Monitoring HP Blade Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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. This is where eG Enterprise lends helping hands to administrators.

Chapter 2: How to Monitor HP Blade Server Using eG Enterprise?

eG Enterprise monitors the HP Blade server in an agentless manner. For this purpose, eG Enterprise deploys a **remote agent** and an **external agent**. For collecting performance statistics, eG agent uses the SNMP MIB of the HP Blade to pull out the metrics pertaining to the performance of the HP Blade.

The broad steps for monitoring the HP Blade using eG Enterprise are as follows:

- Managing the HP Blade Server
- Configuring the tests

These steps have been discussed in following sections.

2.1 Managing the HP Blade Server

The eG Enterprise cannot automatically discover the HP Blade. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a HP Blade, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *HP Blade* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

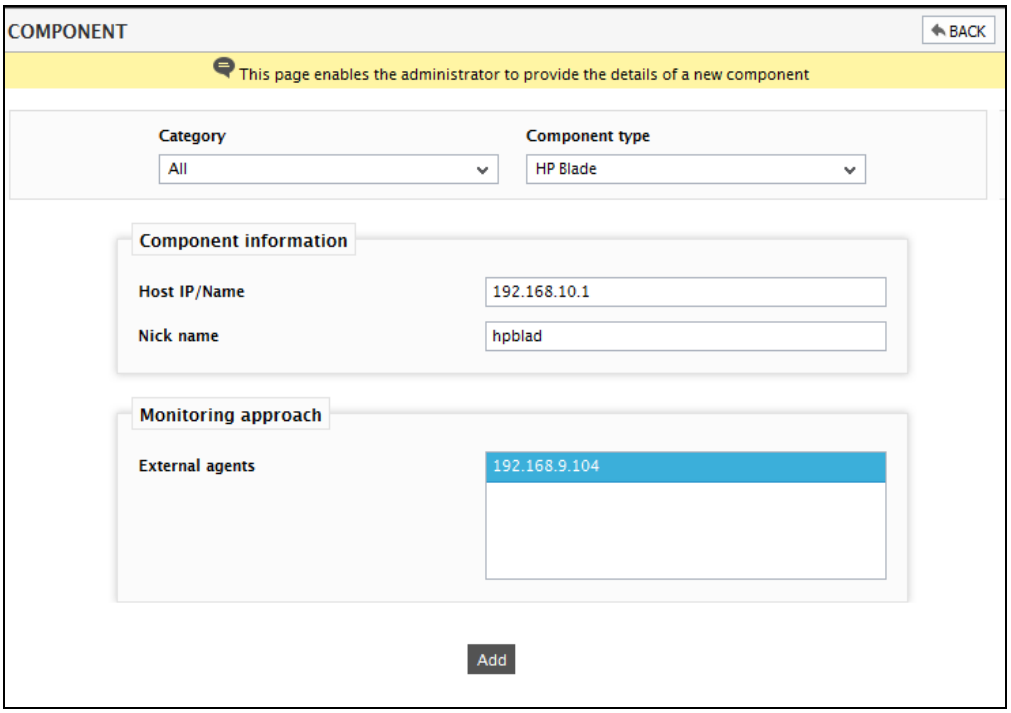

Figure 2.1: Adding a HP Blade

4. Specify the **Host IP** and the **Nick name** of the HP Blade in Figure 2.1. Then, click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

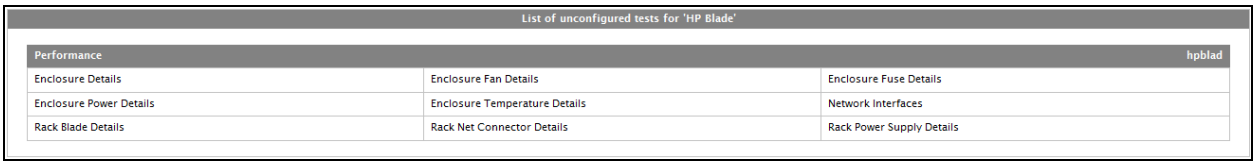

Figure 2.2: List of Unconfigured tests to be configured for the HP Blade

2. Click on the test names to configure. To know how to configure the tests, refer to **Monitoring the HP Blade Servers**.
3. Next, try to signout of the eG administrative interface, now you will be prompted to configure the **Network Interfaces** test. To know how to configure the **Netwok Interfaces** test, refer to *Monitoring Cisco Router* document.
4. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the HP Blade Servers

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.

