Monitoring Dell PowerEdge VRTX

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

Table of Figures

1

Monitoring Dell PowerEdge VRTX

Dell PowerEdge VRTX is a computer hardware product line from Dell. It is a mini-blade chassis with built-in storage system. It integrates servers, storage, networking and management in a compact shared infrastructure optimized for office environments.

The VRTX comes in two models: a 19" rack version that is 5 rack units high or as a stand-alone tower system.

The key components of the VRTX are as follows:

- **Servers:**

  The VRTX chassis has 4 half-height slots available for PowerEdge blade servers system. At launch the PE-M520 and the PE-M620 where the only two supported server blades. The same blades are used in the M1000e but for use in the VRTX they need to run specific configuration. A conversion kit is available from Dell to allow moving a blade from a M1000e to VRTX chassis.

- **Storage:**

  The VRTX chassis includes shared storage slots that connect to a single or dual PERC 8 controller(s). This controller which is managed through the CMC allows RAID groups to be configured and then allows for those RAID groups to be subdivided into individual virtual disks that can be presented out to either single or multiple blades. The shared storage slots are either 12 x 3,5" HDD slots or 25 x 2,5" HDD slots depending on the VRTX chassis purchased.

- **Networking:**

  The VRTX chassis has a built in IOM for supporting ethernet traffic to the server blades. At present the options for this IOM are an 8 port 1Gb pass-through module or a 24 Port 1Gb switch. The 8 port pass through module offers 2 pass-through connections to each internal blade slot where the 24 port 1Gb switch option provides 16 internal ports (4 per blade slot) and 8 external ports to be used to uplink to the network. The I/O modules used on the VRTX have different size then the I/O modules of the M1000e, so you are not able to use the I/O modules that are available for that chassis system. A 10Gb I/O module is planned for future release.

In addition, the VRTX comes bundled with power and cooling systems, USB connectors, a serial communication port, expansion slots, and even a mini LCD screen, all of which enable administrators of small and medium-sized enterprises to deliver high quality IT services to their users.

To ensure that the delivery of these services is not disrupted, administrators must make sure that the VRTX is available 24x7 to cater to the server and storage needs of data centers. For this purpose, eG Enterprise provides a web-based *Dell PowerEdge VRTX* monitoring model.

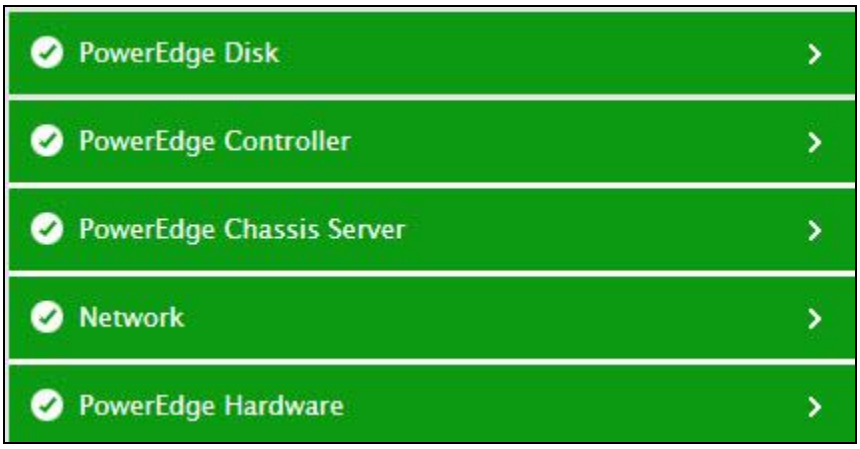

Figure 1.1: Layer model of the Dell PowerEdge VRTX

Each layer of Figure 1.1 above is mapped to a variety of tests. Every test polls the SNMP MIB of the VRTX at configured intervals to check the overall health of the VRTX and that of the PSUs, voltage probes, chassis, cooling units and other hardware components that support the VRTX. This way, administrators can be proactively alerted to the potential failure of the VRTX hardware. In addition, the tests also track the storage capacity and usage of the physical and virtual disks of the VRTX, thus warning administrators early of probable disk space contentions (if any).

With the help of the metrics reported by these tests, administrators can find quick and accurate answers to the following questions:

- Are all hardware components of the VRTX in good health? If not, then which component(s) has failed?
- Are all blade servers in the VRTX chassis functioning normally?
- Is the storage enclosure available to applications?
- Is any hardware component within the enclosure experiencing critical or non-recoverable errors presently?
- Is any RAID controller in an abnormal state now? If so, is it because of the poor health of the hardware components supporting it?
- Are all physical disks operating normally? If not, which physical disk is experiencing critical operational snags?
- Is any physical disk running out of space?
- Is any virtual disk in bad health currently?

The sections that follow discuss each layer of Figure 1.1 above.

1.1 The PowerEdge Hardware Layer

The tests mapped to this layer monitor the health and operational state of the VRTX hardware.

