Monitoring and Eventing the health of RAID Controllers and its drives using Dell Command | Monitor

A technical whitepaper explaining how DCM monitors the health of a RAID Controller and its associated drives.

Dell Engineering
September 2014
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept’ 2014</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2014 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the DELL logo, and the DELL badge are trademarks of Dell Inc. Symantec, NetBackup, and Backup Exec are trademarks of Symantec Corporation in the U.S. and other countries. Microsoft, Windows, and Windows Server are registered trademarks of Microsoft Corporation in the United States and/or other countries. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Trademarks used in this text:
Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOC®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or
# Table of contents

Revisions ........................................................................................................................................................................... 2

Acknowledgements ................................................................................................................................................................ 6

Feedback ............................................................................................................................................................................. 6

Executive summary .......................................................................................................................................................... 6

1 Introduction .................................................................................................................................................................... 7
   1.1 Purpose and scope ..................................................................................................................................................... 7
   1.2 Terminology ........................................................................................................................................................... 8

2 Monitoring RAID Controller ......................................................................................................................................... 9
   2.1 Monitoring Properties ............................................................................................................................................ 9
   2.2 Degraded alert .......................................................................................................................................................... 10
   2.3 Repetative alerts ...................................................................................................................................................... 12
   2.4 Monitoring failure from DCIM class .................................................................................................................... 13
   2.5 Configuration of Alert Interval ......................................................................................................................... 14

3 Monitoring Virtual Disk ............................................................................................................................................... 15
   3.1 Monitoring Properties ........................................................................................................................................... 15
   3.2 Disk Degraded Alert ................................................................................................................................................ 16
   3.3 Disk Rebuilding Alert ........................................................................................................................................... 19
   3.4 Disk Failure Alert .................................................................................................................................................... 19
   3.5 Disk Offline Alert .................................................................................................................................................... 19
   3.6 Repetative alerts .................................................................................................................................................... 21
   3.7 Monitoring failure from DCIM class .................................................................................................................... 22
   3.8 Configuration of Alert Interval ......................................................................................................................... 23

4 Monitoring Physical Disk ............................................................................................................................................ 24
   4.1 Monitoring Properties ............................................................................................................................................. 24
   4.2 Disk Degraded Alert ................................................................................................................................................. 25
   4.3 Disk Rebuilding Alert ............................................................................................................................................. 25
   4.4 Disk Failure Alert .................................................................................................................................................... 27
   4.5 Disk Offline Alert .................................................................................................................................................... 29
   4.6 Repetative alerts .................................................................................................................................................... 31
   4.7 Monitoring failure from DCIM class .................................................................................................................... 32
   4.8 Configuration of Alert Interval ......................................................................................................................... 33
Acknowledgements

This whitepaper has been prepared by the following members of the Dell Enterprise team:

Engineering: Sharmad Naik
Excellence: Karthik Chandran
Strengthening: Mainak Roy

Feedback

We encourage readers of this publication to provide feedback on the quality and usefulness of this by logging information on OMCI – OpenManage Client Instrumentation TechCenter forum.

Executive summary

The Dell Precision system is high end biz-client systems typically used for workstations or as small scale business servers. The range varies from towers to rack systems and notebooks to workstations. This system has a wide variety of configuration including RAID Controllers.

Monitoring RAID Controllers are important for an organization specifically if the system is used as a business critical appliance with RAID enabled configuration of varied RAID Levels (mirroring, stripping and/or parity).

The Dell Command | Monitor (DCM) enables monitoring and eventing of a RAID Controller and its associated drivers. This whitepaper intends to cover the details of how monitoring and eventing is exposed using DCM.

Monitoring of RAID Controllers can be done with 3 classes DCIM_RAIDController, DCIM_VirtualDiskView and DCIM_PhysicalDiskView. Eventing support is enabled with DCM for RAID in the following methods:

- WMI Events
- Events logged in DCM_LogEntry class
- SNMP traps
- Eventlog

Click here to see an earlier whitepaper on overall Health Monitoring with OMCI.

Note: For Monitoring SNMP traps, the SNMP support for DCM has to be enabled on the system. Please refer to the Install Guide, and SNMP Reference Guide for more information.

