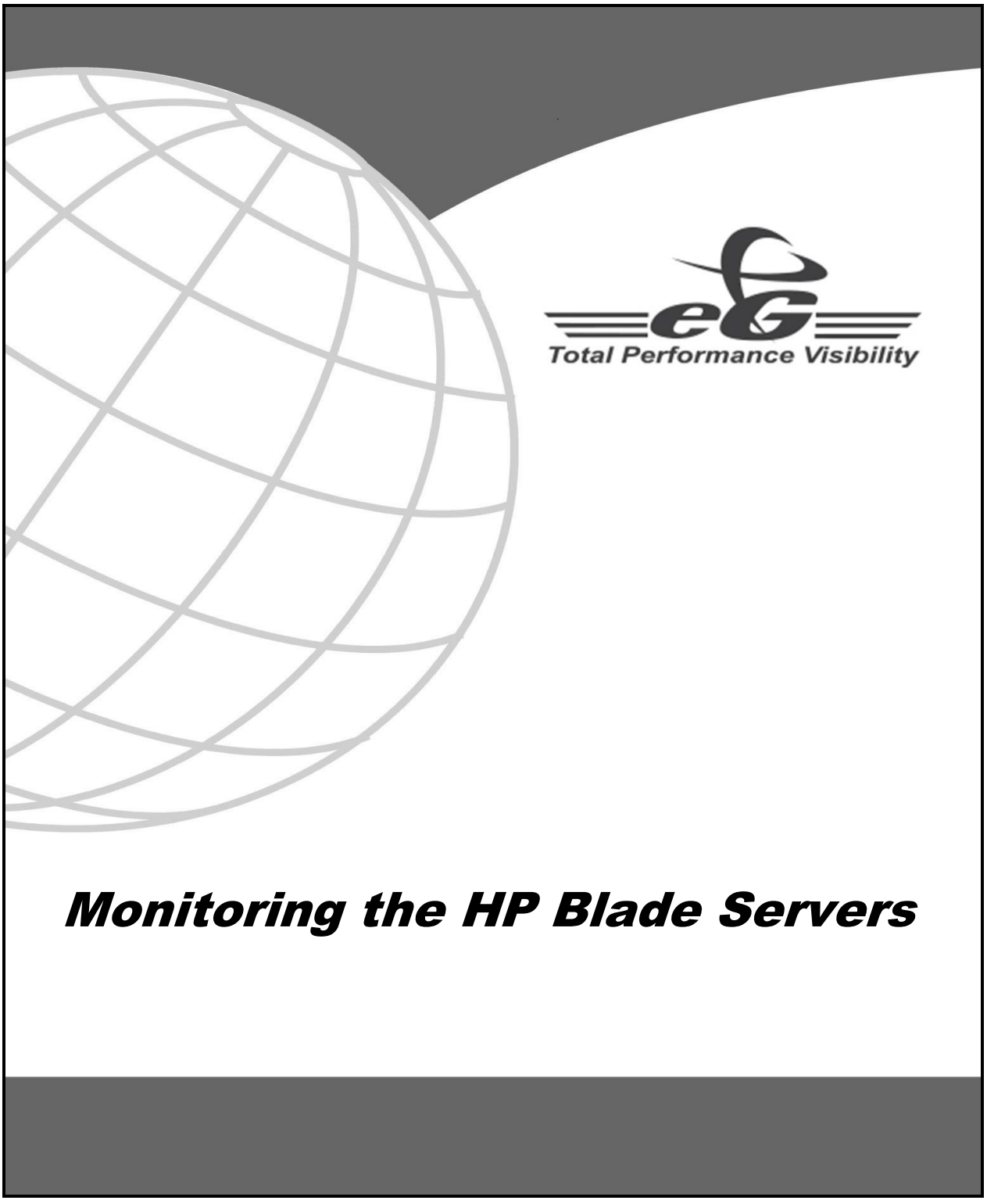

Monitoring the HP Blade Servers

Restricted Rights Legend

Trademarks

Copyright

Table of Contents

Table of Figures

Chapter 1

Monitoring HP Blade Servers

A blade is literally a self-contained server, which collectively fits into an enclosure with other blades. Sometimes known as a chassis, this enclosure provides the power, cooling, connectivity, and management to each blade. The blade servers themselves contain only the core processing elements, making them hot-swappable. HP refers to the entire package as a BladeSystem.

