Monitoring IBM BladeCenter Chassis

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: HOW TO MONITOR IBM BLADECENTER CHASSIS USING EG ENTERPRISE 2

2.1 Managing IBM BladeCenter Chassis 2

CHAPTER 3: MONITORING IBM BLADECENTER CHASSIS 5

3.1 The IBMBlade Hardware Layer 6

3.1.1 Chassis Fanpack Test 6

3.1.2 Chassis Power Module Test 10

3.1.3 Chassis Temperature Test 14

3.1.4 Fuel Gauge Test 16

3.2 The IBM Chassis LED Layer 20

3.2.1 Blade LED Test 20

3.2.2 Blower LED Test 25

3.2.3 FrontPanel LED Test 29

3.3 The IBMBlade Chassis Layer 32

3.3.1 System Health Test 33

3.3.2 User Details Test 35

ABOUT EG INNOVATIONS 39

Table of Figures

Figure 2.1: Adding the IBM Blade Chassis component 3
Figure 2.2: A list of tests that need to be configured for the IBM Blade Chassis 3
Figure 3.1: The layer model of the IBM BladeCenter Chassis 5
Figure 3.2: The tests mapped to the IBMBlade Hardware layer 6
Figure 3.3: The tests mapped to the IBMBlade Chassis LED layer 20
Figure 3.4: The tests mapped to the IBMBlade Chassis layer 33

Chapter 1: Introduction

The IBM BladeCenter Chassis unit is a high-density, high-performance, rack-mounted blade server system. The IBM BladeCenter Chassis is specifically developed for medium-to-large businesses, NEBS telecommunications network applications and other applications requiring physical robustness. The BladeCenter chassis can accommodate multiple blades that share common resources, such as power, cooling, management, and I/O resources.

In order to be able to carry out the designated task smoothly, the blade servers should receive adequate support from the chassis components such as the fans, power modules, management modules etc. In other words, an unexpected failure of the power modules or a sudden increase in the temperature, can affect the operations of not just one, but all the blade servers within the chassis. This in turn adversely affects the performance of the IBM BladeCenter Chassis. To avoid such eventualities, the chassis and its core components have to be continuously monitored. This is where eG Enterprise lends helping hands to administrators.

Chapter 2: How to Monitor IBM BladeCenter Chassis Using eG Enterprise

eG enterprise monitors the IBM BladeCenter Chassis in an agentless manner. For this purpose, you can deploy a single eG agent on a remote Windows host. This agent executes various tests that connect to the SNMP MIB of the chassis to be monitored, and collects critical statistics of interest. To enable the eG agent to access the SNMP MIB, specify the following while configuring the tests:

- Port number on which the target chassis exposes its MIB
- SNMP community to be used for accessing the MIB

To start monitoring the target chassis, first manage the *IBM Blade Chassis* component using the steps explained in the section below.

2.1 Managing IBM BladeCenter Chassis

Using eG Enterprise, you can auto-discover the IBM BladeCenter Chassis as well as manually add the component for monitoring. To manage an *IBM Blade Chassis* component, do the following:

1. Log into the eG admin interface.
2. If the IBM BladeCenter Chassis is already discovered, then directly proceed towards managing it using the **Components – Manage/Unmanage/Delete** page.
3. However, if the target chassis is yet to be discovered, then run discovery (Infrastructure -> Components -> Discovery) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **Components** page. Remember that components manually added are managed automatically.
4. In the **Components** page that appears next, select *IBM Blade Chassis* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