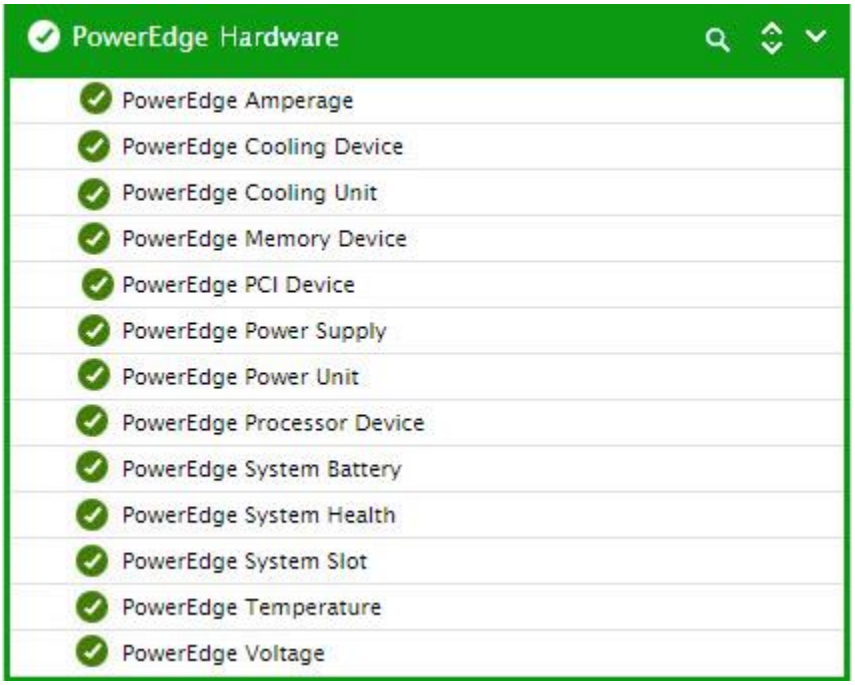

Figure 1. 2: The tests mapped to the PowerEdge Hardware layer

1.1.1 PowerEdge Amperage Test

Amperage probes built into the VRTX help administrators determine the current amperage running through a circuit. If any of these probes fail, administrators will not be able to detect any sudden surge in the input power of a circuit. If this surge persists, it may cause serious damage to the VRTX hardware. It is hence imperative that administrators be notified instantly if an amperage probe behaves abnormally or registers a high input power reading. This is where the **PowerEdge Amperage Test** helps. For each amperage probe, this test reports how healthy that probe currently is, how much input power it registered last, and what its present power state is. This sheds light on the abnormal health and power state of a probe.

Purpose	For each amperage probe, this test reports how healthy that probe currently is, how much input power it registered last, and what its present power state is. This sheds light on the abnormal health and power state of a probe.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each amperage probe of the VRTX being monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this probe currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical Upper</td><td>4</td></tr><tr><td>Critical Upper</td><td>5</td></tr><tr><td>NonRecoverable Upper</td><td>6</td></tr><tr><td>NonCritical Lower</td><td>7</td></tr><tr><td>Critical Lower</td><td>8</td></tr><tr><td>NonRecoverable Lower</td><td>9</td></tr><tr><td>Failed</td><td>10</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of an amperage probe. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td>Input power:
Indicates the current input power recorded by this probe.</td><td>Watts</td><td>A sudden and significant rise in the value of this measure could be a cause of concern.
This measure reports values, only if the temperature probe is of a type other than ‘GenericDiscrete’.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Power status:
Indicates the current power state of this amperage probe.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of an amperage. In the graph of this measure however, the same is represented using the numeric equivalents only.
This measure reports values, only if the temperature probe is of a type other than 'GenericDiscrete'.</td>
</tr>
</table>

1.1.2 PowerEdge Cooling Device Test

Each 1100 Watt PSU in the VRTX has a built-in fan. For cooling of the server-modules there are four blower-modules, each containing two fans, and for cooling of the rest of the chassis there are 6 internal fans. If any of these fans fail, then the temperature of the core hardware components of the VRTX may suddenly soar, causing irreparable damage to those components. If such failures are to be averted, administrators must continuously check on the health, speed, and running condition of every fan, detect potential aberrations in fan state before they actually occur, and quickly initiate preventive measures. This is what the **PowerEdge Cooling Device** test does!

For every fan in the VRTX, this test reports the current health, speed, and running condition of that fan, captures abnormalities on-the-fly, and brings them to the attention of the administrators. This enables administrators to identify those fans that are in the danger of going down and helps them quickly initiate measures to repair or replace such fans to ensure that VRTX operations resume without a glitch.