To get a better idea of what a single blade contains, an HP ProLiant blade holds hot-plug hard-drives, multiple I/O cards, memory, multi-function network interconnects, and Integrated Lights Out remote management. For additional storage, blades can connect to another storage blade or to a network attached SAN.

When compared to other traditional rack-mount servers, a blade server can be dedicated to a single task, such as:

- Database and application hosts
- Virtual server host platforms
- Remote desktop or workstations
- File sharing
- Web page serving and caching
- SSL encrypting of Web communication
- Transcoding of Web page content for smaller displays
- Streaming audio and video content

In order to be able to carry out the designated task smoothly, the blade server should receive adequate support from the enclosure components such as the fans, power supply units, temperature sensors, etc. In other words, an inadvertent failure of a power supply unit or a sudden increase in the temperature of a sensor, can affect the operations of not just one, but all the blade servers within the enclosure. To avoid such eventualities, the enclosure and its core components need to be continuously monitored.

To enable you to promptly detect issues with the enclosure or the services offered by it, and resolve such issues without delay so that the performance of the blades is not compromised, eG Enterprise presents the *HP Blade* monitoring model.

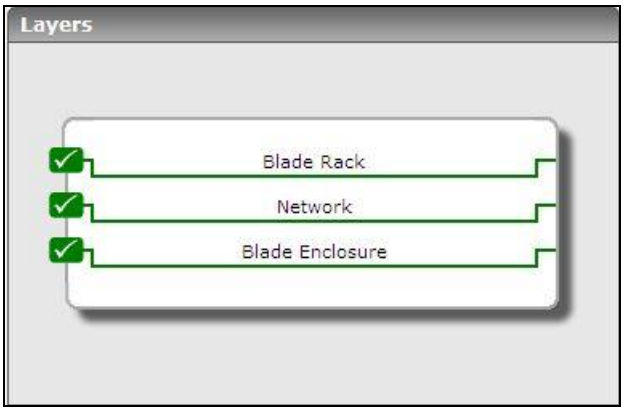

Figure 1: The layer model of the HP Blade Server

Each layer of Figure 1 pulls out a plethora of metrics revealing the condition of the enclosure, the composition of the enclosure, and the state of services offered by it so that, you can find quick and easy answers to the following:

- What does the enclosure contain - blades, power supplies, temperature sensors, net connectors, fuses, fans?
- What is the overall condition of the enclosure - good or bad? If bad, then, what is the root-cause of the abnormal behavior of the enclosure?
- Are all the fans operating normally? If not, which fan has failed?
- Have any fuses experienced failures? If so, which ones?
- Does the enclosure contain any failed temperature sensors? If so, which ones?
- Has any temperature sensor registered an abnormal temperature reading?
- Are all blades available? Which ones are not?
- Are all power supply units in the rack blade operational? Has any power supply experienced performance degradations or has failed completely?
- What is the current power output of each of the power supplies in a rack blade? Is the current power output of any unit unusually high?
- Which power enclosures are not in a load-balanced mode?
- Which power enclosure is in a degraded state?
- Which fan, net connector, temperature sensor, fuse in the enclosure is currently unavailables?

The sections that follow will discuss each layer of Figure 1 in more detail.

1.1 The Blade Enclosure Layer

Using the tests mapped to this layer, you can determine what the blade enclosure contains and also detect failures of critical enclosure components such as fans, fuses, and temperature sensors.