Note: Although much of the content here is presented with LSI RAID Controllers (tested with Integrated Controllers and cards 9217-8i, 9271-8i, 9341-8i and 9361-8i), but DCM also supports integrated Intel Controllers with CSMI v0.81 support.
1 Introduction

Client Instrumentation refers to software applications that enable remote management of a client system. The Dell Command | Monitor (Command | Monitor) software enables remote management using application programs to access the Enterprise Client system information, monitor the status, or change the state of the system such as remotely shutting down the system. Command | Monitor uses key system parameters through standard interfaces allowing administrators to manage inventory, monitor system health, and gather information about deploying Enterprise client systems.

Command | Monitor manages client systems using the Common Information Model (CIM) standard and SNMP, which are management protocols. This reduces the total cost of ownership, improves security, and provides a holistic approach to manage all the devices, including clients, servers, storage, network, and software devices.

Using CIM you can access Command | Monitor through Web Services for Management Standards (WSMAN).

Command | Monitor contains the underlying driver set that collects client system information from different sources, including the BIOS, CMOS, System Management BIOS (SMBIOS), System Management Interface (SMI), operating system, Application programming interface (APIs), Dynamic-link library (DLLs), and registry settings. Command | Monitor fetches this information through the CIM Object Manager (CIMOM) interface, Windows Management Instrumentation (WMI) stacks or SNMP agent.

Command | Monitor enables IT administrators to remotely collect asset information, modify CMOS settings, receive proactive notifications about potential fault conditions, and get alerts for potential security breaches. These alerts are available as events in the event log, CIM Indication or received as SNMP traps after importing the MIB file.

Command | Monitor is used to gather asset inventory from the system, including BIOS settings, through CIM implementation or SNMP agent. It can be integrated into a console such as Microsoft System Center Configuration Manager by directly accessing the CIM information, or through other console vendors who have implemented the Command Monitor integration. Additionally, you can create custom scripts to target key areas of interest. You can use these scripts to monitor inventory, BIOS settings, and system health.

Note: From Dell Command | Monitor version 9.0 onwards, the 10892 MIB is not supported. The 10909 MIB replaces 10892 MIB and identifies only client systems. Please refer to the Installation Guide and SNMP Reference Guide for more information.

1.1 Purpose and scope

This paper is primarily intended for IT administrators who are involved in monitoring the hardware status of a system. This document assumes the reader is familiar with DCM/OMCI usage, RAID and system administration. The scope of this paper is restricted to health monitoring and eventing of the RAID Controller and connected drives.
1.2 Terminology

The following terms are used throughout this document:

Hot Spare: A hot spare or hot standby is used as a failover mechanism to provide reliability in system configurations. The hot spare is active and connected as part of a working system. When a key component fails, the hot spare is switched into operation.

Logical Disk: is a device that provides an area of usable storage capacity on one or more physical disk drive components in a computer system.

Redundant Array of Independent Disks (RAID): is a data storage virtualization technology that combines multiple disk drive components into a logical unit for the purposes of data redundancy or performance improvement.
2 Monitoring RAID Controller

RAID Controller monitoring is supported in DCM for Intel Integrated and LSI (Integrated and Card) Controllers.

2.1 Monitoring Properties

Monitoring is achieved by querying the DCIM class `DCIM_ControllerView`. The following attribute information is populated for every instance of the RAID Controller:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BusType</td>
<td>The property represents the type of the PCI bus. Possible values are 0 - Unknown, 3 - PCI Bus, 4 - PCMCIA Bus, 0x8000 - DMTF Reserved, 0xffff - Vendor Reserved</td>
</tr>
<tr>
<td>ControllerFirmwareVersion</td>
<td>This property represents the firmware version.</td>
</tr>
<tr>
<td>Device</td>
<td>This property represents the device name.</td>
</tr>
<tr>
<td>Driver Version</td>
<td>This property represents the version of the driver.</td>
</tr>
<tr>
<td>ElementName</td>
<td>A user-friendly name for the object. This property allows each instance to define a user-friendly name in addition to its key properties, identity data, and description information.</td>
</tr>
<tr>
<td>InstanceID</td>
<td>This property contains the value of the Fully Qualified Device Description (FQDD).</td>
</tr>
<tr>
<td>PrimaryStatus</td>
<td>This property represents the status of the device. Possible values are 0 - Unknown, 1 – OK, 2 – Degraded, 3 – Error</td>
</tr>
<tr>
<td>ProductName</td>
<td>This property provides the family name of the controller.</td>
</tr>
</tbody>
</table>

Table 1  RAID Controller properties information

When the RAID controller is functioning normal, then the primary status of the card is displayed equal to 1. The snapshot below displays the output of the powershell script to check the controller status.