Purpose	For every fan in the VRTX, this test reports the current health, speed, and running condition of that fan, captures abnormalities on-the-fly, and brings them to the attention of the administrators. This enables administrators to identify those fans that are in the danger of going down and helps them quickly initiate measures to repair or replace such fans to ensure that VRTX operations resume without a glitch.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each fan in the VRTX being monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this fan currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical Upper</td><td>4</td></tr><tr><td>Critical Upper</td><td>5</td></tr><tr><td>NonRecoverable Upper</td><td>6</td></tr><tr><td>NonCritical Lower</td><td>7</td></tr><tr><td>Critical Lower</td><td>8</td></tr><tr><td>NonRecoverable Lower</td><td>9</td></tr><tr><td>Failed</td><td>10</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a fan. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td>Speed:
Indicates the current speed of this fan.</td><td>Rpm</td><td>A sudden and significant rise in the value of this measure could be a cause of concern.</td></tr>
</table>

	Running condition: Indicates the current running condition of this fan.		The values that this measure can report and their corresponding numeric values are discussed below: **Measure Value** / **Numeric Value** Good / 1 Bad / 2 **Note:** By default, this measure reports one of the **Measure Values** listed above to indicate the current condition of a fan. In the graph of this measure however, the same is represented using the numeric equivalents only.

1.1.3 PowerEdge Cooling Unit Test

A cooling unit in VRTX typically consists of many fan modules and blower modules. These cooling units ensure that the temperature of the VRTX is at permissible levels. If a cooling unit fails, then the temperature of the associated hardware components cannot be automatically regulated. This may cause the internal temperature of the VRTX to rise uncontrollably, resulting in considerable damage to the hardware. This is why, the health of each cooling unit should be verified time and again, and abnormalities (if any) escalated to the administrator. This is exactly what the **PowerEdge Cooling Unit** test does! This test reports the current health of each cooling unit of the VRTX, thus turning the spotlight on those units that may potentially fail. In addition, the test also checks the redundancy status of each cooling unit, and highlights the non-redundant units.

Purpose	Reports the current health of each cooling unit of the VRTX, thus turning the spotlight on those units that may potentially fail. In addition, the test also checks the redundancy status of each cooling unit, and highlights the non-redundant units.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each cooling unit in the VRTX being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Health status:
Indicates how healthy this cooling unit currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical Upper</td><td>4</td></tr><tr><td>Critical Upper</td><td>5</td></tr><tr><td>NonRecoverable Upper</td><td>6</td></tr><tr><td>NonCritical Lower</td><td>7</td></tr><tr><td>Critical Lower</td><td>8</td></tr><tr><td>NonRecoverable Lower</td><td>9</td></tr><tr><td>Failed</td><td>10</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a cooling unit. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Redundancy status:
Indicates the current redundancy status of this cooling unit.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Full</td><td>3</td></tr>
<tr><td>Degraded</td><td>4</td></tr>
<tr><td>Lost</td><td>5</td></tr>
<tr><td>Not Redundant</td><td>6</td></tr>
<tr><td>Redundancy Offline</td><td>7</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the redundancy status of a cooling unit. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

1.1.4 PowerEdge Memory Device Test

VRTX supports DDR3 unbuffered ECC DIMMs (UDIMM ECC) and registered DIMMs (RDIMMs).

DIMM or **dual in-line memory module** comprises a series of dynamic random-access memory integrated circuits. **Registered** (also called **buffered**) **DIMMs** have a register between the DRAM modules and the memory controller. They place less electrical load on the memory controller and allow single systems to remain stable with more memory modules than they would have otherwise. When compared with registered memory, conventional memory is usually referred to as **unbuffered memory** or **unregistered memory (UDIMM)**. ECC DIMMs are those that have extra data bits which can be used by the memory controller to detect and correct errors.

A critical error in any of the DIMMs (registered/unregistered) can even render the VRTX unusable. It is therefore imperative that the state of each DIMM in the VRTX be closely tracked, and administrators warned of any impending danger to the health of the DIMM. This is where the **PowerEdge Memory Device** test helps. This test reports the current health of each DIMM, and in this way, alerts administrators to any abnormality related to a DIMM. The test also reports the size and speed configuration of every DIMM.

Purpose	Reports the current health of each DIMM, and in this way, alerts administrators to any abnormality related to a DIMM. The test also reports the size and speed configuration of every DIMM.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each DIMM in the VRTX being monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this DIMM currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a DIMM. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td>Total size:
Indicates the total installed memory size of this DIMM.</td><td>GB</td><td></td></tr>
<tr><td></td><td>Speed:
Indicates the current speed of this DIMM.</td><td>Nanosecs</td><td></td></tr>
</table>

1.1.5 PowerEdge PCI Device Test

PCI refers to a Peripheral Component Interconnect, which is used for attaching hardware devices to the VRTX. A single VRTX chassis supports up to 8 PCI devices. To know which PCI devices are currently operating in an error-free manner and which ones are not, use the **PowerEdge PCI Device** test. This test auto-discovers the PCI devices and

reports the current health of each device.