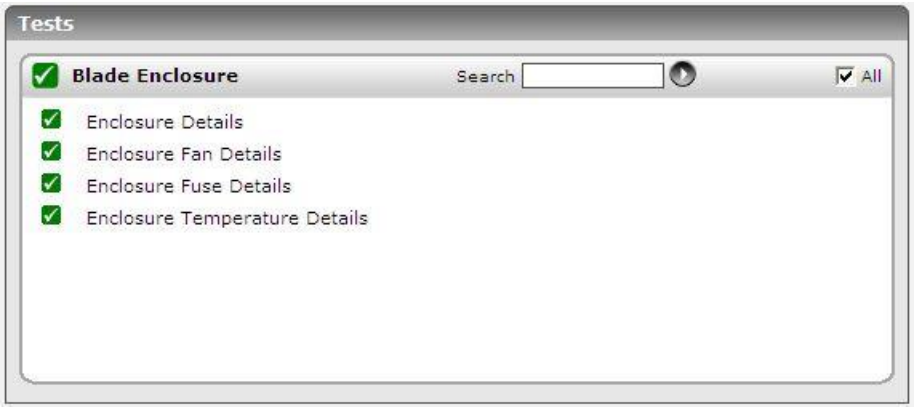

Figure 2: The tests mapped to the Blade Enclosure layer

1.1.1 Enclosure Details Test

A blade enclosure, which can hold multiple blade servers, provides services such as power, cooling, networking, various interconnects and management—though different blade providers have differing principles around what to include in the blade itself (and sometimes in the enclosure altogether).

This test monitors each blade enclosure, and reports its current state and its contents.

Purpose	Monitors each blade enclosure, and reports its current state and its contents
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results the enclosure of the HP Blade server 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>Enclosure condition:
Indicates the current conditions of the enclosure.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:
<table>
<tr><th>Value</th><th>State</th><th>Description</th></tr>
<tr><td>1</td><td>Other</td><td>No temperature sensors, fans, or fuses in the enclosure or the state could not be determined.</td></tr>
<tr><td>2</td><td>OK</td><td>All temperature sensors, fans, and fuses are within the normal operating range</td></tr>
<tr><td>3</td><td>Degraded</td><td>One or more temperature sensors, fans, or fuses are outside of the normal operating range, but none failed.</td></tr>
<tr><td>4</td><td>Failed</td><td>The temperature sensor exceeded the critical threshold value, a required fan has failed, or a fuse has been tripped. The system will automatically shutdown if the failed condition results.</td></tr>
</table></td></tr>
<tr><td></td><td>Does enclosure have a blade?
Indicates whether the enclosure has server blades or not.</td><td>Number</td><td>If the enclosure consists of one/more server blades, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any blades.</td></tr>
</table>

	Does enclosure have power? Indicates whether the enclosure contains power supply units or not.	Number	If the enclosure consists of one/more power supply units, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any power supply units.
	Does enclosure have temperature sensor? Indicates whether the enclosure contains temperature sensors or not.	Number	If the enclosure consists of one/more temperature sensors, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any temperature sensors.
	Does enclosure have net connector? Indicates whether the enclosure contains net connectors or not.	Number	If the enclosure consists of one/more net connectors, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any net connectors.
	Does enclosure have a fan? Indicates whether the enclosure contains fans or not.	Number	If the enclosure consists of one/more fans, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any fans.
	Does enclosure have a fan? Indicates whether the enclosure contains fans or not.	Number	If the enclosure consists of one/more fans, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any fans.
	Does enclosure have a fuse? Indicates whether the enclosure contains fuses or not.	Number	If the enclosure consists of one/more fuses, then this measure will report the value 1. The value 0 on the other hand indicates that the enclosure does not have any fuses.

1.1.2 Enclosure Fan Details Test

This test auto-discovers the fans in each blade enclosure, and reports the availability and current state of each fan.