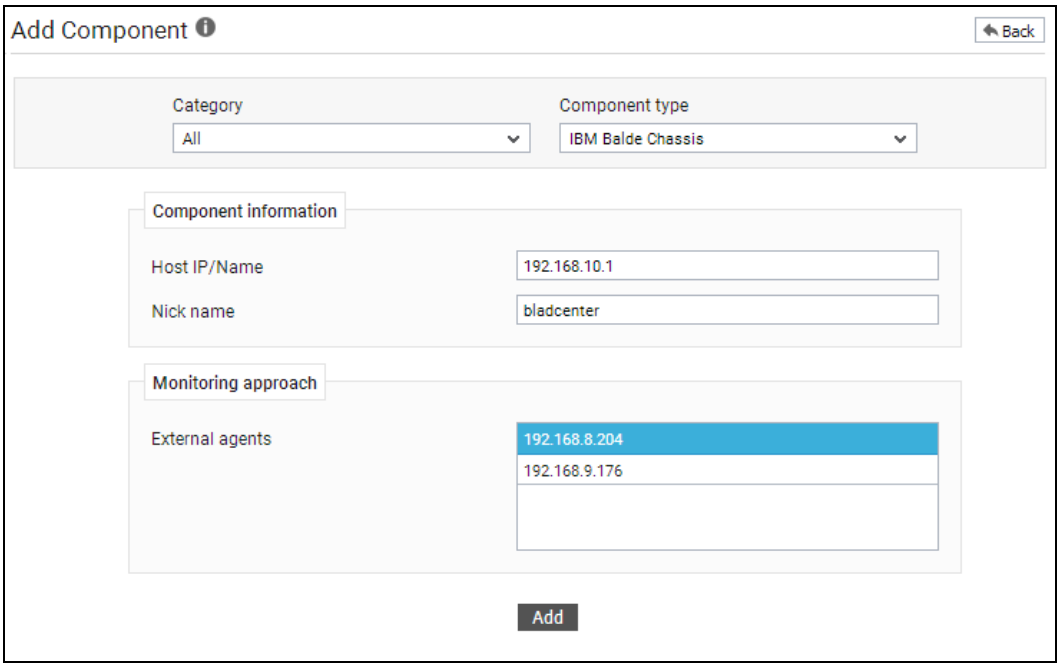

Figure 2.1: Adding the IBM Blade Chassis component

5. Specify the **Host IP/Name** and the **Nick name** for the *IBM Blade Chassis* component.
6. Choose an external agent for the target chassis by picking an option from the **External agents** list box.
7. Then, click the **Add** button to register the changes (see Figure 2.1).
8. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

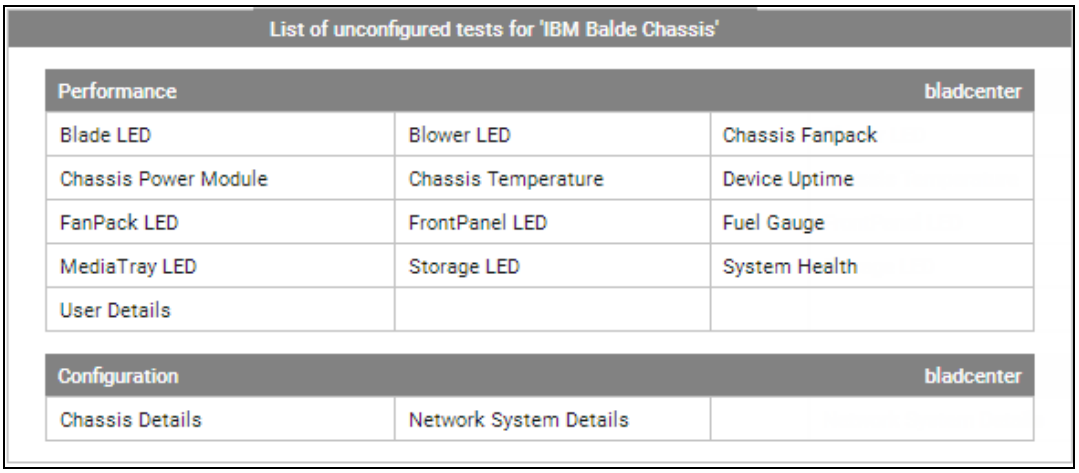

Figure 2.2: A list of tests that need to be configured for the IBM Blade Chassis

9. Click on any test in the list of unconfigured tests to configure. To know how to configure the tests, refer to **Monitoring IBM BladeCenter Chassis**.
10. Finally, signout of the eG admin interface.

Chapter 3: Monitoring IBM BladeCenter Chassis

eG Enterprise offers a specialized IBM BladeCenter Chassis monitoring model that monitors the core hardware components of the target BladeCenter Chassis, and proactively alerts administrators to issues in its overall health and performance. This way, the abnormalities can be fixed before irreparable damage occurs.

