Advanced Monitoring of Dell Devices in Nagios Core Using Dell OpenManage Plug-in

Ankit Bansal
Systems Management Engineering
Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>April 2016</td>
<td>Initial document</td>
<td>Ankit Bansal</td>
</tr>
</tbody>
</table>
## Table of Contents

1. Executive Summary
2. Introduction
3. Key features
4. Troubleshooting Scenarios and Use Cases
   4.1 Dell Server use cases
       4.1.1 Dell Server unreachable
       4.1.2 Dell Server unhealthy component
   4.2 Dell Storage use cases
       4.2.1 Dell Storage unreachable
       4.2.2 Dell Storage unhealthy component
   4.3 Dell Chassis use cases
       4.3.1 Dell Chassis unreachable
       4.3.2 Dell Chassis unhealthy component
   4.4 Dell device warranty Information
       4.4.1 Dell device warranty state
       4.4.2 Configure Dell device warranty state
5. Best Practices
   5.1 Basic monitoring vs. detailed monitoring
   5.2 User defined device service template
   5.3 User defined monitoring cycle
   5.4 Performance tuning during discovery process
6. References
7. Configuration Details
   7.1 Hardware Configuration Details
   7.2 Software Configuration Details
Figure 1: Dell Server unreachable.......................................................... 8
Figure 2: Dell Server status in warning state .................................................. 9
Figure 3: Dell Server alert knowledge base article ........................................... 9
Figure 4: Dell Storage unreachable ................................................................. 10
Figure 5: Dell Storage status in warning state .................................................. 11
Figure 6: Dell Storage alert knowledge base article ......................................... 11
Figure 7: Dell Chassis unreachable ............................................................... 12
Figure 8: Dell Chassis status in warning state .................................................. 13
Figure 9: Dell Chassis alert knowledge base article ......................................... 13
Figure 10: Dell device warranty detail/status ............................................... 14
Figure 11: Dell device warranty configuration setting ....................................... 15
Figure 12: Dell device warranty critical ......................................................... 15
Figure 13: Dell device service template ......................................................... 16
Figure 14: Dell device service configuration ................................................... 17
Figure 15: Dell device discovery process count configuration .......................... 18
1. Executive Summary

This paper provides detailed information on how to monitor Dell hardware in an IT environment managed by Nagios Core.

Nagios Core is an open source monitoring software tool that offers monitoring and alerting services for servers, switches, applications, and services. Nagios Core alerts IT administrators when things go wrong and inform when the problem is resolved. Nagios Core is a popular open-source monitoring solution and is used by organizations of all sizes; it provides the following features:

- Monitoring and scheduling
- Event handling and alerting
- Performing checks
- Sending notifications
- Processing performance data

Dell OpenManage Plug-In seamlessly integrates with the Nagios Core and provides monitoring of Dell devices in environments managed using Nagios Core. This Plug-in offers feature such as discovery, monitoring, console launches, and troubleshooting of the supported Dell devices. Using this Plug-In you can get complete hardware-level visibility including overall and component-level health monitoring, basic inventory information and event monitoring of Dell devices. It also supports context specific one-to-one web console launch of the discovered Dell devices directly from Nagios console for further troubleshooting, configuration, and management activities.

This document presents key features, configuration guidelines, use cases, and best practices that will help you to successfully deploy Dell OpenManage Plug-in for Nagios Core on Dell hardware.

**Target audience:** IT Administrators who are using Nagios Core software to monitor Dell hardware.
2. Introduction

Dell OpenManage Plug-in for Nagios Core provides capabilities to monitor 12th and later generations of Dell PowerEdge Servers using an agent-free method using Integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller, Datacenter Scalable Solutions (DSS), Dell Chassis, and Dell Storage devices in the Nagios Core console. This Plug-in provides comprehensive hardware-level visibility including overall and component-level health monitoring using both SNMP and WS-MAN (Web Services for Management) protocols. The following table shows the protocol support matrix for Dell devices.

<table>
<thead>
<tr>
<th>Dell Devices</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell PowerEdge servers</td>
<td>SNMP and WS-MAN</td>
</tr>
<tr>
<td>Dell Chassis</td>
<td>WS-MAN</td>
</tr>
<tr>
<td>Dell Storage</td>
<td>SNMP</td>
</tr>
</tbody>
</table>
3. Key features

Following are the key features offered by Dell Nagios Core Plug-in:

- Discover Dell devices.
- Display Dell device basic information.
- Monitor overall health and component level health of Dell devices.
- Monitor Dell device SNMP traps.
- Launch Dell device web console.
- Display Warranty information for Dell devices.