Purpose	Monitors each blade enclosure, and reports its current state and its contents
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each fan in the enclosure of the HP Blade server 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>Is fan present?:
Indicates the availability of this fan.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:
<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>Absent</td></tr><tr><td>3</td><td>Present</td></tr></table></td></tr>
<tr><td></td><td>Fan condition:
Indicates the current condition of this fan.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:
<table><tr><th>Value</th><th>State</th><th>Description</th></tr><tr><td>1</td><td>Other</td><td>Fan status detection not supported</td></tr><tr><td>2</td><td>OK</td><td>The fan is working properly</td></tr><tr><td>3</td><td>Degraded</td><td>The redundant fan is not operating properly</td></tr><tr><td>4</td><td>Failed</td><td>The non-redundant fan is not operating properly</td></tr></table></td></tr>
</table>

1.1.3 Enclosure Fuse Details Test

This test auto-discovers the fuses in each blade enclosure, and reports the availability and current state of each fuse.

Purpose	Auto-discovers the fuses in each blade enclosure, and reports the availability and current state of each fuse
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each fuse in the enclosure of the HP Blade server 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>Is fuse present?:
Indicates the availability of this fuse.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>Absent</td></tr><tr><td>3</td><td>Present</td></tr></table></td></tr>
<tr><td></td><td>Fuse condition:
Indicates the current condition of this fuse.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:<table><tr><th>Value</th><th>State</th><th>Description</th></tr><tr><td>1</td><td>Other</td><td>Fuse status detection not supported</td></tr><tr><td>2</td><td>OK</td><td>The fuse is working properly</td></tr><tr><td>3</td><td>Failed</td><td>The fuse is not operating properly</td></tr></table></td></tr>
</table>

1.1.4 Enclosure Temperature Details Test

This test auto-discovers the temperature sensors in each blade enclosure, and reports the current temperature reading and current state of each sensor.

Purpose	Auto-discovers the temperature sensors in each blade enclosure, and reports the current temperature reading and current state of each sensor
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each temperature sensor in the blade 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>Current temperature of enclosure:
Indicates the current temperature reading for this sensor.</td><td>Celsius</td><td>By comparing the value of this measure across sensors, you can accurately determine which sensor is currently experiencing abnormally high temperatures. The value -1 for this measure indicates that the eG agent could not determine the temperature of the sensor.</td></tr>
<tr><td></td><td>Temperature condition of enclosure:
Indicates the current condition of this sensor.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:
<table>
<tr><th>Value</th><th>State</th><th>Description</th></tr>
<tr><td>1</td><td>Other</td><td>Temperature could not be detected</td></tr>
<tr><td>2</td><td>OK</td><td>The temperature sensor is within the normal operating range</td></tr>
<tr><td>3</td><td>Degraded</td><td>The temperature sensor is outside of the normal operating range</td></tr>
<tr><td>4</td><td>Failed</td><td>The temperature sensor detects a condition that could possibly damage the system. The system will automatically shutdown if the failed condition results.</td></tr>
</table></td></tr>
</table>

1.2 The Network Layer

The availability of the blade server over the network, its responsiveness to requests, the speed and bandwidth usage of each network interface supported by the blade server, and the overall health of network connections to and from the server can be determined using the tests mapped to this layer.

Figure 3: The tests mapped to the Network layer

Since the *Monitoring Unix and Windows Servers* and the *Monitoring Network Elements* documens discuss both the tests mapped to this layer at great length, let us proceed to the next layer.

1.3 The Blade Rack Layer

This layer focuses on the rack blades within an enclosure. Besides reporting the current status of each rack blade, this layer reveals the following:

- The current condition of each power enclosure supported by the rack blades;
- Issues experienced by every power supply unit in each rack blade
- The current state and conditon of the network connector

