description	Attributes Displayed when using WS-MAN	Attributes Displayed when using SNMP
Dell Server Overall Health Status	The following states are possible: • **OK** • **Warning** • **Unknown** • **Critical**	Provides global health status of Dell servers.	• Overall System • Battery • Memory • Voltage • Storage • Power Supply • Fan	• Overall System • Dell Internal Dual SD Module (IDSDM) Card Unit • Battery • Power Supply • Secure Digital (SD) Card Device • SD Card Unit • Cooling Unit • Fan • Chassis • IDSDM Card Device • Amperage • Power Unit • Voltage • Processor • Temperature

Service	Status	Description	Attributes Displayed when using WS-MAN	Attributes Displayed when using SNMP
				• Chassis Intrusion • Storage

NOTE: Status of Storage attribute is representative of cumulative health status of storage components like physical disk, virtual disk, controller, and so on.

Viewing Overall Health

Before you monitor the health of the discovered Dell devices in your data center environment, ensure that the discovered devices are reachable.

To view the overall health of Dell devices:

1. In Nagios Core user interface, under **Current Status**, select **Services**.
2. Select the associated service to view the overall health status.

   Health polling of servers is done through iDRAC with LC and the corresponding objects are shown in their respective health service with proper severity health color.

Monitor Component Health of Dell Devices

You can monitor the health of individual components in the Dell servers.

About Monitoring Component Health of Dell Devices

This is periodic poll based health monitoring of the Dell servers' component level health status.

Once the discovery utility is run with the relevant option, the corresponding services are created. These services run periodically and update the overall health of the components. The component's status and information are displayed in the Nagios Core user interface.

The format of the component information in the Status Information column is `<Attribute>=<Value>[, <Attribute>=<Value>]`.

For example: `Status=CRITICAL, FQDD=Fan.Embedded.1, State=Enabled`

Table 7. Component health information

Service	Status	Description	Attributes Displayed when using WS-MAN	Attributes Displayed when using SNMP
Dell Server Physical Disk Status	The following states are possible: • **OK** • **Warning** • **Unknown** • **Critical**	Provides worst case health status of the physical disks in Dell servers.	• Status • Fully Qualified Device Descriptor (FQDD) • State • Product ID • Serial No	• Status • FQDD • State • Product ID • Serial No • Size (GB) • Media Type

Service	Status	Description	Attributes Displayed when using WS-MAN	Attributes Displayed when using SNMP
			• Size (GB) • FirmwareVersion • Media Type • FreeSpace (GB)	• FreeSpace (GB) • FirmwareVersion
Dell Server Virtual Disk Status		Provides worst case health status of the virtual disks in Dell servers.	• Status • FQDD • State • Size (GB) • WritePolicy • ReadPolicy • Layout • StripeSize • Media Type	• Status • FQDD • State • Size (GB) • WritePolicy • ReadPolicy • Layout • StripeSize • Media Type
Dell Server Fan Status		Provides overall health status of the fans in Dell servers.	• Status • FQDD • State • Speed (RPM)	• Status • FQDD • State • Speed (RPM)
Dell Server Battery Status		Provides overall health status of the battery in Dell servers.	• Status • Location • State • Reading	• Status • Location • State • Reading
Dell Server Intrusion Status		Provides overall health status of the chassis intrusion in Dell servers.	• Status • Location • State • Reading	• Status • Location • State • Type • Reading
Dell Server Network Device Status		Provides worst case health status of the NIC in Dell servers.	• ConnectionStatus • FQDD • Name • FirmwareVersion • LinkSpeed	• ConnectionStatus • FQDD • Name
Dell Server CPU Status		Provides overall health status of the	Not Available	• Status • FQDD • State

Service	Status	Description	Attributes Displayed when using WS-MAN	Attributes Displayed when using SNMP
		CPUs in Dell servers.		• Name • CurrentSpeed (GHz) • CoreCount
Dell Server Power Supply Status		Provides overall health status of the power supply in Dell servers.	Not Available	• Status • FQDD • CapabilitiesState • OutputWattage (W) • InputWattage (W) • SensorState
Dell Server Temperature Probe Status		Provides overall health status of the temperature probe in Dell servers.	Not Available	• Status • Location • State • Reading (degree Celsius) • Reading
Dell Server Voltage Probe Status		Provides overall health status of the voltage probe in Dell servers.	Not Available	• Status • Location • State • Reading (V) • Reading
Dell Server Controller Status		Provides worst case health status of the storage controllers in Dell servers.	Not Available	• Status • FQDD • Location • FirmwareVersion • CacheSize (MB)
Dell Server Amperage Probe Status		Provides overall health status of the amperage probe in Dell servers.	Not Available	• Status • Location • State • Reading (A) or Reading (W)
Dell Server SD Card Status		Provides overall health status of the	• Status • FQDD • State • WriteProtected	Not Available

