Monitoring Fujitsu Primergy Rack Server

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The FUJITSU Server PRIMERGY RX rack systems are versatile rack-optimized servers providing best-in-class performance and energy efficiency, and thus form the “standard” in each datacenter.

In order to be highly efficient, the rack server should receive adequate support from the hardware components such as the fans, memory modules 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 the rack server. To avoid such eventualities, the core hardware components need to be continuously monitored. This is where eG Enterprise lends helping hands to the administrators.

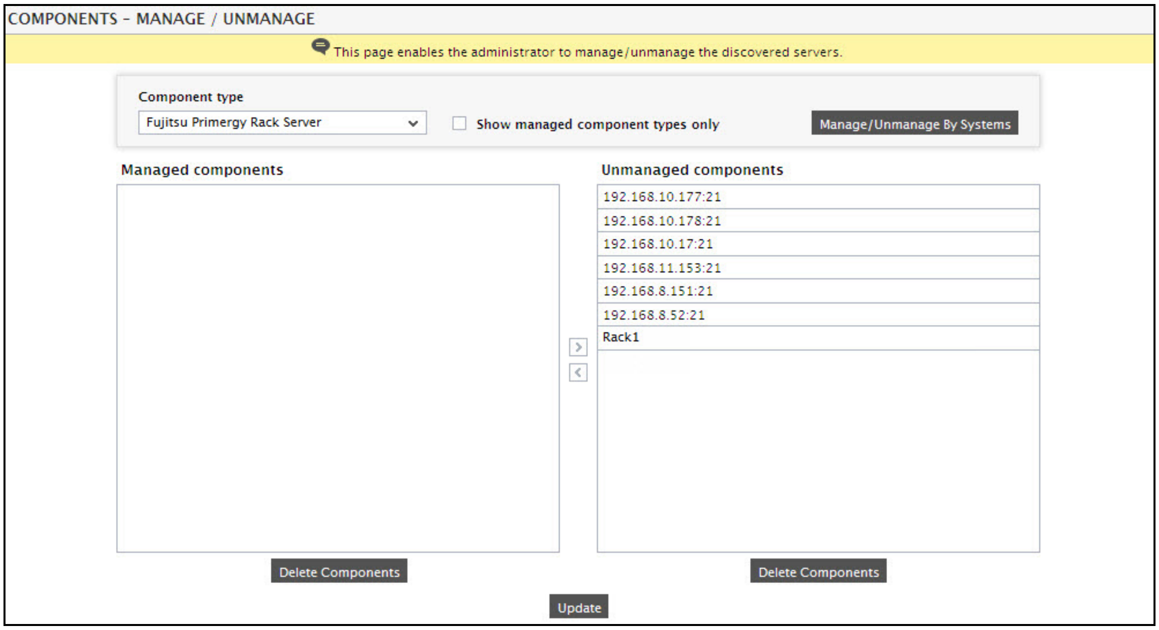
Chapter 2: How to Monitor Fujitsu Primergy Rack Server Using eG Enterprise?

eG Enterprise monitors the Fujitsu Primergy Rack Server in an *agentless* manner. For this purpose, the eG Enterprise employs an eG external agent on a remote Windows host. This agent polls the SNMP MIB of the switch to gather the statistics of interest at configured intervals. Before attempting to monitor the Fujitsu Primergy Rack Server, ensure that the Fujitsu Primergy Rack Server is SNMP-enabled.

2.1 Managing the Fujitsu Primergy Rack Server

eG Enterprise can automatically discover the Fujitsu Primergy Rack Server in the environment and also lets you to add the Fujitsu Primergy Rack Server component if the server is not auto-discovered. The following steps explain you how to manage the server that is auto-discovered using the eG administrative interface.

1. Log into the eG administrative interface.
2. If a Fujitsu Primergy Rack Server is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or add the component manually using the **COMPONENTS** page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are managed automatically. Discovered components, however, are managed using the **COMPONENTS – MANAGE / UNMANAGE** page.
4. To manage the Fujitsu Primergy Rack Server component that is auto-discovered, follow the Infrastructure -> Components -> Manage/Unmanage in the **Infrastructure** tile of the **Admin** menu.
5. In the **COMPONENTS – MANAGE/UNMANAGE** page that appears next, select *Fujitsu Primergy Rack Server* as the **Component type**. Then, the auto-discovered components will be displayed under **Unmanaged Components** section.
6. Figure 2.1 and Figure 2.2 clearly illustrate the process of managing a Fujitsu Primergy Rack Server.