Purpose	Auto-discovers the PCI devices and reports the current health of each device.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each PCI device in the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this PCI device currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a PCI device. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

1.1.6 PowerEdge Power Supply Test

Each power supply unit in the VRTX will contain multiple power supply points. The availability and proper functioning of each of these ppower supply points is critical to the uninterrupted operations of the VRTX. Irrecoverable errors, sensor failures, or erratic voltage fluctuations experienced by a power point can stall VRTX operations for hours, slowing down or completely suspending the delivery of the dependent business services. If such an unpleasant eventuality is to be pre-empted, administrators must be able to proactively detect potential problems with a power supply point and take remedial action before anything untoward happens. The **PowerEdge Power Supply** test helps administrators achieve this end. For each power supply point on the VRTX, this test reports how healthy that power supply point currently is, how well (or badly) its sensor is performing currently, and what is that power supply's current voltage. In the process, administrators can quickly isolate those power supply points that are behaving abnormally and can immediately initiate measures to correct the anomaly.

Purpose	For each power supply point on the VRTX, this test reports how healthy that power supply point currently is, how well (or badly) its sensor is performing currently, and what is that power supply's current voltage. In the process, administrators can quickly isolate those power supply

	points that are behaving abnormally and can immediately initiate measures to correct the anomaly.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each power supply point in the VRTX being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Health status:
Indicates how healthy this power supply point currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a power supply point. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Sensor status:
Indicates the current operational state of this power supply's sensor.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Sensor detected</td><td>1</td></tr>
<tr><td>Failure detected</td><td>0</td></tr>
<tr><td>Predictive failure</td><td>4</td></tr>
<tr><td>AC lost</td><td>8</td></tr>
<tr><td>AC lost or out of range</td><td>16</td></tr>
<tr><td>AC out of range but present</td><td>32</td></tr>
<tr><td>Configuration error</td><td>64</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a power supply's sensor. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Input voltage:
Indicates the current input voltage of this power supply.</td>
<td>Volts</td>
<td>A sudden and significant spike in the value of this measure could prove to be detrimental to the health of the power supply point and other internal components of the VRTX.</td>
</tr>
</table>

1.1.7 PowerEdge Power Unit Test

VRTX is powered by two to four Dell 1100W PSUs. VRTX uses these PSUs to support both low-line (115 VAC) and high-line (220 VAC) power sources. Dell 1100W PSUs support a maximum of four PSUs with the current sharing circuitry. Critical errors in a PSU can affect the health of the power supplies in that PSU, which in turn can adversely impact VRTX operations. This is why, it is very important for an administrator to detect the failure of a PSU before it occurs and do whatever it takes to avert the disaster. The **PowerEdge Power Unit** test aids administrators in this exercise. The test reports the current status of each PSU in VRTX, and in the process, highlights those PSUs that are error-prone. Additionally, the test also points to those PSUs that are not redundant. This way, the test brings the very vulnerabke PSUs to the attention of the administrator.

Purpose	Reports the current status of each PSU in VRTX, and in the process, highlights those PSUs that are error-prone. Additionally, the test also points to those PSUs that are not redundant. This way, the test brings the very vulnerabke PSUs to the attention of the administrator
Target of the	A Dell PowerEdge VRTX

test	
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each PSU in the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this PSU currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a PSU. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Redundancy status:
Indicates the current redundancy status of this PSU.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Full</td><td>3</td></tr>
<tr><td>Degraded</td><td>4</td></tr>
<tr><td>Lost</td><td>5</td></tr>
<tr><td>Not Redundant</td><td>6</td></tr>
<tr><td>Redundancy Offline</td><td>7</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the redundancy status of a PSU. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

1.1.8 PowerEdge Processor Device Test

The VRTX supports up to two Intel Xeon processor E5-2600 product family. How quickly the VRTX services requests to it depends upon how efficient each of these processors is. This can be determined using the **PowerEdge Processor Device** test. This test reports the configuration and current health status of every processor, and reveals those processors that are not performing at peak capacity currently and those that have not been sized right.

Purpose	Reports the configuration and current health status of every processor, and reveals those processors that are not performing at peak capacity currently and those that have not been sized right
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each processor in the VRTX being monitored</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this processor currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a processor. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td>Speed:
Indicates the current speed of this processor.</td><td>MHz</td><td></td></tr>
<tr><td>Voltage:
Indicates the current voltage of this processor.</td><td>mV</td><td></td></tr>
<tr><td>Processor cores:
Indicates the number of processor cores.</td><td>Number</td><td></td></tr>
<tr><td>Enabled cores:
Indicates the number of processor cores enabled.</td><td>Number</td><td></td></tr>
</table>

	Thread count: Indicates the number of processor threads configured for this processor.	Number	

1.1.9 PowerEdge System Battery Test

A faulty battery can deal a fatal blow to the availability and operational efficiency of the VRTX. An administrator should hence proactively detect which battery is malfunctioning and should swiftly arrange to remove and replace such a battery, so as to ensure service continuity. This is where the **PowerEdge System Battery** test helps. This test reports the health of each VRTX battery, thus leading administrators to the exact battery that is defective.