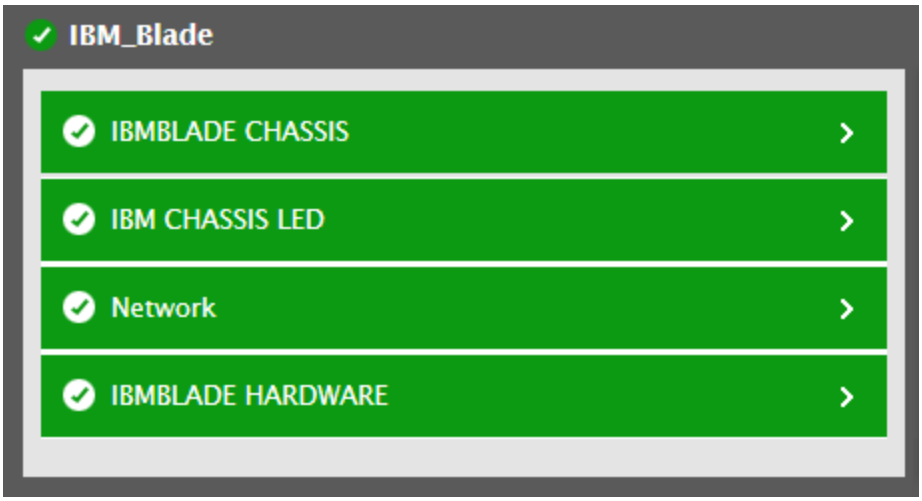

Figure 3.1: The layer model of the IBM BladeCenter Chassis

By continuously monitoring the IBM BladeCenter Chassis, administrators can accurately find out the answers the following performance questions:

- What is the current status of the chassis?
- What is the current health and power supply status of each blade?
- Does the blower module exist?
- What is the current status of each power module?
- Does the fanpack exist?
- What is the current status of error LED of the fanpack?
- What is the current temperature of the management module?
- What is the current temperature and error LED status of the front panel?
- Does the storage module exist?
- What is the current status of error LED of the storage module?

- Does the MediaTray exist?
- What is the current status of error LED of the MediaTray?
- What is the current status of each power domain?
- How much power is utilized from each power domain?

Since the tests of the **Network** layer have already been discussed in the *Monitoring Cisco Router* document in detail, the sections to come will discuss all other layers of Figure 3.1 in detail.

3.1 The IBMBlade Hardware Layer

The tests mapped to this layer help administrators to find out the status of fanpack and power modules and also detect the temperature of the core components of the target chassis. In addition, administrators can also determine the amount of power utilized from the power domains of the chassis.

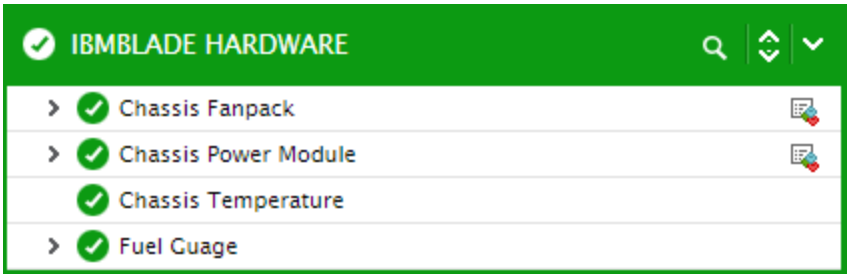

Figure 3.2: The tests mapped to the IBMBlade Hardware layer

3.1.1 Chassis Fanpack Test

The IBM BladeCenter Chassis comes with four hot-swappable fan modules (fan packs). The fan modules are designed to provide cooling airflow to the chassis and other modules. Each fan module contains two fans. These fan modules ensure that the temperature of the target chassis is within a permissible level. If any of the fan modules are not working properly or become unavailable suddenly, then the temperature of the chassis cannot be automatically regulated. This may cause the internal temperature of the chassis to rise uncontrollably, resulting in considerable damage to the modules in the chassis. This is why, the availability of the fan modules should be verified time and again, and abnormalities (if any) should be escalated to administrators. This is exactly what the **Chassis Fanpack** test does!

This test auto-discovers the fan modules of the target chassis and reports the availability and current status of each fan module. In addition, the test also checks the number of fans in each fan module

and the average speed of the fan modules. This way, it turns the spotlight on those fan modules that are not operating within the permissible range.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan module in the BladeCenter chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
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 target host. 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

Parameter	Description
	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 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 exist?</td><td>Indicates whether this fan module exists or not.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above indicating whether each fan module exists or not. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>State</td><td>Indicates the current status of this fan module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Good</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Bad</td><td>3</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of each fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Controller state</td><td>Indicates the current status of controller of this</td><td></td><td>The values that this measure can report and the numeric values they indicate</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>fan module.</td><td></td><td>have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Operational</td><td>0</td></tr><tr><td>Flashing</td><td>1</td></tr><tr><td>Not present</td><td>2</td></tr><tr><td>Communication error</td><td>3</td></tr><tr><td>Unknown</td><td>255</td></tr></table>Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of the controller of each fan module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Fan Count</td><td>Indicates the number of fans in this fan module.</td><td>Number</td><td></td></tr>
<tr><td>Average speed</td><td>Indicates the average speed that this fan module can operate.</td><td>Rpm</td><td>The value of this measure should be within the permissible range. It is a cause for concern if the permissible range is violated for any reason.</td></tr>
</table>