Service	Status	Description	Attributes Displayed when using WS-MAN	Attributes Displayed when using SNMP
		SD card in Dell servers.	• InitializedState • Size (GB) • AvailableSpace (GB)	

NOTE: Nagios console displays a component's status as CRITICAL in the Status Information column when the actual status is Unknown.

NOTE:

Unit	Description
GHz	Giga Hertz
W	Watt
GB	Giga Byte
RPM	Revolutions Per Minute
A	Ampere
V	Volts
MB	Mega Bytes

By default, the preceding services are scheduled once every four hours.

Monitoring Health of Dell Devices

To monitor the health of Dell devices:

1. In Nagios Core user interface, under **Current Status**, select **Services**.
2. Select the associated service to monitor the health of Dell devices.
   Health monitoring of servers is performed through iDRAC with LC and corresponding details are shown in their respective component health service with proper severity health color.

Monitor SNMP Alerts

About SNMP Alert Monitoring

You can asynchronously receive the SNMP alerts forwarded from the devices.

Once an SNMP alert is received, the **Dell Server Traps** service will display the alert summary message and alert severity in the Nagios Core console.

Table 8. Server Trap Information

Service	Status	Description
Dell Server Traps	The following states are possible: • **OK** • **Warning** • **Unknown** • **Critical**	Provides trap Information of the Dell server raised through agent-free method. Displays the last received SNMP alert. To view all the SNMP alerts that were received, select **Reports → Alerts → History**.

Viewing SNMP Alerts

Prerequisites:

- Nagios Core with SNMPTT is installed and configured and the Dell integration on SNMPTT is configured.
- SNMP Trap destination is configured with Nagios Core server in iDRAC.

  For information on configuring SNMP Trap destination in the iDRAC interface, see Appendix.

To view SNMP alerts:

In Nagios Core user interface, under **Current Status**, select service **Dell Server Traps**.

The SNMP alerts are displayed in the status information, and the severity of the alert is updated in the status.

5

Launching iDRAC Web Console

To launch console for an iDRAC device:

1. In Nagios Core console, under **Current Status**, select any of the following:
   - **Hosts**
   - **Services**
   - **Host Groups → Dell Agent-Free Servers**
2. Click  (**Perform Extra Host Actions** icon) adjacent to the Dell device.

6

Removing Dell Devices

You can remove a Dell device that you do not want to monitor.

1. Navigate to `<NAGIOS_HOME>/dell/config/objects`, and delete the corresponding `<IP OR FQDN>.cfg` file.
2. For completing the removal of the Dell device, restart the Nagios Core services by running the command: `service nagios restart`.

7

Troubleshooting

This section lists the problems that you may encounter while using the Dell OpenManage Plug-in Version 1.0 for Nagios Core and their workarounds.

Ensure that you meet the requirements, or perform the steps listed in this section.

The Dell OpenManage Plug-in for Nagios Core installation script is failing

1. You have adequate permissions to run the script.
   Recommended: Nagios Administrator.
2. The prerequisites as mentioned in the Installation Guide are met.
3. You have provided correct inputs to the installation script.

The Dell OpenManage Plug-in for Nagios Core uninstallation script is failing

1. You have adequate permissions to run the script.
   Recommended: Nagios Administrator.
2. The uninstallation script is running from the location where the Dell OpenManage Plug-in is installed.

The discovery script is failing to execute

1. The discovery script has appropriate permissions.
   Recommended: Nagios Administrator.
2. The appropriate arguments are provided while running the script.

The discovery script is not creating the host and service definition file for IPv4 or IPv6 addresses or hosts when the protocol selected is 1 (SNMP)

1. Net-SNMP is installed.
2. The IP addresses or hosts are reachable.
3. SNMP is enabled on the given IP addresses or hosts.