Purpose	Reports the health of each VRTX battery, thus leading administrators to the exact battery that is defective
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each battery in the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this battery currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a battery. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

1.1.10 PowerEdge System Health Test

The Dell PowerEdge VRTX chassis comprises of many components such as processors, memory devices, batteries, PSUs, amperage probes, voltage sensors, temperature probes, cooling units, and blade servers. Each of these components influence the availability and overall performance of the VRTX system. This is why, at any given point in time, administrators will not only need to know how well the VRTX system as a whole is performing, but will also require pointers to which component could be adversely impacting its performance. Such a useful insight on performance is provided by the **PowerEdge System Health** test. Besides revealing the current health of the VRTX system as a whole, this test all reports the collective state of each of the component types that form an integral part of the VRTX system. This way, administrators can figure out whether/not the VRTX is healthy, and if not, can also determine where the source of the problem lies – is it with the memory devices? the processors? the batteries? the PSUs? the cooling units? the amperage probes? the voltage sensors? or the temperature probes? Or the blade servers? Once the area of concern is isolated, administrators can use the eG test that deep dives into that realm of performance to accurately diagnose the root-cause of the problem. For instance, if the **PowerEdge System Health** test reveals that one/more batteries are adversely impacting the health of the VRTX system, then administrators can use the **PowerEdge System Battery** test to find the defective battery.

Purpose	Besides revealing the current health of the VRTX system as a whole, this test all reports the collective state of each of the component types that form an integral part of the VRTX system.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Global system status:
Indicates how healthy the VRTX system as a whole is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the entire VRTX system. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Chassis server status :
Indicates the collective state of all blade servers in the the VRTX chassis.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the blade servers in the chassis. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Overall power unit status:
Indicates the current collective status of all the power units of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the power units. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Overall power supply status :
Indicates the current collective state of all the power supply points of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the power supply points. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Overall cooling unit status :
Indicates the current collective state of all the cooling units of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the cooling units. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Overall cooling device status :
Indicates the current collective state of all the cooling deviices of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the cooling devices. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Overall voltage probe status:
Indicates the current collective state of all the voltage probes of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the voltage probes. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Overall temperature probe status:
Indicates the current collective state of all the temperature probes of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the temperature probes. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Overall amperage probe status :
Indicates the current collective state of all the amperage probes of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the amperage probes. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Overall memory device status :
Indicates the current collective state of all the DIMMs of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the memory devices. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Overall processor device status :
Indicates the current collective state of all the processors of the VRTX system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the processor devices. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

	Overall system battery status : Indicates the current collective state of all the batteries of the VRTX system.		The values that this measure can report and their corresponding numeric values are discussed below: <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table> **Note:** By default, this measure reports one of the **Measure Values** listed above to indicate the current health of the batteries. In the graph of this measure however, the same is represented using the numeric equivalents only.

1.1.11 PowerEdge System Slot Test

The Dell VRTX chassis has slots available based on the versions to manage the dell blade server system. Before attempting to install a server in a slot, administrators should determine whether/not that slot is free or is already in use. Also, once a server is installed in a slot, administrators should continuously track the health of that slot. This is because, if a slot experiences a critical problem, then users may not be able to access the server installed in that slot. To effectively plan and efficiently execute server installations and to ensure that installed servers are always accessible to users, administrators can take the help of the **PowerEdge System Slot** test. This test not only reports the health of each slot, but also indicates whether/not a slot is available for use.

Purpose	Reports the health of each VRTX battery, thus leading administrators to the exact battery that is defective
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each slot in the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this slot currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a slot. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Slot usage status :
Indicates whether/not this slot is available for use.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Available</td><td>3</td></tr>
<tr><td>In Use</td><td>4</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate whether/not a slot is free. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

1.1.12 PowerEdge Temperature Test

Temperature probes in the VRTX system are configured with threshold values, which when violated, automatically increases the speed of the corresponding fans, so that temperatures never rise beyond a permissible limit. In the absence of these temperature probes, such automated cooling actions will not occur, causing the internal temperature of the VRTX to soar uncontrollably, fatally damaging hardware components in the process. This is why, it is important that administrators periodically check that the temperature probes are up and operating without a glitch.

Also, the threshold values defined for each of the temperature probes may have to be fine-tuned from time to time, so that the fan speed is changed only when there is a genuine need and not for marginal spikes in temperature. For this, the administrator should keep track of the temperature probe readings over time, understand whether/not that reading is good or bad as per the current threshold definition, and accordingly make changes (if required) to the configuration.