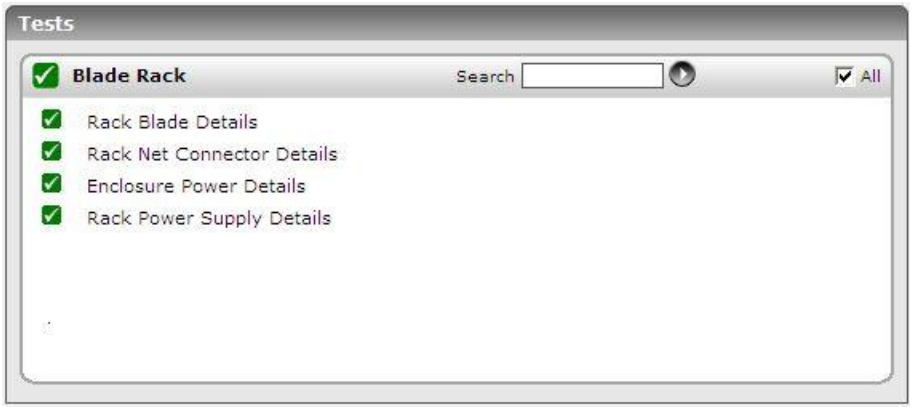

Figure 4: The tests mapped to the Blade Rack layer

1.3.1 Rack Blade Details Test

This test auto-discovers the rack blades and reports the current status of each blade. In addition, this test reports the current health, power supply status and LED status of each rack blade. Using this test, administrators can easily identify the blades that are malfunctioning and replace them. Also, faulty LEDs can also be identified and replaced at the earliest.

Purpose	Auto-discovers the rack blades and reports the current status of each blade
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Test period** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each blade in the blade 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>Is blade server available?:
Indicates the current status of this rack blade.</td><td></td><td>The table below lists the values that this measure can report, and the states they indicate:
<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>Absent</td></tr><tr><td>3</td><td>Present</td></tr></table>
Note:
By default, this measure can report the States mentioned above while indicating the current status of this rack blade. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td></td><td>Blade server health status:
Indicates the current health of this rack blade.</td><td></td><td>The table below lists the values that this measure can report, and the states they indicate:
<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>OK</td></tr><tr><td>3</td><td>Degraded</td></tr><tr><td>4</td><td>Failed</td></tr></table>
Note:
By default, this measure can report the States mentioned above while indicating the current health of this rack blade. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

	Blade server power status: Indicates the current power status of this rack blade.		The values that this measure can report and the numeric values they indicate are listed in the table below: **Numeric Value** / **State** 1 – Other 2 – On 3 – Off 4 – Power staged off **Note:** By default, this measure can report the **State**s mentioned above while indicating the current power status of this rack blade. However, the graph of this measure is indicated using the numeric equivalents.
	Blade server LED status: Indicates the current LED status of this rack blade.		The values that this measure can report and the numeric values they indicate are listed in the table below: **Numeric Value** / **State** 1 – Other 2 – None 3 – LED On 4 – LED Off **Note:** By default, this measure can report the **State**s mentioned above while indicating the current LED status of this rack blade. However, the graph of this measure is indicated using the numeric equivalents.

1.3.2 Rack Net Connector Details

This test auto-discovers the net connectors supported by each rack blade, and reports the type and current condition of every net connector.

Purpose	Auto-discovers the net connectors supported by each rack blade, and reports the

	type and current condition of every net connector
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for each net connector supported by the rack blades in an enclosure		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Net connector type: Indicates the type of this net connector.	Number	The table below lists the values that this measure can report, and the states they indicate: **Value** / **State** 1 / Other 2 / Passive 3 / Active
	Is net connector present? Indicates the availability of this net connector.	Number	The table below lists the values that this measure can report and the states they indicate: **Value** / **State** 1 / Other 2 / Absent 3 / Present

1.3.3 Enclosure Power Details

This test auto-discovers the power enclosures of each rack blade and reports the availability, condition, and redundant state of each enclosure.

Purpose	Auto-discovers the power enclosures of each rack blade and reports the availability, condition, and redundant state of each enclosure
Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every power enclosure of every rack blade</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>Power enclosure state:
Indicates whether this power enclosure is currently in a load-balanced state or not.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:
<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>Not load balanced</td></tr><tr><td>3</td><td>Load balanced</td></tr></table></td></tr>
<tr><td></td><td>Is power redundancy enabled?
Indicates the redundant state of this power enclosure.</td><td>Number</td><td>The table below lists the values that this measure can report and the states they indicate:
<table><tr><th>Value</th><th>State</th><th>Description</th></tr><tr><td>1</td><td>Other</td><td>The power enclosure condition could not be determined</td></tr><tr><td>2</td><td>OK</td><td>The power enclosure is operating normally</td></tr><tr><td>3</td><td>Degraded</td><td>The power enclosure is in a degraded state. The power subsystem may not be load balanced or may have lost redundancy</td></tr></table></td></tr>
</table>

1.3.4 Rack Power Supply Details

This test monitors every power supply unit in each rack blade of a blade server, and reports the availability, operational status, and current power of each unit.