Figure 1  Powershell output to display the Controller Status
2.2 Degraded alert

Whenever the RAID Controller detects a failure, it generates a degraded alert (ID #1804). The Severity level of the alert is of type “Warning”. The alert is displayed in the EventLog as follows:

![EventLog output to display the degraded RAID Controller alert](image)

Figure 2 EventLog output to display the degraded RAID Controller alert

An equivalent SNMP trap is displayed (if SNMP is enabled and configured) as follows.
The status of the attribute PrimaryStatus of the class DCIM_ControllerView for that instance of RAID Controller now reflects the new status (value = 2). A snapshot of the same is as shown below.
2.3 Repetative alerts

All RAID Controller alerts are repetitive and continuously adding till the failure is resolved. The first alert in the set has the previous state value in the description field of the alert defined in the normal or previous state of the system.

The following snapshot displays the first alert of RAID Controller failure.

![Event Viewer](image)

**Figure 5** EventLog output to display the first degraded RAID Controller alert

The snapshot below displays the onwards next alert of the RAID Controller failure till the hardware failure is addressed and resolved.
2.4 Monitoring failure from DCIM class

An entry of the failure of the RAID Controller is logged into the DCIM_LogEntry class. Enumeration of the class displays all the failures that have occurred.

The snapshot below displays the output using a CIMStudio application for the failures in the system.

Figure 6  EventLog output to display the next repetitive degraded RAID Controller alert

Figure 7  Enumeration of the DCIM_LogEntry class display failure alerts
The command used to get the above information is as follows.

```bash
gwmi -Namespace root\dcim\sysman -Class Dcim_logentry | select ele*,rec* / Format-List
```

### 2.5 Configuration of Alert Interval

The RAID Controller alerting interval can be modified by changing the dcsdby<32/64>.ini file in the folder `<INSTALLDIR>/Dell/CommandMonitor/omsa/ini`. For each defined event of a particular type, there is configuration defined in this file that could be customized for the time interval. The minimal refresh time interval implemented for RAID Controller monitoring is 23 secs. Hence, one can modify the typical configuration for the supported RAID Controller is as follows

```
[RAID Controller]
StartDelay=1
RunDelay=0
```

The start delay is used to indicate the delay in the first event since the data manager service is started. The RunDelay value is used to indicate the delay in the periodic or successive event since the current event occurs. Hence, considering the refresh interval defined as 23 secs, and the RunDelay defined as “0”, then the next event occurs during the next refresh cycle for the Controller. If the value was defined as “1”, then the event would occur in the adjacent refresh cycle (i.e. after 46 secs).
3 Monitoring Virtual Disk

Virtual Disk monitoring is supported in DCM for Intel Integrated and LSI (Integrated and Card) Controllers.