4. The appropriate protocol credentials are correctly configured in the following files before running a discovery:

   `dell_resource.cfg`

   `.dell_device_comm_params.cfg`
5. For an IPv6 address, ensure that the Perl Module Socket6 is installed in the same Perl library path.
6. At least one of the applicable service is enabled in the following service template:

   `dell_server_services_template.cfg`

   .

The discovery script is not creating the host and service definition file for IPv4 or IPv6 addresses or hosts when the protocol selected is 2 (WS-MAN)

1. OpenWSMAN and its perl binding are installed.
2. The IP addresses or hosts are reachable.
3. The appropriate protocol credentials are correctly configured in the following files before running a discovery:

   `dell_resource.cfg`

   `.dell_device_comm_params.cfg`
4. For an IPv6 address, ensure that the Perl Module Socket6 is installed in the same Perl library path.
5. At least one of the applicable service is enabled in the following service template:

   `dell_server_services_template.cfg`

   .

The Dell device's IP address or host name changes after discovery of the device

Remove the old configuration file and rediscover the Dell device using a new IP address or hostname.

The Nagios Core Console is not displaying the Dell devices that are discovered using the Dell discovery script

1. The host and service definition files exist in the **<NAGIOS_HOME>/dell/config/objects** folder.
2. The Nagios service has been restarted after running a discovery.
3. The host and service definition files have appropriate permissions.

The Nagios Core Console is not displaying the Trap Service for Dell devices that are discovered using the Dell discovery script

1. SNMPTT is installed.
2. If SNMPTT is not installed, then the trap service is not created for any of the discovered Dell device.

3. After you install SNMPTT, ensure that the Trap Integration is performed.

   To perform Trap Integration, from **<NAGIOS_HOME>/dell/install**, run the command:

   ```
   install.sh trap
   ```

4. Once the trap integration is complete, restart the SNMPTT service, run the command:
   ```
   service snmptt restart
   ```

The Dell OpenManage Plug-in specific services are displaying the message, “Error while creating SNMP Session”

1. The recommended versions of Net-SNMP and Net-IP are installed. If you are using IPv6, then the Perl module Socket6 should also be installed.
2. The IP addresses or hosts provided are reachable.
3. SNMP is enabled on the IP addresses or hosts.
4. The appropriate SNMP parameters are correctly configured in the following files:
   ```
   dell_resource.cfg
   ```
   ```
   .dell_device_comm_params.cfg
   ```

Dell OpenManage Plug-in specific services are displaying the message, “WSMAN Error while communicating with host”

1. OpenWSMAN and its perl binding and Net-IP are installed.
2. The IP addresses or hosts provided are reachable.
3. The appropriate WS-MAN parameters are correctly configured in the following files:
   ```
   dell_resource.cfg
   ```
   ```
   .dell_device_comm_params.cfg
   ```

Dell OpenManage Plug-in specific services are displaying the message, “Component Information = UNKNOWN”

NOTE: This is an expected message if the component is not available in the discovered Dell device.

If the component is available and you are still receiving the message, then this message is due to protocol time-out. Set the required protocol specific time-out values in the `.dell_device_comm_params.cfg` file.

Unable to view the SNMP alerts generated by the Dell device in the Nagios Core Console

1. Perform Trap Integration, from **<NAGIOS_HOME>/dell/install**, run the command:
   ```
   install.sh trap
   ```

2. The binary **<NAGIOS_HOME>/libexec/eventhandlers/submit_check_result** is present.
3. The trap configuration file `Dell_Agent_free_Server_Traps.conf` and the binary `submit_check_result` have appropriate permissions.

The Overall Health status is not getting refreshed after receiving a Dell device alert

If the Overall Health service is not created for a discovered Dell device, then the Dell device trap will not trigger an Overall health status. If Overall health service exists for a device, then ensure the following:

1. The file `<NAGIOS_HOME>/libexec/eventhandlers/submit_check_result` is present.
2. The trap configuration file `Dell_Agent_free_Server_Traps.conf` and the binary `submit_check_result` have appropriate permissions.
3. The SNMPTT process has appropriate permissions to run scripts in `<NAGIOS_HOME>/dell/scripts`.

Where do I find the OpenWSMAN distribution and its Perl binding?

If the system has default Perl version (installed as part of operating system), go to *build.opensuse.org/package/show/Openwsman/openwsman* and download the OpenWSMAN library and its Perl binding.