For detailed, refer to Downloading and installing section in the Dell OpenManage Plug-in Version 2.0 for Nagios Core User’s Guide at Dell.com/OpenManageManuals.

IT administrators need to ensure that they meet the following pre-requisites based on the monitoring protocol selected.

The requirements for the management systems are as follows:

- Red Hat Enterprise Linux (RHEL) 7 and RHEL 6.6 (32-bit and 64-bit)
- SUSE Linux Enterprise Server (SLES) 11 and SLES 10 (32-bit and 64-bit)

For detailed instructions, refer to Downloading and installing section in the Dell OpenManage Plug-in Version 2.0 for Nagios Core Installation guide at Dell.com/OpenManageManuals.
4. Troubleshooting Scenarios and Use Cases

This section discusses the Dell OpenManage Plug-in for Nagios Core use cases which can help IT administrators to quickly identify and troubleshoot issues related to Dell hardware. The use cases discussed in this section are listed below:

- Dell server use cases
- Dell storage use cases.
- Dell chassis use cases.
- Dell Hardware warranty Information.

**Note:** To simulate the test cases, the server, storage, and chassis components are manually shutdown or their configurations are changed to generate alerts and are verified if the alerts are available in Dell OpenManage Plug-in for Nagios Core.

4.1 Dell Server use cases

4.1.1 Dell Server unreachable

IT administrator can monitor whether the discovered Dell agent-free server in Nagios Core console is reachable or unreachable by observing the **Hosts** page in the Nagios Core console. Please refer Figure 1 where, one of the Dell agent-free servers has become unreachable during monitoring and its status column has changed to “DOWN” with its Status Information as “PING CRITICAL”.

![Figure 1: Dell Server unreachable](image)

4.1.2 Dell Server unhealthy component

If one of the components in a discovered Dell agent-free server has a problem, then that device will generate an SNMP alert and this alert will be received in the Nagios Core console and is mapped with the “Dell Server Traps” service.

IT administrators also would be able to observe the Status change with the corresponding component as well as in the device’s Overall Health Status.
Please refer Figure 2 where one of the Temperature sensor readings has crossed the warning threshold value which in turn triggered a Temperature trap and associated it to the “Dell Server Traps” service.

As one of the Temperature sensor moved to the ‘WARNING’ state, the overall “Dell Server Temperature Probe Status” and the “Dell Server Overall Health Status” services correspondingly moves to the “WARNING” state.

**Figure 2: Dell Server status in warning state**

For each of the generated trap message ID, IT administrators can simply click on the “More Information” link and then open in a new browser to check the root cause and resolution suggestions. Please refer Figure 3.

**Temperature Messages**

**Figure 3: Dell Server alert knowledge base article**

Dell Plug-in helps IT administrators to monitor Dell agent-free server components from event trigger phase all the way to providing suggestions on the root cause and end-to-end monitoring.

**Note:** The individual and overall component status in the device health service and its specific component service status will not be the same till the next cycle of the corresponding component service check completes.
4.2  Dell Storage use cases

4.2.1  Dell Storage unreachable

IT administrators can monitor whether the discovered Dell Storage in the Nagios Core console is reachable or unreachable by observing the **Hosts** page of Nagios Core console. Please refer Figure 4 where one of the Dell Storage is unreachable and therefore monitoring and status column shows the device in "DOWN" state along with “PING CRITICAL” information.

![Nagios Console Screenshot](image)

Figure 4: Dell Storage unreachable

4.2.2  Dell Storage unhealthy component

If one of the components in discovered Dell EqualLogic (Storage) device having some problem then device will generate an SNMP alert and same alert will get received in Nagios Core console and mapped with “Dell Storage EqualLogic Traps” service.

IT administrator would be able to observe the status change in device overall health service.

Please refer Figure 5 where one of the Disks (11) has been removed from the discovered EqualLogic device so a SNMP alert with “WARNING” severity has been generated and monitored/mapped with corresponding Storage trap service e.g. “Dell Storage EqualLogic Traps”.