3.1 Monitoring Properties

Monitoring is achieved by querying the DCIM class `DCIM_VirtualDiskView`. The following attribute information is populated for every instance of the Physical Disk.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElementName</td>
<td>A user-friendly name for the object. This property allows each instance to define a user-friendly name in addition to its key properties, identity data, and description information.</td>
</tr>
<tr>
<td>InstanceID</td>
<td>The property contains the value of the Fully Qualified Device Description (FQDD).</td>
</tr>
<tr>
<td>PrimaryStatus</td>
<td>This property represents the status of the device. Possible values are: 0 - Unknown 1 - OK 2 - Degraded 3 - Error 4 – Rebuilding 5 – Offline</td>
</tr>
<tr>
<td>RAIDStatus</td>
<td>This property represents the RAID specific status. Possible values are: 0 - Unknown 1 - Ready 2 - Online 3 - Foreign 4 - Offline 5 - Blocked 6 - Failed 7 – Degraded 8 – Rebuilding</td>
</tr>
<tr>
<td>RAIDTypes</td>
<td>This property represents the current RAID level. Possible values are: 1 - No RAID 2 - RAID-0 4 - RAID-1 64 - RAID-5 128 - RAID- 6 2048 - RAID-10 8192 - RAID-50 16384 - RAID- 60</td>
</tr>
<tr>
<td>SizeinMegabytes</td>
<td>The property represents the size of the virtual disk in megabytes.</td>
</tr>
<tr>
<td>StripeSize</td>
<td>This property represents the current strip size. Possible values are: 0 - Default 1 - 512Bytes</td>
</tr>
<tr>
<td>PhysicalDiskIDs</td>
<td>The property represents the array of physical disk FQDDs.</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>2 – 1 KB</td>
<td></td>
</tr>
<tr>
<td>4 – 2 KB</td>
<td></td>
</tr>
<tr>
<td>8 - 4 KB</td>
<td></td>
</tr>
<tr>
<td>16 - 8 KB</td>
<td></td>
</tr>
<tr>
<td>32 - 16 KB</td>
<td></td>
</tr>
<tr>
<td>64 - 32 KB</td>
<td></td>
</tr>
<tr>
<td>128 - 64 KB</td>
<td></td>
</tr>
<tr>
<td>256 - 128 MB</td>
<td></td>
</tr>
<tr>
<td>512 - 256 MB</td>
<td></td>
</tr>
<tr>
<td>1024 - 512 MB</td>
<td></td>
</tr>
<tr>
<td>2048 - 1 MB</td>
<td></td>
</tr>
<tr>
<td>4096 - 2 MB</td>
<td></td>
</tr>
<tr>
<td>8192 - 4 MB</td>
<td></td>
</tr>
<tr>
<td>16384 – 8 MB</td>
<td></td>
</tr>
<tr>
<td>32768 – 16 MB</td>
<td></td>
</tr>
</tbody>
</table>

### Table 2 Virtual Disk properties information

When the Virtual Disk is functioning normal than the primary status of the drives is displayed equal to 1. The snapshot below displayed the output of the powershell script to check the controller status.

![Powershell output to display the Virtual Disk Status](image)

#### Figure 8  Powershell output to display the Virtual Disk Status

### 3.2 Disk Degraded Alert

When the logical drive degrades, DCM detects that and generates an alert (and SNMP trap) of ID #1821. The Severity level of the alert is of type “Error”. The alert is displayed in the EventLog as follows:
Figure 9  EventLog output to display the degraded Virtual Disk alert

An equivalent SNMP trap is displayed (if SNMP is enabled and configured) is as follows.
Figure 10   SNMP trap displayed the degraded Virtual Disk alert

The status of the attribute PrimaryStatus of the class DCIM_VirtualDiskView for that instance of RAID Controller reflects the new status. A snapshot of the same is shown below

Figure 11   Attribute value of PrimaryStatus and Raid Status for Degraded Virtual Disk
3.3 **Disk Rebuilding Alert**
When the logical drive is rebuilding, DCM detects that and generates an alert (and SNMP trap) of ID #1822. The Severity level of the alert is of the type “Warning”.

The status of the attribute PrimaryStatus of the class DCIM_VirtualDiskView for that instance of RAID Controller updates to the new status.

3.4 **Disk Failure Alert**
When the logical drive fails, DCM detects that and generates an alert (and SNMP trap) of ID #1823. The Severity level of the alert is of the type “Error”.

The status of the attribute PrimaryStatus of the class DCIM_VirtualDiskView for that instance of RAID Controller updates to the new status.

3.5 **Disk Offline Alert**
When the logical drive gets offline, DCM detects that and generates an alert (and SNMP trap) of ID #1824. The Severity level of the alert is of type “Error”. The alert is displayed in the EventLog as follows:

![EventLog output to display the Offline alert for Virtual Disk](image)

Figure 12  EventLog output to display the Offline alert for Virtual Disk
An equivalent SNMP trap displays (if SNMP is enabled and configured) as follows.

**Figure 13** SNMP trap displayed the Offline Virtual Disk alert

The status of the attribute PrimaryStatus of the class DCIM_VirtualDiskView for that instance of RAID Controller reflects the new status. A snapshot of the same is shown below.

**Figure 14** Attribute value of PrimaryStatus and Raid Status for Offline Virtual Disk
3.6 Repetative alerts

All Logical Disk alerts are repetitive and continuously adding till the failure is resolved. The first alert in the set will have the previous state value in the description field of the alert defined in the normal or previous state of the system.