COMPONENTS - MANAGE / UNMANAGE

This page enables the administrator to manage/unmanage the discovered servers.

Component type: Fujitsu Primergy Rack Server

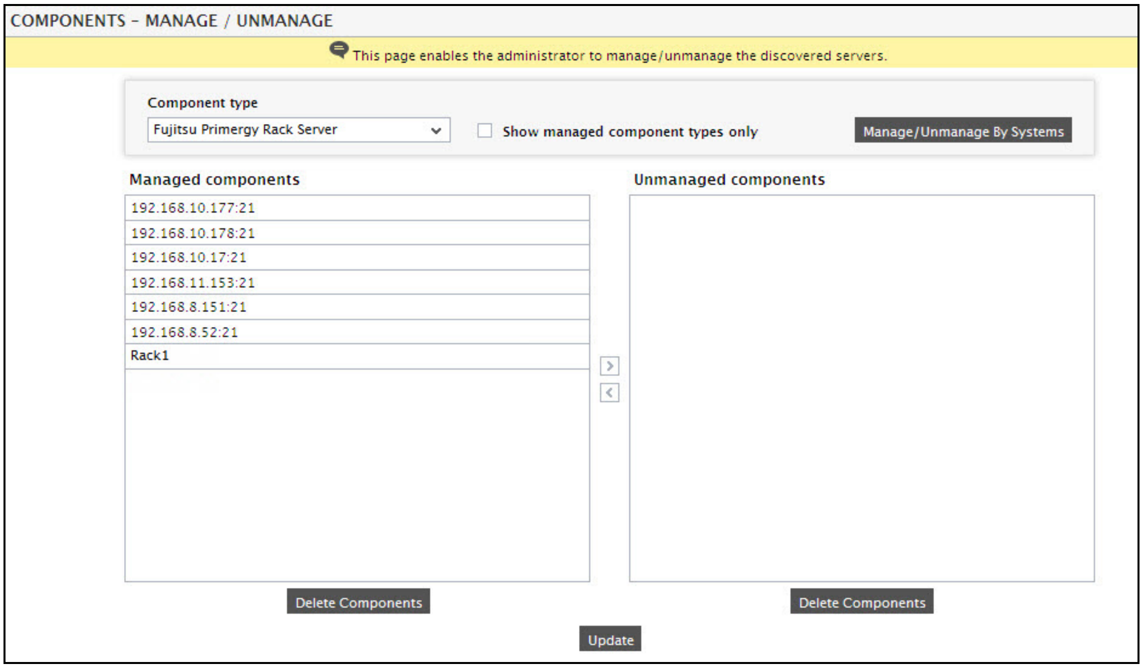
□ Show managed component types only

Managed components

Unmanaged components

192.168.10.177:21
192.168.10.178:21
192.168.10.17:21
192.168.11.153:21
192.168.8.151:21
192.168.8.52:21
Rack1

Figure 2.1: Viewing the unmanaged Fujitsu Primergy Rack Servers



COMPONENTS - MANAGE / UNMANAGE

This page enables the administrator to manage/unmanage the discovered servers.