Since one of the disks is missing, the “Dell EqualLogic Member Overall health” status has changed to the “WARNING” state.
For each generated EqualLogic traps, IT administrator can refer "More Information" link and open in new browser tab to check root cause and resolution suggestion. Please refer Figure 6

### DiskStatus Messages

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
<th>Severity</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The status of the EqualLogic &lt;Disk Slot&gt; has changed to (online).</td>
<td>Information</td>
<td>Disk drive is functioning.</td>
<td>No resolution required.</td>
</tr>
<tr>
<td>1</td>
<td>The status of the EqualLogic &lt;Disk Slot&gt; has changed to (spare).</td>
<td>Information</td>
<td>Disk drive is a spare drive.</td>
<td>No resolution required.</td>
</tr>
<tr>
<td>1</td>
<td>The status of the EqualLogic &lt;Disk Slot&gt; has changed to (replacement).</td>
<td>Information</td>
<td>Disk drive is a replacement drive for failed drive.</td>
<td>No resolution required.</td>
</tr>
<tr>
<td>1</td>
<td>The status of the EqualLogic &lt;Disk Slot&gt; has changed to (encrypted).</td>
<td>Information</td>
<td>Disk drive is an encrypted drive.</td>
<td>No resolution required.</td>
</tr>
<tr>
<td>1</td>
<td>The status of the EqualLogic &lt;Disk Slot&gt; has changed to (Offline).</td>
<td>Warning</td>
<td>Indicates that the disk drive does not fall into the other status categories.</td>
<td>Check if disk is offline.</td>
</tr>
</tbody>
</table>

Figure 5: Dell Storage status in warning state

Figure 6: Dell Storage alert knowledge base article
4.3 Dell Chassis use cases

4.3.1 Dell Chassis unreachable

IT administrator can monitor if the discovered Dell chassis in Nagios Core console is reachable or unreachable by observing Hosts page of Nagios Core console. Please refer Figure 7 where one of the Dell chassis went unreachable during monitoring and status column shows “DOWN” along with information says “PING CRITICAL”.

Figure 7: Dell Chassis unreachable

4.3.2 Dell Chassis unhealthy component

If one of the components in discovered Dell chassis having some problem then device will generate an SNMP alert and same alert will get received in Nagios Core console and mapped with “Dell Chassis Traps” service.

IT administrator would be able to observe the status change with corresponding component and also in device overall health service.

Please refer Figure 8, where one of the Power Supply (redundant) instances has been removed, which in turn triggered a ‘CRITICAL’ SNMP alert and associate to “Dell Chassis Traps” service.

Due to that overall Power Supply service status changed to ‘CRITICAL’. As this Chassis have the redundant Power Supply so Overall Chassis health status will be ‘WARNING’ state but not ‘CRITICAL’.
Advanced Monitoring of Dell Device in Nagios Core with Dell OpenManage Plug-in

Figure 8: Dell Chassis status in warning state

For each generated Dell chassis traps, IT administrator can refer “More Information” link and open in new browser tab to check root cause and resolution suggestion by searching with corresponding alert message ID. Please refer Figure 9.

**PowerSupply Messages**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Message ID</th>
<th>Description</th>
<th>Severity</th>
<th>Cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2185</td>
<td>PSU0001</td>
<td>Power supply number</td>
<td>Critical</td>
<td>None</td>
<td>Remove and re-install the power supply. If the issue persists, contact technical support. Refer to the product documentation to choose a convenient contact method.</td>
</tr>
<tr>
<td></td>
<td>PSU0003</td>
<td>The power input for power supply is not connected</td>
<td>Critical</td>
<td>The power supply is installed correctly but an input source is not connected or is not functional.</td>
<td>Verify the input source is attached to the power supply. Verify the input power is within the operating requirements for the power supply.</td>
</tr>
<tr>
<td></td>
<td>PSU0004</td>
<td>The power supply number is outside of range</td>
<td>Critical</td>
<td>The operating requirements for the power supply may be found in product documentation or on the power supply itself.</td>
<td>Verify the input source is attached to the power supply. Verify the input power is within the operating requirements for the power supply.</td>
</tr>
</tbody>
</table>

Figure 9: Dell Chassis alert knowledge base article

4.4 Dell device warranty Information

4.4.1 Dell device warranty state

The warranty information for the respective Dell devices will be displayed in the Nagios core console. The Dell devices are polled for their warranty information at regular intervals. The default schedule for warranty polls on the discovered devices is once every 24 hours.