The **PowerEdge Temperature** test helps achieve both these ends. This test auto-discovers the temperature probes, reports the current status of each probe, reveals the current temperature reading of that probe, and indicates whether that reading is good or bad. This way, the test alerts administrators to unexpected probe failures and urges them to instantly initiate corrective action and restore normalcy. Additionally, the test also helps administrators quickly analyze the current temperature reading of a probe vis-à-vis its threshold setting, and thus helps them figure out whether the thresholds need to be refined or not.

Purpose	Auto-discovers the temperature probes, reports the current status of each probe, reveals the current temperature reading of that probe, and indicates whether that reading is good or bad. This way, the test alerts administrators to unexpected probe failures and urges them to instantly initiate corrective action and restore normalcy. Additionally, the test also helps administrators quickly analyze the current temperature reading of a probe vis-à-vis its threshold setting, and thus helps them figure out whether the thresholds need to be refined or not.
Target of the	A Dell PowerEdge VRTX

test	
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each temperature probe n the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this temperature probe currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical Upper</td><td>4</td></tr><tr><td>Critical Upper</td><td>5</td></tr><tr><td>NonRecoverable Upper</td><td>6</td></tr><tr><td>NonCritical Lower</td><td>7</td></tr><tr><td>Critical Lower</td><td>8</td></tr><tr><td>NonRecoverable Lower</td><td>9</td></tr><tr><td>Failed</td><td>10</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a temperature probe. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td></td><td>Temperature :
Indicates the current temperature reading of this probe.</td><td>DegreeC</td><td>This measure reports values, only if the temperature probe is of a type other than ‘GenericDiscrete’.
A sudden and a significant rise in temperature may require closer scrutiny.</td></tr>
</table>

	Temperature status : Indicates whether the temperature recording of this probe is good or bad.		The values that this measure can report and their corresponding numeric values are discussed below: **Measure Value** / **Numeric Value** Good / 1 Bad / 2 **Note:** By default, this measure reports one of the **Measure Values** listed above to indicate the current temperature status of a probe. In the graph of this measure however, the same is represented using the numeric equivalents only. **This measure reports values, only if the temperature probe is of a type other than 'GenericDiscrete'.**

1.1.13 PowerEdge Voltage Test

Voltage probes in the VRTX help administrators determine the current voltage of a VRTX component. If any of these probes fail, administrators will not be able to detect sudden and severe voltage fluctuations. As a result, such fluctuations may occur frequently, causing serious damage to the VRTX hardware. It is hence imperative that administrators be notified instantly if a voltage probe behaves abnormally or registers a high voltage reading. This is where the **PowerEdge Voltage Test** helps. For each voltage probe, this test reports how healthy that probe currently is, what its last voltage reading was, and whether that reading was good or bad. This sheds light on the abnormal health and voltage state of a probe.

Purpose	For each voltage probe, this test reports how healthy that probe currently is, what its last voltage reading was, and whether that reading was good or bad. This sheds light on the abnormal health and voltage state of a probe.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each voltage probe in the VRTX being monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this voltage probe currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical Upper</td><td>4</td></tr><tr><td>Critical Upper</td><td>5</td></tr><tr><td>NonRecoverable Upper</td><td>6</td></tr><tr><td>NonCritical Lower</td><td>7</td></tr><tr><td>Critical Lower</td><td>8</td></tr><tr><td>NonRecoverable Lower</td><td>9</td></tr><tr><td>Failed</td><td>10</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a voltage probe. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td>Voltage:
Indicates the current voltage reading of this probe.</td><td>mV</td><td>This measure reports values, only if the voltage probe is of a type other than 'GenericDiscrete'.
A sudden and a significant rise in voltage may require closer scrutiny.</td></tr>
</table>

	Voltage status : Indicates whether the voltage level recorded by this probe is good or bad.		The values that this measure can report and their corresponding numeric values are discussed below: **Measure Value** / **Numeric Value** Good / 1 Bad / 2 **Note:** By default, this measure reports one of the **Measure Values** listed above to indicate the current voltage status of a probe. In the graph of this measure however, the same is represented using the numeric equivalents only. **This measure reports values, only if the voltage probe is of a type other than 'GenericDiscrete'.**

1.2 The PowerEdge Chassis Server Layer

The Dell PowerEdge VRTX integrates compute and storage capabilities through a 5U rackable tower chassis. This chassis supports up to four 12th generation, hot-plug PowerEdge M520 or PowerEdge M620 blade servers. The M620 is a half-height blade server that supports up to 24 DIMMs and two processors. The M520 is a half-height blade server that supports up to 12 DIMMs and two processors.

Using the test mapped to this layer, you can rapidly detect those blade servers that are in an abnormal state currently.

Figure 1. 3: The test mapped to the PowerEdge Chassis Server layer

1.2.1 PowerEdge Chassis Server Test

The VRTX chassis consists of blade servers. If a user complains that he/she is not able to access a particular blade, adminisrators can use the **PowerEdge Chassis Sever** test to instantly identify the blade server that is in an abnormal state and is hence unable to handle user requests.