Component type: Fujitsu Primergy Rack Server

□ Show managed component types only

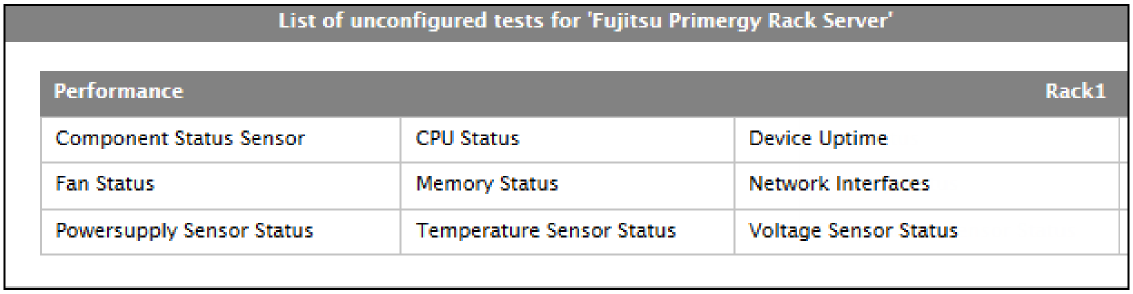
Managed components

192.168.10.177:21
192.168.10.178:21
192.168.10.17:21
192.168.11.153:21
192.168.8.151:21
192.168.8.52:21
Rack1

Unmanaged components

Figure 2.2: Managing a Fujitsu Primergy Rack Server

7. Now when you try to sign out of the eG administrative interface, a list of tests that need to be configured for the Fujitsu Primergy Rack Server will appear (see Figure 2.3).

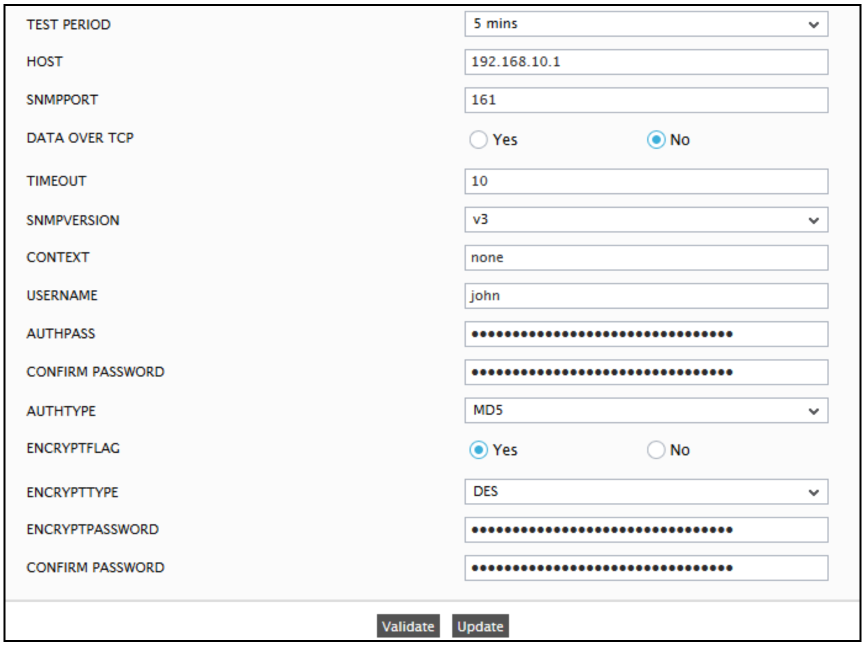


List of unconfigured tests for 'Fujitsu Primergy Rack Server'

Performance		Rack1
Component Status Sensor	CPU Status	Device Uptime
Fan Status	Memory Status	Network Interfaces
Powersupply Sensor Status	Temperature Sensor Status	Voltage Sensor Status

Figure 2.3: Viewing the list of tests that need to be configured for the Fujitsu Primergy Rack Server

8. Clicking on the **Component Status Sensor** test will open a page (see Figure 2.4) wherein the test parameters can be configured. Refer to Section **3.1.1** to know how to configure the test.



TEST PERIOD	5 mins
HOST	192.168.10.1
SNMPPORT	161
DATA OVER TCP	○ Yes ● No
TIMEOUT	10
SNMPVERSION	v3
CONTEXT	none
USERNAME	john
AUTHPASS	••••••••••••••••••••••••••••••••
CONFIRM PASSWORD	••••••••••••••••••••••••••••••••
AUTHTYPE	MD5
ENCRYPTFLAG	● Yes ○ No
ENCRYPTTYPE	DES
ENCRYPTPASSWORD	••••••••••••••••••••••••••••••••
CONFIRM PASSWORD	••••••••••••••••••••••••••••••••

Figure 2.4: Configuring the parameters of the Component Status Sensor test

9. On completing configuration, click on the **Update** button to save the changes and signout of the eG administrative interface.