3.1.2 Chassis Power Module Test

The BladeCenter Chassis comes with two or four hot-swap power modules. The availability and proper functioning of each of the power modules is critical to the uninterrupted operations of the chassis. Frequent erratic voltage fluctuations or failures of the power supply modules can stall the operations for hours, slowing down or completely suspending the delivery of the dependent business services. If such an unpleasant eventuality is to be pre-empted, administrators should proactively detect potential problems with the power supply modules and take remedial action before anything untoward happens. The **Chassis Power Module** test helps administrators in this regard!

For each power supply module on the target BladeCenter chassis, this test reports the availability and current status. Using this test, administrators can prevent failures of the power supply modules at the earliest and rectify failures before the operation of the target chassis is completely affected.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for each power supply module on the BladeCenter Chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host 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 target host. 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

Parameter	Description
	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 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 exist?</td><td>Indicates whether this power supply module exists or not.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above indicating whether each power supply module exists or not. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>State</td><td>Indicates the current status of this power supply module.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Good</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Not Available</td><td>3</td></tr><tr><td>Critical</td><td>4</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of each power supply module. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.1.3 Chassis Temperature Test

Hardware components in the BladeCenter Chassis are configured to operate within a certain temperature range. When the temperature of components suddenly soars/drops for any abnormal reason, temperature of the chassis will also rise/drop beyond a permissible limit. This in turn will fatally damage the hardware components of the target chassis. This is why, it is important for administrators to periodically check the temperature of the components in the chassis. This can be easily done using the **Chassis Temperature** test!

This test monitors the core components of the chassis and reports the current temperature of the management modules and front panels.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for the target chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host 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 target host. 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

Parameter	Description
	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.
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

Parameter	Description
	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
Management module temperature	Indicates the current temperature of the management module.	Celsius	The value of this measure should be within the permissible range. Sudden spikes in the value of this measure indicates abnormal rise/drop in the temperature of the management module. This in turn may affect the operations of the target chassis.
Front panel temperature	Indicates the current temperature of the front panel1.	Celsius	The value of this measure should be within the permissible range. A significant rise/drop in the value of this measure is a cause for concern.
Front panel2 temperature	Indicates the current temperature of the front panel2.	Celsius	The value of this measure should be within the permissible range. A significant rise/drop in the value of this measure is a cause for concern.

3.1.4 Fuel Gauge Test

To manage the power consumption of the components of the target chassis and provide power redundancy during failures, administrators create two power domains using the advanced management module Web interface. Each power domain is allocated with a specific amount of power which will be shared among the chassis components. The chassis components in each power domain are grouped based on their types and estimated power consumption. The power domains should be able to supply the adequate amount of power to power-on and ensure smooth functioning

of the chassis components such as blade servers. If the power domains run out of the allocated power, the chassis components may start to malfunction or shut-down completely, which in turn stalls the operations of the target chassis. To avoid such eventualities, administrators should be alerted to the power shortage immediately before the chassis operations shut down. This can be easily done using the **Fuel Gauge** test!

This test auto-discovers the power domains on the target chassis and for each power domain, reports the current status and power utilization, thus turning the spotlight on the power domain that is being over-utilized.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for each power domain in the BladeCenter chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
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 target host. 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

Parameter	Description
	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.
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

Parameter	Description
	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
State	Indicates the current status of this power domain.		The values that this measure can report and the numeric values they indicate have been listed in the table below: Measure Value / Numeric Value Good / 1 Warning / 2 Bad / 3 **Note:** By default, this measure can report the **Measure Value**s mentioned above while indicating the current status of each power domain. However, the graph of this measure is indicated using the numeric equivalents.
Total available power	Indicates the total amount of power that is available in this power domain.	Watts	Total power is calculated by the management module according to the rated capacities of the power modules that are installed in each power domain and the power-management policy that has been set for each power domain.
Reserved power	Indicates the amount of	Watts	

Measurement	Description	Measurement Unit	Interpretation
	power reserved for use by the components in this power domain.		
Available remaining power for use	Indicates the amount of power that is available for use in this power domain.	Watts	The value of this measure is calculated according to the *Total available power* and the *Reserved power* measures for each power domain.
Power in used	Indicates the amount of power that is being used in this power domain.	Watts	If the value of this measure is close to the value of the *Total available power* measure, it is a cause for a concern. Comparing the value of this measure across the power domains can help you instantly identify the power domain that is being over-utilized.
Remaining power to be utilized	Indicates the percentage of power that is available for use in this power domain.	Percent	

3.2 The IBM Chassis LED Layer

Using the tests mapped to this layer, administrators can find out whether the blade, blower and front panel exist or not and the status of the error LEDs on the blade, blower and front panel.