Purpose	To instantly identify the blade server that is in an abnormal state and is hence unable to handle user requests
Target of the test	A Dell PowerEdge VRTX
Agent	An external agent

deploying the test	
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each blade server in the VRTX chassis being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Health status:
Indicates how healthy this blade server currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a blade server. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

1.3 The PowerEdge Controller Layer

Problems in the hardware supporting the enclosure and the RAID controllers are revealed by the tests mapped to this layer.

Figure 1. 4: The tests mapped to the PowerEdge Controller layer

1.3.1 PowerEdge Enclosure Test

The VRTX storage enclosure includes shared storage slots that connect to a single or dual PERC 8 controller(s). This enclosure can include 12 x 3,5" HDD slots or 25 x 2,5" HDD slots depending on the VRTX chassis purchased. Critical problems in this storage enclosure can render the storage infrastructure of VRTX unavailable for the use of your mission-critical applications. To avoid this, an administrator should be able to detect problems with the enclosure well before they affect storage availability and performance. This is where the **PowerEdge Enclosure** test helps. This test periodically scans the storage enclosure for holes and proactively alerts administrators to potential abnormalities with the enclosure. In addition, the test also monitors the hardware supporting the HDD slots within the enclosure – i.e., the fans, PSUs, temperature and voltage probes, etc. – and reports their collective state from time to time, so that hardware failures inside the enclosure are promptly brought to the attention of the administrators.

Purpose	Periodically scans the storage enclosure for holes and proactively alerts administrators to potential abnormalities with the enclosure. In addition, the test also monitors the hardware supporting the HDD slots within the enclosure – i.e., the fans, PSUs, temperature and voltage probes, etc. – and reports their collective state from time to time, so that hardware failures inside the enclosure are promptly brought to the attention of the administrators.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the storage enclosure being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this enclosure currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of an enclosure. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>RollUp status :
Indicates the current status of the enclosure hardware.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the enclosure hardware. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

1.3.2 PowerEdge Raid Controllers Test

VRTX uses a single or dual (for redundancy) Shared PowerEdge Raid Controller (SPERC). This controller which is managed through the CMC allows RAID groups to be configured and then allows for those RAID groups to be subdivided into individual virtual disks that can be presented out to either single or multiple blades.

If a Raid controller or the hardware supporting it experiences critical or fatal issues, the blade servers in the VRTX will not be able to access the virtual disks. If such an outcome has to be averted, administrators must rapidly detect deviations in the performance of the Raid controller and its hardware, and should remedy the situation before it aggravates and affects storage access for the blade servers. This is exactly what the **PowerEdge Raid Controllers** test helps administrators do! At configured intervals, this test reports the current state of every Raid controller and its hardware, and in the process, warns administrators of their potential failure.

Purpose	At configured intervals, this test reports the current state of every Raid controller and its hardware, and in the process, warns administrators of their potential failure.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each Raid controller of the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this Raid controller currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a Raid controller. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>RollUp status :
Indicates the current status of the hardware supporting this Raid controller.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>NonCritical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>NonRecoverable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the controller hardware. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Cache size :
Indicates the current size of the cache memory of this Raid controller.</td>
<td>MB</td>
<td></td>
</tr>
</table>

1.4 The PowerEdge Disk Layer

The current health state, capacity, and usage of physical and virtual disks are reported by the tests mapped to this layer.

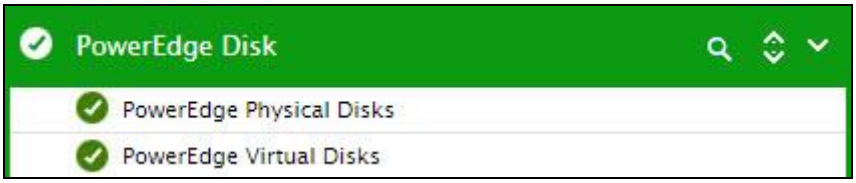

Figure 1. 5: The tests mapped to the PowerEdge Disk layer

1.4.1 PowerEdge Physical Disks Test

VRTX allows physical disks to be grouped into virtual/logical disks and presented for consumption by single or multiple blade servers. If one/more of these disks fail or run out of space, it is bound to impact the virtual storage resources available to the blade servers, causing multiple blade servers to contend for limited storage space. The lack of adequate storage space will eventually degrade blade server performance.

To make sure that blade servers perform at peak capacity at all times, administrators must proactively and accurately identify the physical disks that are about to fail or run out of space, determine the cause for the failure/space crunch, and swiftly address it, so that the disk failure can be prevented.

This is where the **PowerEdge Physical Disks** test helps. For each physical disk in the VRTX, this test reports the current state of that physical disk and tracks how space in that disk has been utilized. This way, the test points administrators to those disks that are behaving abnormally and those that have been utilized excessively.