10. With that, test configuration is complete and Fujitsu Primergy Rack Server is finally ready to be monitored.

Chapter 3: Monitoring Fujitsu Primergy Rack Servers

eG Enterprise prescribes an exclusive Fujitsu Primergy Rack Server monitoring model (see Figure 3.1), that determines the status of the core hardware components at frequent intervals.

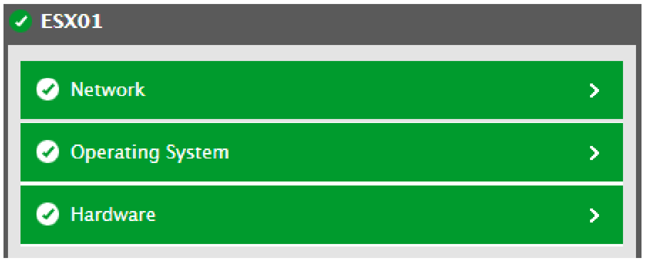


Figure 3.1: The layer model of the Fujitsu Primergy Rack server

Using the metrics reported, administrators can find quick and accurate answers for the following performance questions:

- What is the current status of each CPU?
- What is the current status of each power supply unit?
- What is the current status of each temperature sensor?
- What is the temperature recorded by each temperature sensor?
- What is the current status of each fan?
- What is the speed of each fan?
- What is the current status of each voltage sensor?
- What is the current status of each sensor of the hardware component?

The **Network** layer of the **Fujitsu Primergy Rack Server** model is similar to that of a **Windows Generic** server model. Since these tests have been dealt with in the *Monitoring Windows and Unix Servers* document, the section to come focuses on the other layers associated with the server.

3.1 The Hardware Layer

Using the tests associated with this layer, administrators can determine the status of each hardware component of the target server and identify the hardware component that has already failed and is about to fail with ease!

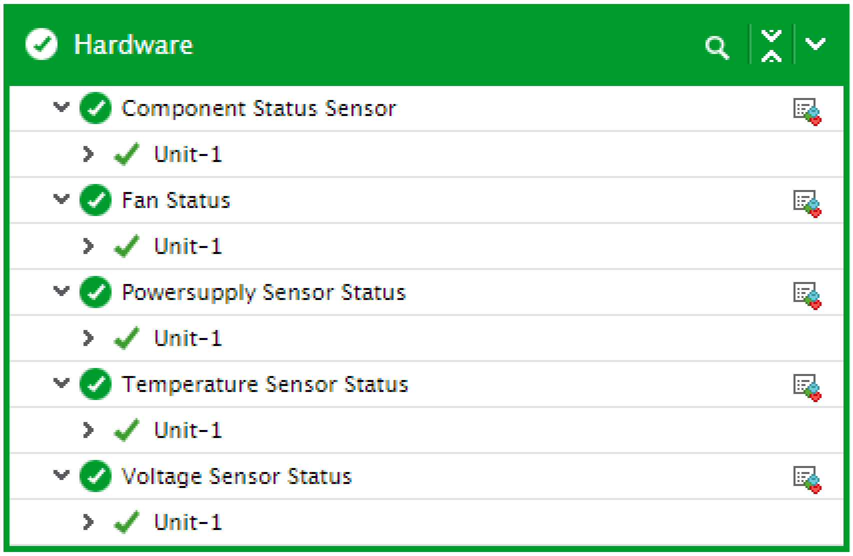


Figure 3.2: The test mapped to the Hardware layer

Each test associated with this layer is discussed in detail in the following sections.

3.1.1 Component Status Sensor Test

This test auto-discovers the hardware components of the target server and for each hardware component reports the current state. Using this test, administrators can figure out the hardware component that failed and replace them swiftly.