Figure 3.3: The tests mapped to the IBMBlade Chassis LED layer

3.2.1 Blade LED Test

The BladeCenter chassis contains multiple blade slots to accommodate blade servers, also called blades or server blades. The blades are independent servers containing one or more processors,

memory, disk storage, and network controllers. Each blade slot is designed with a set of LEDs to indicate the various states:

- Power - This green LED indicates the power status of the blade server
- Error or Fault - When this amber LED is lit, it indicates that a system error has occurred in the blade server. The blade-error LED turns off only after the error is corrected.
- Information - When this amber LED is lit, it indicates that information about a system event in the blade server has been placed in the Advanced-Management-Module event log.

Using these LEDs, administrators can find out the health, power state and errors (if any) of the blade slots at a single glance. Critical or fatal errors, power failures or connectivity failures of the blade slots can render the blades unavailable/inoperable. This in turn affects performance of the blades as well as the target chassis. To prevent such eventualities, it is imperative that administrators should closely monitor the blades and take immediate measures before the users complaint.

This test auto-discovers the blades on the target chassis and reports the availability and current health of each blade server. In addition, this test also reports the power supply status and the status of error LED of each blade.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
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 target host. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

Parameter	Description
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 encryption types:

Parameter	Description
	• **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 exist?	Indicates whether/not this blade slot exists.		The values that this measure can report and the numeric values they indicate have been listed in the table below: **Measure Value** / **Numeric Value**: Yes – 1; No – 0 **Note:** By default, this measure can report the **Measure Value**s mentioned above indicating whether each blade slot exists or not. However, the graph of this measure is indicated using the numeric equivalents.
Power state	Indicates the current power state of this blade		The values that this measure can report and the numeric values they indicate

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>slot.</td><td></td><td>have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr><tr><td>Standby</td><td>3</td></tr><tr><td>Hibernate</td><td>4</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of each blade slot . However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Health state</td><td>Indicates the current health of this blade slot.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Good</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Critical</td><td>3</td></tr><tr><td>Kernal mode</td><td>4</td></tr><tr><td>Discovering</td><td>5</td></tr><tr><td>Common Error</td><td>6</td></tr><tr><td>No Power</td><td>7</td></tr><tr><td>Flashing</td><td>8</td></tr><tr><td>Initialization Failure</td><td>9</td></tr><tr><td>Insufficient Power</td><td>10</td></tr><tr><td>Power Denied</td><td>11</td></tr></table></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>Note:

By default, this measure can report the Measure Values mentioned above while indicating the current health of each blade slot. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Error LED state</td><td>Indicates the current error LED state of this blade slot.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr></table>
Note:

By default, this measure can report the Measure Values mentioned above while indicating the current status of the error LED of each blade slot . However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
</table>

3.2.2 Blower LED Test

The BladeCenter chassis contains two hot-swap blowers for cooling redundancy. The blower speeds vary depending on the ambient air temperature at the front of the BladeCenter chassis and the temperature of core components. If the ambient temperature is 25°C (77°F) or below, the target chassis blowers run at their minimum rotational speed, increasing their speed as required to control internal temperature. If the ambient temperature is above 25°C (77°F), the blowers run faster, increasing their speed as required to control internal temperature. If the blowers stopped suddenly due to some fatal errors, the temperature of the core hardware components may suddenly soar, causing irreparable damage to those components. To avoid such failures, administrators should regularly check the availability and errors (if any) of the blowers. This is where the **Blower LED** test helps administrators.