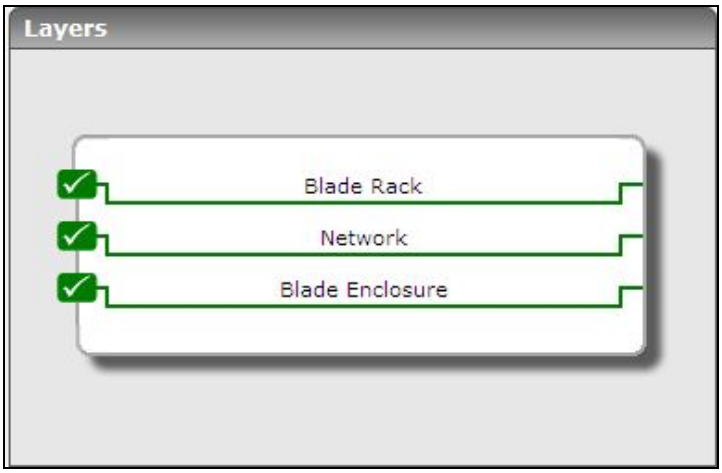

Figure 3.1: The layer model of the HP Blade Server

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 unavailable?

The sections that follow will discuss each layer of the layer model in more detail.

3.1 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.

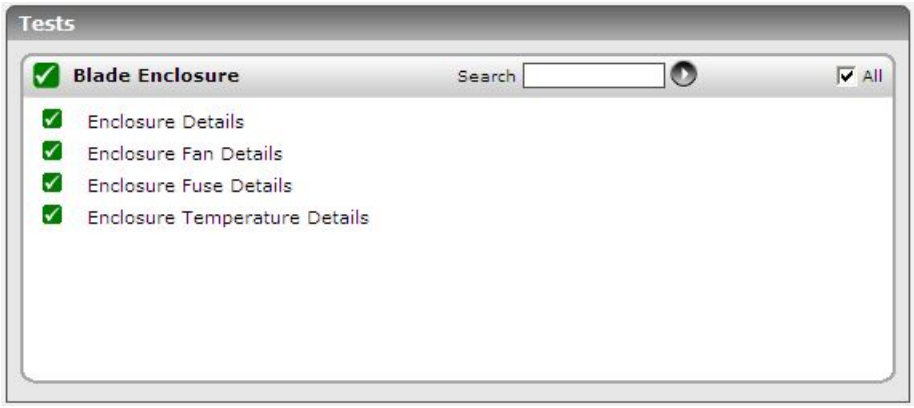

Figure 3.2: The tests mapped to the Blade Enclosure layer

3.1.1 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.

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results the enclosure of the HP Blade server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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

Parameter	Description
	transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Enclosure condition	Indicates the current conditions of the enclosure.	Number	The table below lists the values that this measure can report, and the states they indicate:

Measurement	Description	Measurement Unit	Interpretation

Value	State	Description
1	Other	No temperature sensors, fans, or fuses in the enclosure or the state could not be determined.
2	OK	All temperature sensors, fans, and fuses are within the normal operating range
3	Degraded	One or more temperature sensors, fans, or fuses are outside of the normal operating range, but none failed.
4	Failed	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

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Value</th><th>State</th><th>Description</th></tr><tr><td></td><td></td><td>failed condition results.</td></tr></table>
Does enclosure have a blade?	Indicates whether the enclosure has server blades or not.	Number	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.
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.

Measurement	Description	Measurement Unit	Interpretation
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.

3.1.2 Enclosure Fan Details Test

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

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for each fan in the enclosure of the HP Blade server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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

Parameter	Description
	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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.

Parameter	Description
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Is fan present?</td><td>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>Fan condition</td><td>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></table></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Value: 3, State: Degraded, Description: The redundant fan is not operating properly Value: 4, State: Failed, Description: The non-redundant fan is not operating properly

3.1.3 Enclosure Fuse Details Test

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

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for each fuse in the enclosure of the HP Blade server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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

Parameter	Description
	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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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

Parameter	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Is fuse present?</td><td>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>Fuse condition</td><td>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>

3.1.4 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.