Target of the test : A Fujitsu Primergy Rack Server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Rack Unit:hardware component* available on the target Rack 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current state of the sensor of this hardware component.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Not available</td><td>2</td></tr>
<tr><td>Identify</td><td>3</td></tr>
<tr><td>Prefailure warning</td><td>4</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><table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>Failure</td><td>5</td></tr><tr><td>Not present</td><td>0</td></tr></table>
<b>Note:</b>
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the sensor of each hardware component. The graph of this measure however is represented using the numeric equivalents only.</td></tr>
</table>

3.1.2 Fan Status Test

If the fan suddenly stops running, temperature of the Rack server will soar, causing serious damage to the core components of the server. This is why, it's good practice to keep track of the fan status using the **Fan Status** test. For each fan available on each rack unit, this test reports how healthy the fan is and what is its current operational speed.

Target of the test : A Fujitsu Primergy Rack Server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Rack Unit: Fan* available on the target Rack 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
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

Parameter	Description
	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 default. To ensure that SNMP requests sent by the eG agent are encrypted, select the

Parameter	Description
	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>Status</td><td>Indicates the current state of this fan.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Disabled</td><td>2</td></tr>
<tr><td>Ok</td><td>3</td></tr>
<tr><td>Not manageable</td><td>7</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><table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>Not present</td><td>8</td></tr><tr><td>Failed</td><td>9</td></tr><tr><td>Prefailure predicted</td><td>10</td></tr><tr><td>Redundant fan failed</td><td>11</td></tr></table>
Note:
By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of each fan. The graph of this measure however is represented using the numeric equivalents only.</td></tr>
<tr><td>Speed</td><td>Indicates the current speed of this fan.</td><td>RPM</td><td>Ideally, the speed of the fan should be within admissible range. A sudden/gradual increase/decrease in the speed of the fan may result in failure of the fan thus causing degradation of the hardware components of the server.</td></tr>
</table>

3.1.3 Powersupply Sensor Status Test

This test auto-discovers the powersupply units of the target Fujitsu Primergy Rack server and for each powersupply unit determines the current status and the output passing through each unit. This way, administrators can be proactively alerted to powersupply units that are about to fail and the units through which abnormal amount of output power is passing through.

Target of the test : A Fujitsu Primergy Rack Server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Rack Unit: Powersupply unit* available on the target Rack 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
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

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
Status	Indicates the current state of this powersupply unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<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>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Power safe mode</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Not present</td><td>2</td></tr>
<tr><td>Ok</td><td>3</td></tr>
<tr><td>AC failed</td><td>5</td></tr>
<tr><td>DC failed</td><td>6</td></tr>
<tr><td>Critical temperature</td><td>7</td></tr>
<tr><td>Not manageable</td><td>8</td></tr>
<tr><td>Fan failure predicted</td><td>9</td></tr>
<tr><td>Fan failure</td><td>10</td></tr>
<tr><td>Non redundant DC failed</td><td>12</td></tr>
<tr><td>Non redundant AC failed</td><td>13</td></tr>
<tr><td>Failed</td><td>14</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each powersupply unit. The graph of this measure however is represented using the numeric equivalents only.</td></tr>
<tr><td>Powersupply load</td><td>Indicates the actual output power passing through this powersupply unit.</td><td>Watts</td><td>The value of this measure should be within admissible range. If the value of this measure increases/decreases suddenly, then it may damage the powersupply unit and this may in turn affect the performance of the hardware components of the target server.</td></tr>
</table>

3.1.4 Temperature Sensor Status Test

This test auto-discovers the temperature sensors on the target Fujitsu Primergy Rack server and for each temperature sensor, this test reports the current status and the temperature. Using this test, administrators can easily figure out the temperature sensors that have failed and are about to fail. This way, administrators can replace the faulty temperature sensors before the hardware components fail. In addition, the temperature recorded by each temperature sensor too can be determined and sensors recording abnormal temperatures can be replaced.

Target of the test : A Fujitsu Primergy Rack Server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Rack Unit: Temperature sensor* available on the target Rack 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
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.

Parameter	Description
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 should time out in this text box. The default is 10 seconds.

Parameter	Description
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>Status</td><td>Indicates the current state of this temperature sensor.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Normal temperature</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Not available</td><td>2</td></tr>
<tr><td>Ok</td><td>3</td></tr>
<tr><td>Sensor failed</td><td>4</td></tr>
<tr><td>Failed</td><td>5</td></tr>
<tr><td>Temperature warning too hot</td><td>6</td></tr>
<tr><td>Temperature critical toohot</td><td>7</td></tr>
<tr><td>Temperature warning</td><td>9</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each temperature sensor. The graph of this measure however is represented using the numeric equivalents only.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Temperature	Indicates the current temperature recorded by this temperature sensor.	Celsius	Ideally, the value of this measure should be low. A high value could be a cause for concern.