This test auto-discovers the blowers on the target chassis and reports the availability and error LED status of each blower.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for each blower on the BladeCenter chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
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 target host. 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

Parameter	Description
	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 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 exist?</td><td>Indicates whether/not this blower exists.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above indicating whether each blower exists or not. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Error LED state</td><td>Indicates the current status of the error LED of this blower.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of the error LED of each blower. However, the graph of this measure is indicated using the numeric equivalents.
When the amber LED on a blower module is lit, it indicates an error detected in the blower or power to the blower is not present.</td></tr>
</table>

3.2.3 FrontPanel LED Test

The BladeCenter chassis contains the following LEDs in the front panel LED system:

- **Power-on :** This green LED is lit indicating that the BladeCenter chassis is powered on. This LED is turned off when the power subsystem, the ac power or the LED is failed, or the management module is unavailable or not functioning properly, or the media tray is not fully seated.
- **Attention :** If the power-on LED is off, it does not mean that the BladeCenter chassis has no power supply. The LED might be burned out. To remove all electrical current from the BladeCenter unit, you must disconnect all power cords from the BladeCenter unit.
- **Location :** When this blue LED is lit or flashing, it has been turned on by the system administrator to aid in visually locating the BladeCenter unit. If a blade server requires attention, the location LED on the blade server usually will also be lit. After the BladeCenter unit has been located, you can have the system administrator turn off the location LED.
- **Over-temperature :** When this amber LED is lit, the temperature in the BladeCenter unit exceeds the temperature limits, or a blade server reports an over-temperature condition. The BladeCenter unit might have already taken corrective action, such as increasing the blower speed. This LED turns off automatically when there is no longer an over-temperature condition.
- **Information :** When this amber LED is lit, a noncritical event has occurred that requires attention, such as the wrong I/O module inserted in a bay or power demands that exceed the capacity of power modules that are currently installed. The event is recorded in the event log. Check the LEDs on the BladeCenter unit and the blade servers to isolate the component. After the situation is corrected, have the system administrator turn off the information LED.
- **System-error :** When this amber LED is lit, it indicates that a system error has occurred, such as a failed module or a system error in a blade server. An LED on one of the components or on a blade server is also lit to further isolate the error.
- **Optical drive activity LED :** When this LED is lit, it indicates that the optical drive is in use.

Tracking the status of these LEDs, administrators can find out the power status, errors, temperature, etc. of the target chassis at a single glance. This can be easily done using the **FrontPanel LED** test! This test monitors the LEDs on the front panel of the chassis and reports the current status of temperature LED and error LED.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for the BladeCenter chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
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 target host. 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

Parameter	Description
	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 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
Temperature LED state	Indicates the current status of the temperature LED on the front panel.		The values that this measure can report and the numeric values they indicate have been listed in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr></table> **Note:** By default, this measure can report the **Measure Value**s mentioned above indicating the current status of the temperature LED on the front panel. However, the graph of this measure is indicated using the numeric equivalents.
Error LED state	Indicates the current status of the error LED on the front panel.		The values that this measure can report and the numeric values they indicate have been listed in the table below: <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr></table> **Note:** By default, this measure can report the **Measure Value**s mentioned above while indicating the current status of the error LED on the front panel. However, the graph of this measure is indicated using the numeric equivalents.

3.3 The IBMBlade Chassis Layer

Using the tests mapped to this layer, you can determine the health of the target chassis and also detect the number of users accessing the chassis.

Figure 3.4: The tests mapped to the IBMBlade Chassis layer

3.3.1 System Health Test

This test reports the current status of the target BladeCenter chassis. Using this test, administrators can easily find out whether/not the chassis is healthy, if not administrators can proactively take necessary actions before the target chassis fails.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for the BladeCenter Chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host 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 target host. 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

Parameter	Description
	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.
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

Parameter	Description
	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
State	Indicates the current status of the BladeCenter chassis.		The values that this measure can report and the numeric values they indicate have been listed in the table below: Measure Value / Numeric Value Critical – 0 Non Critical – 2 System Level – 4 Normal – 255 **Note:** By default, this measure can report the **Measure Value**s mentioned above while indicating the current status of the BladeCenter chassis. However, the graph of this measure is indicated using the numeric equivalents.

3.3.2 User Details Test

In the large environments, multiple users can be configured to access the chassis. Some times, administrators may wish to know the users who are currently accessing the chassis. Analyzing the user details, administrators can easily find out the current load on the chassis. This is where the

User Details test helps administrators! This test periodically reports the number of users accessing the chassis.

Target of the test : An IBM BladeCenter Chassis

Agent deploying the test : An external agent

Outputs of the test : One set of results for the BladeCenter chassis being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be *NULL*.
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 target host. 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

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

Parameter	Description
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total user	Indicates the total number of users accessing the blades in the chassis.	Number	This measure is a good indicator of the workload on the chassis. The detailed diagnosis of this measure reveals the user ID and the method through which the user accesses the chassis.

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.