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for each temperature sensor in the blade enclosure being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a

Parameter	Description
	contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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

Parameter	Description
	to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current temperature of enclosure	Indicates the current temperature reading for this sensor.	Celsius	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.
Temperature condition of enclosure	Indicates the current condition of this sensor.	Number	The table below lists the values that this measure can report, and the states they indicate:

Value	State	Description
1	Other	Temperature could not be detected
2	OK	The temperature sensor is within the normal operating range
3	Degraded	The temperature sensor is outside of the normal operating range
4	Failed	The temperature sensor detects a condition that could pos-

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Value</th><th>State</th><th>Description</th></tr><tr><td></td><td></td><td>sibly damage the system. The system will auto-matically shut-down if the failed con-dition results.</td></tr></table>

3.2 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 3.3: The tests mapped to the Network layer

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

3.3 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 condition of the network connector

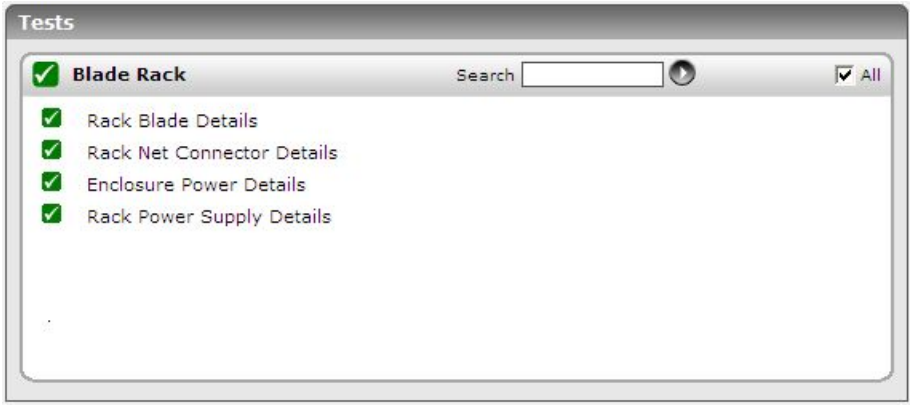

Figure 3.4: The tests mapped to the Blade Rack layer

3.3.1 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.

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for each blade in the blade enclosure being monitored .

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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

Parameter	Description
	environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.

Parameter	Description
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is blade server available?	Indicates the current status of this rack blade.		The table below lists the values that this measure can report, and the states they indicate: Value / State: 1 – Other; 2 – Absent; 3 – Present **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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Blade server health status</td><td>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>
<tr><td>Blade server power status</td><td>Indicates the current power status of this rack blade.</td><td></td><td>The values that this measure can report and the numeric values they indicate are listed in the table below:
<table><tr><th>Numeric Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>On</td></tr><tr><td>3</td><td>Off</td></tr><tr><td>4</td><td>Power staged off</td></tr></table>
Note:
By default, this measure can report the States mentioned above while indicating the current power status of this rack blade. However, the graph of</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Blade server LED status</td><td>Indicates the current LED status of this rack blade.</td><td></td><td>The values that this measure can report and the numeric values they indicate are listed in the table below:
<table><tr><th>Numeric Value</th><th>State</th></tr><tr><td>1</td><td>Other</td></tr><tr><td>2</td><td>None</td></tr><tr><td>3</td><td>LED On</td></tr><tr><td>4</td><td>LED Off</td></tr></table>
Note:
By default, this measure can report the States mentioned above while indicating the current LED status of this rack blade. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.3.2 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.

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for each net connector supported by the rack blades in an enclosure.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.

Parameter	Description
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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

Parameter	Description
	• **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	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: 1 – State: Other

Measurement	Description	Measurement Unit	Interpretation
			Value: 2 — State: Passive Value: 3 — State: 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: 1 — State: Other Value: 2 — State: Absent Value: 3 — State: Present

3.3.3 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.

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for every power enclosure of every rack blade.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This

Parameter	Description
	parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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

Parameter	Description
	encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Power enclosure state	Indicates whether this power enclosure is currently in a load-balanced state or not.	Number	The table below lists the values that this measure can report, and the states they indicate: Value: 1 – State: Other Value: 2 – State: Not load balanced Value: 3 – State: Load balanced
Is power redundancy enabled?	Indicates the redundant state of this power enclosure.	Number	The table below lists the values that this measure can report and the states they indicate:

Measurement	Description	Measurement Unit	Interpretation
			<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>

3.3.4 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.

Target of the test : A HP Blade server

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for every power supply unit in each rack blade of a blade server.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the storage device for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by

Parameter	Description
	default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Rack power supply status	Indicates the current status of this power supply unit.	Number	The table below lists the values that this measure can report, and the states they indicate: Value: 1 – State: noError Value: 2 – State: generalFailure Value: 3 – State: bistFailure Value: 4 – State: fanFailure

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Value</th><th>State</th></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>
<tr><td>Rack input line status</td><td>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>Max rack power</td><td>Indicates the maximum power output of this power supply unit.</td><td>Watts</td><td></td></tr>
<tr><td>Current rack power</td><td>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>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Is rack power supply present?</td><td>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>
<tr><td>Power supply condition</td><td>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>

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.