3.2 The Operating System Layer

Using the tests mapped to this layer, administrators can figure out the current status of the CPU and the memory modules of the target server. The count of CPU cores that are busy too can be determined.

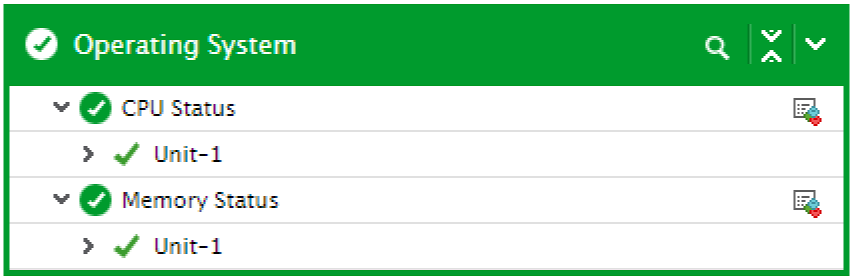


Figure 3.3: The test associated with the Operating System layer

3.2.1 CPU Status Test

This test auto-discovers the CPUs of each rack unit on the target Fujitsu Primergy Rack Server and for each CPU discovered, reports the current status and the number of CPU cores enabled. Using this test, administrators would be able to identify the CPUs that have failed already and are about to fail and take remedial measures before users start complaining.

Target of the test : A Fujitsu Primergy Rack Server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Rack Unit: CPU* available on the target Rack server being monitored.

Configurable parameters for the test

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

Parameter	Description
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
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:

Parameter	Description
	• **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
Status	Indicates the current state of this CPU.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<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>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Missing termination</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Not present</td><td>2</td></tr>
<tr><td>Ok</td><td>3</td></tr>
<tr><td>Disabled</td><td>4</td></tr>
<tr><td>Error</td><td>5</td></tr>
<tr><td>Prefailure warning</td><td>8</td></tr>
<tr><td>Failed</td><td>9</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each CPU. The graph of this measure however is represented using the numeric equivalents only.</td></tr>
<tr><td>Enabled CPU core count</td><td>Indicates the number of CPU cores enabled on this CPU.</td><td>Number</td><td>The higher the number of enabled CPU cores, the higher is the processing capacity of the CPU.</td></tr>
</table>

3.2.2 Memory Status Test

This test auto-discovers the memory modules of the target Fujitsu Primergy Rack server and for each memory module, this test reveals the current status. In addition, the size of the memory module too can be determined. Using this test, administrators can determine the memory module that had failed already and is about to fail with ease and replace the same before end users start complaining.

Target of the test : A Fujitsu Primergy Rack Server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Rack Unit: Memory Module* available on the target Rack 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 host for which this test is to be configured.
Port	Refers to the port at which the specified host listens to.
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

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
Status	Indicates the current state of this memory module.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<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>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Not present</td><td>2</td></tr>
<tr><td>Ok</td><td>3</td></tr>
<tr><td>Disabled</td><td>4</td></tr>
<tr><td>Hot spare</td><td>8</td></tr>
<tr><td>Mirror</td><td>9</td></tr>
<tr><td>Raid</td><td>10</td></tr>
<tr><td>Hidden</td><td>11</td></tr>
<tr><td>Error</td><td>12</td></tr>
<tr><td>Failed</td><td>13</td></tr>
<tr><td>Prefailure predicted</td><td>14</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each memory module. The graph of this measure however is represented using the numeric equivalents only.
</td></tr>
<tr><td>Size</td><td>Indicates the size of this memory module.</td><td>GB</td><td></td></tr>
</table>

Restricted Rights Legend

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

Trademarks

Microsoft Windows, Windows 2008, Windows 7, Windows 8, Windows 10, Windows 2012, Windows 2016 and Windows 2019 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

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

Copyright

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.