Purpose	Monitors every power supply unit in each rack blade of a blade server, and reports the availability, operational status, and current power of each unit

Target of the test	A HP Blade server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161. 4. **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. 5. **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. 6. **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. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every power supply unit in each rack blade of a blade server</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>Rack power supply status:
Indicates the current status of this power supply unit.</td><td>Number</td><td>The table below lists the values that this measure can report, and the states they indicate:
<table>
<tr><th>Value</th><th>State</th></tr>
<tr><td>1</td><td>noError</td></tr>
<tr><td>2</td><td>generalFailure</td></tr>
<tr><td>3</td><td>bistFailure</td></tr>
<tr><td>4</td><td>fanFailure</td></tr>
<tr><td>5</td><td>tempFailure</td></tr>
<tr><td>6</td><td>interlockOpen</td></tr>
<tr><td>7</td><td>epromFailed</td></tr>
<tr><td>8</td><td>vrefFailed</td></tr>
<tr><td>9</td><td>dacFailed</td></tr>
<tr><td>10</td><td>ramTestFailed</td></tr>
<tr><td>11</td><td>voltageChannelFailed</td></tr>
<tr><td>12</td><td>orringdiodeFailed</td></tr>
<tr><td>13</td><td>brownOut</td></tr>
<tr><td>14</td><td>giveupOnStartup</td></tr>
<tr><td>15</td><td>nvramInvalid</td></tr>
<tr><td>16</td><td>calibrationtableInvalid</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>Rack input line status:
Indicates the current status of the input line of this power supply unit.</td><td>Number</td><td>The table below lists the values that this measure can report and the states they indicate:
<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>noError</td></tr><tr><td>2</td><td>lineOverVoltage</td></tr><tr><td>3</td><td>LineUnderVoltage</td></tr><tr><td>4</td><td>lineHit</td></tr><tr><td>5</td><td>brownOut</td></tr><tr><td>6</td><td>linePowerLoss</td></tr></table></td></tr>
<tr><td></td><td>Max rack power:
Indicates the maximum power output of this power supply unit.</td><td>Watts</td><td></td></tr>
<tr><td></td><td>Current rack power:
Indicates the current power output of this power supply unit.</td><td>Watts</td><td>By comparing the value of this measure across power supply units, you can quickly identify the unit that is producing the maximum power output currently, and the rack blade with which it is associated.</td></tr>
<tr><td></td><td>Is rack power supply present?
Indicates the availability of this power supply unit.</td><td>Number</td><td>The table below lists the values that this measure can report and the states they indicate:
<table><tr><th>Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>Absent</td></tr><tr><td>3</td><td>Present</td></tr></table></td></tr>
</table>

<table>
<tr>
<td></td>
<td>Power supply condition:

Indicates the current condition of this power supply unit.</td>
<td>Number</td>
<td>The table below lists the values that this measure can report and the states they indicate:
<table>
<tr><th>Value</th><th>State</th><th>Description</th></tr>
<tr><td>1</td><td>Other</td><td>The status could not be determined or not present</td></tr>
<tr><td>2</td><td>OK</td><td>The status could not be determined or not present</td></tr>
<tr><td>3</td><td>Degraded</td><td>A temperature sensor, fan or other power supply component is outside of normal operating range</td></tr>
<tr><td>4</td><td>Failed</td><td>A power supply component detects a condition that could possibly damage the system</td></tr>
</table>
</td>
</tr>
</table>

Chapter 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 **HP Blade Servers**. 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.