The first snapshot displays the first alert of Virtual Disk Degraded.

![Event Viewer output to display the first degraded Virtual Disk alert](image)

The snapshot below displays the onwards next alert of the Virtual Disk Degraded till the hardware failure is addressed and resolved.
3.7 Monitoring failure from DCIM class

An entry of the failure of the Virtual Disk is logged in the DCIM_LogEntry class. Enumeration of the class displays all the failures that have occurred.

The command used to get the above information is as follows.

```
gwmi -Namespace root\dcim\sysman -Class Dcim_logentry | select ele*,rec* | Format-List
```
3.8 Configuration of Alert Interval

The RAID Controller alerting interval can be modified by changing the dcsdby<32/64>.ini file in the folder <INSTALLDIR>/Dell/CommandMonitor/omsa/ini. For each defined event of a particular type, there is configuration defined in this file that could be customized for the time interval. The minimal refresh time interval implemented for Virtual disk monitoring is 23 secs. Hence, one can modify the typical configuration for the supported Virtual Disk is as follows

```
[Virtual Disk]
StartDelay=1
RunDelay=0
```

The start delay is used to indicate the delay in the first event since the data manager service is started. The RunDelay value is used to indicate the delay in the periodic or successive event since the current event occurs. Hence, considering the refresh interval defined as 23 secs, and the RunDelay defined as “0”, then the next event occurs during the next refresh cycle for the Controller. If the value was defined as “1”, then the event would occur in the adjacent refresh cycle (i.e. after 46 secs).
4 Monitoring Physical Disk

Physical Disk monitoring is supported in DCM for Intel Integrated and LSI (Integrated and Card) Controllers.

4.1 Monitoring Properties

Monitoring is achieved by querying the DCIM class *DCIM_PhysicalDiskView*. The following attribute information is populated for every instance of the Physical Disk

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ElementName</td>
<td>A user-friendly name for the object. This property allows each instance to define a user-friendly name in addition to its key properties, identity data, and description information.</td>
</tr>
<tr>
<td>InstanceID</td>
<td>The property contains the value of the Fully Qualified Device Description (FQDD).</td>
</tr>
<tr>
<td>PrimaryStatus</td>
<td>This property represents the status of the device. Possible values are: 0 - Unknown 1 - OK 2 - Degraded 3 - Error 4 – Rebuilding 5 – Offline 0x8000 – DMTF Reserved 0xFFFF – Vendor Reserved</td>
</tr>
<tr>
<td>DriveUsage</td>
<td>This property indicates if the physical disk is in a RAID set. Possible values are: 0 - Not in a RAID Set 1 - In a RAID Set 2 – Hot Spare</td>
</tr>
<tr>
<td>Model</td>
<td>This property represents the model name of the physical disk</td>
</tr>
<tr>
<td>SerialNumber</td>
<td>This property represents the serial number of the physical disk.</td>
</tr>
<tr>
<td>DriveAFStatus</td>
<td>This property indicates if the physical disk is an advanced format drive. Possible values are: 0 - Non AF Drive 1 - AF Drive 2 – Unknown</td>
</tr>
</tbody>
</table>

Table 3 Physical Disk properties information

When the Physical Disk is functioning normal than the primary status of the drives is displayed as 1. The snapshot below displays the output of the powershell script to check the controller status.
4.2 **Disk Degraded Alert**

When the physical drive gets degraded, DCM detects it and generate an alert (and SNMP trap) of ID #1811. The Severity level of the alert is of type “Error”.

The status of the attribute PrimaryStatus of the class DCIM_PhysicalDiskView for that instance of physical Drive updates to the new status.

4.3 **Disk Rebuilding Alert**

When the physical drive is rebuilding, DCM detects that and generates an alert (and SNMP trap) of ID #1812. The Severity level of the alert is of type “Warning”. The alert is displayed in the EventLog as follows:

![EventLog output to display the Rebuilding Physical Disk alert](image)

An equivalent SNMP trap displays (if SNMP is enabled and configured) is as follows:

---

Monitoring and Eventing the health of RAID Controllers and its drives using Dell Command | Monitor
Figure 20  SNMP trap displayed the Rebuilding Physical Disk alert

The status of the attribute PrimaryStatus of the class DCIM_PhysicalDiskView for that instance of physical Drive reflects the new status. A snapshot of the same is shown below.