If you have installed a Perl version other than the default version, or the Perl binding is not available then go to *github.com/Openwsman/openwsman* and follow the instructions to compile and use.

8

Frequently Asked Questions

1. **Question:** Can you provide information on Licensing of Dell OpenManage Plug-in for Nagios Core?

   Answer: You can install and use this plug-in for free.

2. **Question:** What are the Dell hardware models supported by the plug-in?

   Answer: For the list of supported Dell platforms, see Support Matrix.

3. **Question:** I have earlier generation of servers (9th Generation – 11th Generation) in my data center. Can I still monitor them using the plug-in?

   Answer: No, you cannot monitor earlier generations of servers (9th Generation through 11th Generation) using this plug-in. You can only monitor Dell servers through iDRAC with LC, supported for 12th and later generations of Dell PowerEdge servers using this Plug-in. There are other plug-ins available on Nagios Exchange using which you can monitor earlier generation of servers.

4. **Question:** What is the difference between in-band versus out-of-band (OOB) method of monitoring Dell servers?

   Answer: There are two ways to monitor Dell servers, one is by using in-band method through software called OpenManage Server Administrator (OMSA) installed on a server operating system and the other is out-of-band method through iDRAC with LC.

   iDRAC with LC, a hardware, is on the server motherboard and iDRAC with LC enables systems administrators to monitor and manage dell servers regardless of whether the machine is powered on, or if an operating system is installed or functional. The technology works from any location and without the use of software agents like OMSA. By contrast, in-band management, that is, OMSA must be installed on the server being managed and only works after the machine is booted and the operating system is running and functional. The OMSA software has its limitations such as it does not allow access to BIOS settings, or the reinstallation of the operating system and cannot be used to fix problems that prevent the system from booting.

5. **Question:** Can I monitor Dell servers using OpenManage Server Administrator (OMSA) agent instead of iDRAC with LC using this plug-in?

   Answer: No, using this plug-in you cannot monitor Dell servers using OMSA agent. However, there are other plug-ins available on Nagios Exchange using which you can achieve the same. For more information, regarding the list of available Dell Plug-ins, visit URL: exchange.nagios.org/directory/Plugins/Hardware/Server-Hardware/Dell

6. **Question:** How is this plug-in different from other plug-ins available on the Nagios Exchange site?

   Answer: The primary functionality of this Plug-in is to monitor Dell servers' hardware through an agent-free, out-of-band method using iDRAC with LC. With this plug-in, you can get a comprehensive hardware-level information on Dell PowerEdge servers including overall and component-level health monitoring through SNMP and WS-MAN protocols. The plug-in enables

you to monitor SNMP alerts generated from Dell servers and supports one-to-one iDRAC web console launch to perform further troubleshooting, configuration, and management activities. Some of the capabilities provided here are not available in other plug-ins present on Nagios Exchange.

7. **Question:** What are the languages supported by the plug-in?

   Answer: The plug-in currently supports only English language.

A

Appendix

Configuring SNMP settings from web console

1. Launch the iDRAC (12th and later generation of Dell PowerEdge servers) web console and navigate to **Network** → **Services** in the console.
2. Configure the SNMP Agent properties:
   a. Set Enabled to true and SNMP Protocol to All (SNMP v1/v2/v3).
   b. Set **SNMP Community Name** with a community string.
   c. Click **Apply** to submit the configuration.

NOTE: The Plug-in communicates with iDRAC using only SNMP V1 or SNMP V2c protocol.

Configuring SNMP settings from RACADM CLI

1. Launch the iDRAC RACADM CLI by running the following ssh command:
   `ssh root@<iDRAC IP>`
2. Change the command mode to **racadm** by running the following command:
   `racadm`
3. Set the SNMP community string by running the following command:
   `racadm set idrac.snmp.agentcommunity <community string>`
4. Enable the SNMP agent by running the following command:
   `racadm set idrac.snmp.agentenable 1`
   (Values: 0 — Disabled, 1 — Enabled)
5. Set the SNMP protocol to **All** by running the following command:
   `racadm set idrac.snmp.snmpprotocol 0`
   (Values: 0 — All, 1 — SNMPv3)
6. Verify the configuration by running the following command:
   `racadm get idrac.snmp`

Setting up SNMP trap destination

1. Launch iDRAC Console and select **Overview** → **Server** → **Alerts**.
2. In **SNMP and Email Settings** tab, provide the destination IP address and select the **State**.