The warranty information severity will be determined based on the warranty parameter definitions and has the following severities:

- **Normal** - If the warranty is due to expire in more than <Warning> days.
- **Warning** - If the warranty is due to expire within <Critical> to <Warning> days.
**Critical** - If the warranty is due to expire within <Critical> days.

**Unknown** - If the warranty information cannot be retrieved.

Attribute ‘Days Remaining’ – Number of days left for the warranty to expire will decide the Dell device overall Status.

Please refer Figure 10 where the ‘Days Remaining’ value is greater than 30 (default) days therefore the overall Warranty service status is displayed as ‘OK’

![Figure 10: Dell device warranty detail/status](image)

### 4.4.2 Configure Dell device warranty state

In case IT administrator wish to receive a CRITICAL warranty status notification for a discovered Dell device earlier than 10 days, which is the default value for a critical status notification, navigate to `Dell_OpenManage_Plugin → resources → dell_pluginconfig.cfg` file and change the default value of this parameter from RemainingDaysCritical=10 to RemainingDaysCritical=<any custom value>. Please refer Figure 11 for the warranty configuration file.

For detailed instructions, refer warranty detail section in the Dell OpenManage Plug-in version 2.0 for Nagios Core User’s guide at [Dell.com/OpenManageManuals](https://www.dell.com/support/manuals)
The Warranty service overall status will change based on the values provided for the **RemainingDaysCritical** and **RemainingDaysWarning** parameters as shown in Figure 12.

![Figure 11: Dell device warranty configuration setting](image1)

![Figure 12: Dell device warranty critical](image2)
6 Best Practices

6.1 Basic monitoring vs. detailed monitoring

Basic Monitoring includes monitoring of Dell device information, Dell device Overall Health, and Dell SNMP Traps. In general, to monitor the Dell device health, creating the basic services is sufficient.

In case IT administrators still need detailed monitoring, which includes basic monitoring along with monitoring of components such as Processor, Memory, Physical Disk, Virtual Disk, Controllers, NIC, Power Supply, Fan, Battery, Voltage Probe, Temperature Probe, Amperage Probe, Intrusion, SD Card, Volume, etc. he or she can do so by enabling this service during device discovery itself by providing the 'detail (-d)' parameter.

However, IT administrators need to keep in mind that enabling the detailed monitoring services will consume more system resources. Please refer Figure 13.

---

**Figure 13: Dell device service template**

```bash
# Template for Basic/Detailed monitoring service Option
#
# Comment the line using '#' in the beginning, if you do not want the
# services to be created. Do not modify any other content of the file,
# else you may experience problems in creating the Services.
# These services are applicable for Dell iDRAC basic monitoring
Dell Server Information
Dell Server Overall Health Status
Dell Server Traps

# These services are applicable for both SNMP and WSMAN based Dell iDRAC monitoring
Dell Server Physical Disk Status
Dell Server Battery Status
Dell Server Fan Status
Dell Server Intrusion Status
Dell Server Virtual Disk Status
Dell Server Network Device Status
Dell Server Voltage Probe Status
Dell Server Amperage Probe Status
Dell Server Controller Status
Dell Server Temperature Probe Status
```
For detailed instructions, refer to Device discovery and inventory section in the Dell OpenManage Plug-in version 2.0 for Nagios Core User’s guide at Dell.com/OpenManageManuals

6.2 User defined device service template

By default, all the available services are created for a Dell device during discovery as supported by the protocol you have selected. It is always advisable for IT administrators to maintain a separate service template file with only specific services to be discovered for a Dell device while ignoring those services he or she does not need to monitor.

IT administrators can do this by navigating to the "<Nagios Installed Location>/scripts/dell_device_services_template.cfg" file and commenting those services you do not wish to monitor. Navigate to <NAGIOS_HOME>/dell/scripts, and then run the following PERL script:

```
perl dell_device_discovery.pl -H <host or IP Address> -t <dell_device_services_template_custom.cfg>
```

This user defined template can be maintained in a non-default location too.
For detailed instructions, refer to ‘Dell discovery and inventory’ section in the Dell OpenManage Plug-in Version 2.0 for Nagios Core User’s guide at Dell.com/OpenManageManuals

6.3 User defined monitoring cycle

The discovery utility creates the required services for the hosts to be monitored. These services get triggered periodically as per their configured interval of the "normal_check_interval" attribute in the file "<Nagios Installed Location>/dell/config/templates/dell_templates.cfg". The default intervals for the various parameters are as follows:

- Dell Device Information – 1440 Minutes (24 Hours)
- Dell Device Warranty Information – 1440 Minutes (24 Hours)
- Dell Device Overall Health Status – 60 Minutes (01 Hour)
- Dell Device <Component> Status – 240 Minutes (04 Hours)

To change the default scheduled interval for all the discovered Dell devices, you can modify the "normal_check_interval" attribute value in the "<Nagios Installed Location>/dell/config/templates/dell_templates.cfg" file. To change the default scheduled interval for the discovered Dell devices, add the "normal_check_interval" attribute with the required value in the host specific configuration file in the services definition block. For example:

```
<Nagios Installed Location>/dell/config/objects/<IP / FQDN>< host specific configuration file >.cfg
```

Nagios service restart is required for these interval changes to take effect.
Please refer Figure 14.

```
define service{
    name Dell Device Health Status
    use Dell-Service
    register
    service_description Dell Device Overall Health Status
    normal_check_interval 50 ; Polling interval in minutes
    retry_check_interval 15
    contact_groups delladmins
}
```

Figure 14: Dell device service configuration
6.4 Performance tuning during discovery process

Dell device discovery is an important and unique feature for the Dell OpenManage Plug-in for Nagios Core. In a large IT environment, discovery might take time to discover and classify Dell devices and can result in an adverse impact on user experience. It can be addressed by customizing the number of simultaneously discovery processes. In order to custom define the number of simultaneously discovery processes you can set the `process.count` parameter in `dell_pluginconfig.cf`. This file can be accessed by navigating to `<Dell_OpenManage_Plugin/ resources/dell_pluginconfig.cfg>`. Default value of `process.count` parameter is 20. Dell recommends this value to be set between 1 and 150, however administrators are advised to observe Nagios Core server performance while fine tuning this parameter. Please refer Figure 15.

```
# Dell PLUGIN CONFIG.CFG - Configuration file for Dell OpenManage Plugin for Nagios core
# parameters are specified in a Key-Value pair.
# Do not modify any key. Only modify the value.
# In case the key is tampered with, then the default value will be used.

# Dell Warranty API server URL

# Warranty Service - Number of days left for critical status
RemainingDaysCritical=10

# Warranty Service - Number of days left for warning status
# 'RemainingDaysWarning' should be greater than 'RemainingDaysCritical'.
# 'RemainingDaysWarning' and 'RemainingDaysCritical' value should be between 0 to 365
RemainingDaysWarning=30

# Number of discovery process to be forked
process.count=20
```

Figure 15: Dell device discovery process count configuration
7. References

a. Download for Dell OpenManage Plug-in version 2.0 for Nagios Core
   
   https://marketing.dell.com/omc-Nagios Core-software

   
   http://en.community.dell.com/techcenter/systems-management/w/wiki/6277.dell-openmanage-
   plug-in-for-nagios-core

c. Wiki link to configure trap destination in iDRAC using RCADM utility
   
   http://en.community.dell.com/techcenter/systems-management/w/wiki/11460.snmp-parameters-
   configuration-script-for-dell-idracs
8. Configuration Details

Following hardware and software configuration used for providing the use cases in this whitepaper.

8.1 Hardware Configuration Details

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Dell Remote Access Controller (iDRAC) 7/8</td>
</tr>
</tbody>
</table>
| Chassis   | Dell PowerEdge M1000e Chassis (Firmware Version – 5.1 and 2.0)  
Dell PowerEdge VRTX Chassis (Firmware Version – 2.1 and 2.0)  
Dell PowerEdge FX2/FX2s Chassis (Firmware Version – 1.3 and 1.2) |
| Storage   | Dell Compellent Storage Arrays (Firmware Version – 6.6 and 6.5)  
Dell EqualLogic PS-Series Storage Arrays (Firmware Version – 8.0.4 and 7.1.7)  
Dell PowerVault MD 34/38 Series Storage Arrays (Firmware Version – 8.20.09.60 and 8.20.05.60) |

8.2 Software Configuration Details

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nagios Core</td>
<td>Nagios Core version 3.5.0 or later</td>
</tr>
</tbody>
</table>
| Operating System | - Red Hat Enterprise Linux (RHEL) 7 and RHEL 6.6 (32-bit and 64-bit)  
- SUSE Linux Enterprise Server (SLES) 11 and SLES 10 (32-bit and 64-bit) |