Figure 21  Attribute value of PrimaryStatus and Drive Usage for Rebuilding Physical Disk
4.4 Disk Failure Alert

When the physical drive fails, DCM detects it and generate an alert (and SNMP trap) of ID #1813. The Severity level of the alert is of type “Error”. The alert is displayed in the EventLog as follows:

![Event Log Output]

Figure 22  EventLog output to display the Failure alert for Physical Disk
An equivalent SNMP trap is displayed (if SNMP is enabled and configured) as follows.

**Figure 23**  SNMP trap displayed the Failure of Physical Disk alert

The status of the attribute PrimaryStatus of the class DCIM_PhysicalDiskView for that instance of physical Drive reflects the new status. A snapshot of the same is shown below.

**Figure 24**  Attribute value of PrimaryStatus and Drive Usage for Failure Physical Disk
4.5 Disk Offline Alert

When the physical drive fails, DCM detects that and generates an alert (and SNMP trap) of ID #1814. The severity level of the alert is of type “Warning”. The alert is displayed in the EventLog as follows.

![EventLog output to display the Offline alert for Physical Disk](image)

Figure 25  EventLog output to display the Offline alert for Physical Disk
An equivalent SNMP trap is displayed (if SNMP is enabled and configured) is as follows.

![SNMP trap displayed the Offline Physical Disk alert](image1)

**Figure 26** SNMP trap displayed the Offline Physical Disk alert

The status of the attribute PrimaryStatus of the class DCIM_PhysicalDiskView for that instance of physical Drive reflects the new status. A snapshot of the same is shown below.

![Attribute value of PrimaryStatus and Drive Usage for Offline Physical Disk](image2)

**Figure 27** Attribute value of PrimaryStatus and Drive Usage for Offline Physical Disk
4.6 Repetative alerts

All Physical Disk alerts are repetitive and continuously added till it is resolved. The first alert in the set has the previous state value in the description field of the alert defined in the normal or previous state of the system.

The first snapshot displays the first alert of Physical Disk Offline.

![Event Log output to display the first Offline Physical Disk alert](image)

Figure 28  EventLog output to display the first Offline Physical Disk alert
The snapshot below displays the next onwards alert of the Physical Disk offline till the issue is resolved.

![Event Viewer](image)

Figure 29  EventLog output to display the next Offline Physical Disk alert

4.7 Monitoring failure from DCIM class

An entry of the failure of the Physical Disk is logged into the DCIM_LogEntry class. Enumeration of the class will display all the failures that have occurred.

![Select Administrator: Windows PowerShell](image)

Figure 30  Enumeration of the DCIM_LogEntry class  display failure alerts

The command used to get the above information is as follows.

```
gwmi -Namespace root\dcim\sysman -Class Dcim_logentry | select ele*,rec* | Format-List
```
4.8 Configuration of Alert Interval

The Physical Disk alerting interval can be modified by changing the dcsdby<32/64>.ini file in the folder <INSTALLDIR>/Dell/CommandMonitor/omsa/ini. For each defined event of a particular type, there is configuration defined in this file that could be customized for the time interval. The minimal refresh time interval implemented for Physical Disk monitoring is 23 secs. Hence, one can modify the typical configuration for the supported Physical Disk as follows:

```ini
[CSMI Physical Disk]
StartDelay=1
RunDelay=0
```

The start delay is used to indicate the delay in the first event since the data manager service is started. The RunDelay value is used to indicate the delay in the periodic or successive event since the current event occurs. Hence, considering the refresh interval defined as 23 secs, and the RunDelay defined as “0”, then the next event occurs during the next refresh cycle for the Physical drive. If the value was defined as “1”, then the event would occur in the adjacent refresh cycle (i.e after 46 secs).
A  Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell Customers and Dell SMEs for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

Referenced or recommended Dell publications:

- Install Guide:
- User Guide:
- Reference Guide
- SNMP Reference Guide:
  http://downloads.dell.com/published/Pages/index.html#esuprt_client_sys_mgmt_opnmang_clnt_instr

- Extending Client Instrumentation uses OMCI
  http://en.community.dell.com/techcenter/extras/m/white_papers/20410895.aspx

- Using SNMP with OMCI:
  http://en.community.dell.com/dell-groups/dtcmedia/m/mediagallery/19852516/download.aspx