Purpose	For each physical disk in the VRTX, this test reports the current state of that physical disk and tracks how space in that disk has been utilized. This way, the test points administrators to those disks that are behaving abnormally and those that have been utilized excessively.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each physical disk of the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this physical disk currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a physical disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Operation status:
Indicates the current operational status of this physical disk.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Ready</td><td>2</td></tr>
<tr><td>Online</td><td>3</td></tr>
<tr><td>Foreign</td><td>4</td></tr>
<tr><td>Offline</td><td>6</td></tr>
<tr><td>Blocked</td><td>5</td></tr>
<tr><td>Non Raid</td><td>8</td></tr>
<tr><td>Removed</td><td>9</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of the physical disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Disk spare status:
Indicates whether/not this physical disk.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Not a spare</td><td>1</td></tr>
<tr><td>Dedicated hot spare</td><td>2</td></tr>
<tr><td>Global hot spare</td><td>3</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate whether/not the physical disk is a spare disk or not. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Total space :
Indicates the total space in this physical disk.</td>
<td>GB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used space :
Indicates the amount of disk space used in this physical disk.</td>
<td>GB</td>
<td>Compare the value of this measure across disks to know from which disk maximum space has been consumed.</td>
</tr>
</table>

	Free space : Indicates the amount of space in this disk that is currently unused.	GB	A high value is desired for this measure. Compare the value of this measure across physical disks to know which disk has maximum free space.
	Space utilization : Indicates the percentage of space in this disk that is in use.	Percent	A value close to 100% for this measure is indicative of excessive space usage. Compare the value of this measure across physical disks to identify that disk that could be running out of space.

1.4.2 PowerEdge Virtual Disks Test

VRTX's Shared PowerEdge Raid Controller (SPERC) allows RAID groups to be configured and then allows for those RAID groups to be subdivided into individual virtual disks that can be presented out to either single or multiple blades.

If one/more of these virtual disks experience critical issues or fail, then they will be rendered unusable by the blade servers. In the absence of sufficient virtual disk space, blade server performance will begin to degrade shortly thereafter. To make sure that the blade servers are able to maintain high levels of performance at all times, virtual disk health should be monitored continuously, problems captured instantly, and administrators notified of these problems promptly. This is precisely what the **PowerEdge Virtual Disks** test does!

This test monitors every virtual disk configured in the VRTX and tracks the current health and operational status of each virtual disk. In the process, the test highlights those virtual disks that are deviating from the norm and draws administrator attention to them.

Purpose	Monitors every virtual disk configured in the VRTX and tracks the current health and operational status of each virtual disk. In the process, the test highlights those virtual disks that are deviating from the norm and draws administrator attention to them.
Target of the test	A Dell PowerEdge VRTX
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the VRTX exposes its SNMP MIB. The default port is 161. 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified **USERNAME** and **PASSWORD** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each virtual disk of the VRTX being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Health status:
Indicates how healthy this physical disk currently is.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>NonCritical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>NonRecoverable</td><td>6</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current health of a virtual disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Operation status:
Indicates the current operational status of this virtual disk.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Online</td><td>2</td></tr>
<tr><td>Degraded</td><td>4</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the current operational status of the virtual disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Disk size:
Indicates current capacity of this virtual disk.</td>
<td>GB</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Diskstrip size:
Indicates the current stripe size of this virtual disk.</td>
<td>GB</td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Default</td><td>2</td></tr>
<tr><td>520 bytes</td><td>3</td></tr>
<tr><td>1 KB</td><td>4</td></tr>
<tr><td>2 KB</td><td>5</td></tr>
<tr><td>4 KB</td><td>6</td></tr>
<tr><td>8 KB</td><td>7</td></tr>
<tr><td>16 KB</td><td>8</td></tr>
<tr><td>32 KB</td><td>9</td></tr>
<tr><td>64 KB</td><td>10</td></tr>
<tr><td>128 KB</td><td>11</td></tr>
<tr><td>256 KB</td><td>12</td></tr>
<tr><td>512 KB</td><td>13</td></tr>
<tr><td>1 MB</td><td>14</td></tr>
<tr><td>2 MB</td><td>15</td></tr>
<tr><td>4 MB</td><td>16</td></tr>
<tr><td>8 MB</td><td>17</td></tr>
<tr><td>16 MB</td><td>18</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the stripe size of the virtual disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Read policy:
Indicates the read policy used by the controller to read from this virtual disk.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No read ahead</td><td>1</td></tr>
<tr><td>Read ahead</td><td>2</td></tr>
<tr><td>Adaptive read ahead</td><td>3</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the read policy of the virtual disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Write policy:
Indicates the write policy used by the controller to write data to this virtual disk.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Write through</td><td>1</td></tr>
<tr><td>Write back</td><td>2</td></tr>
<tr><td>Write back force</td><td>3</td></tr>
</table>
Note:
By default, this measure reports one of the Measure Values listed above to indicate the write policy of the virtual disk. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
</table>

2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **Dell PowerEdge VRTX**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.