Enabling Service Excellence

Hardware Monitoring using eG Enterprise

eG Enterprise v6

Restricted Rights Legend

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

Trademarks

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

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

Copyright

Table of Contents

INTRODUCTION 1

HARDWARE MONITORING USING NATIVE OS COMMANDS 3

2.1 Hardware Monitoring on Solaris Environments 3

2.1.1 CpuStatus Test 3

2.1.2 MemoryStatus Test 4

2.1.3 DiskStatus Test 4

2.1.4 FanStatus Test 5

2.1.5 SystemFaults Test 5

2.1.6 Temperature Test 6

2.1.7 Hardware-PowerSupply Test 6

2.1.8 CurrentSensors Test 7

2.1.9 CurrentVoltage Test 7

2.1.10 TemperatureSensors Test 8

2.1.11 LedSensors Test 9

2.2 Hardware Monitoring on AIX Environments 9

2.2.1 Hardware-Temperature Test 9

2.2.2 Hardware-Fan Test 11

2.2.3 Hardware-Voltage Test 13

HARDWARE MONITORING USING IBM DIRECTOR/DELL OPENMANAGER OR COMPAQ INSIGHT MANAGEMENT 16

3.1 Hardware-Status Test 17

3.2 Hardware-Overview Test 20

3.3 Hardware-Temperature Test 22

3.4 Hardware-Fan Test 24

3.5 Hardware-Voltage Test 26

3.6 Hardware-ArrayControl Test 27

3.7 Hardware-Drive Test 29

3.8 Hardware-Processor Test 34

3.9 Hardware-PowerSupply Test 37

3.10 Hardware-Memory Test 40

3.11 Hardware-Battery Test 43

3.12 Hardware-Amperage Test 46

3.13 Dell Array Controllers Test 49

3.14 Dell Drives Test 53

HARDWARE MONITORING USING INTEGRATED MANAGEMENT MODULE (IMM) 58

4.1 IBM - IMM Processor Test 58

4.2 IBM - IMM Temperature Test 60
4.3 IBM - IMM Voltage Test 62
4.4 IBM - IMM System Test 65
4.5 IBM - IMM Memory Module Test 69
4.6 IBM - IMM Fan Test 71
4.7 IBM - IMM Power Test 74
4.8 IBM - IMM Events Test 76
4.9 IBM - IMM HardDisk Test 78
HARDWARE MONITORING USING ILO 81
5.1 HP - ILO Fan Test 81
5.2 HP - ILO Sensor Temperature Test 84
5.3 HP - ILO Memory Details Test 86
5.4 HP - ILO Memory Summary Test 91
5.5 HP - ILO System Board Controller Test 93
5.6 HP -ILO Logical Drive Test 96
5.7 HP - ILO Physical Drive Test 99
5.8 HP - ILO Power Test 102
5.9 HP - ILO Drive Test 106
5.10 HP - ILO Processors Test 110
5.11 HP - ILO Event Test 113
HARDWARE MONITORING USING ILOM 116
6.1 ILOM Fan Test 116
6.2 ILOM Hard Disk Test 119
6.3 ILOM Power Supply Test 122
6.4 ILOM Server CPU Test 126
6.5 ILOM Fan Sensor Test 129
6.6 ILOM Power Sensor Test 132
6.7 ILOM Temperature Sensor Test 135
6.8 ILOM Voltage Sensor Test 139
6.9 ILOM Server power Test 142
6.10 ILOM Battery Test 144
6.11 Benefits 146
CONCLUSION 148

Chapter

1

Introduction

The need for monitoring applications and software is unquestionable, but monitoring of the hardware is equally important. Sometimes, a malfunctioning hardware component can cause server downtime, thereby adversely impacting the performance of a critical business service. Detecting and fixing a hardware problem on time can increase service uptime and enhance customer satisfaction. Furthermore, if a hardware failure is not identified and addressed on time, it could cause irreparable damage to the hardware device as such, bring down critical IT services, cause colossal data loss, and catapult maintenance costs.

One of the biggest challenges in managing hardware is the heterogeneity. IT infrastructures typically comprise of equipment from multiple manufacturers. Each manufacturer provides their own solution for monitoring and managing their hardware. For example, Sun Microsystems provides the Sun Management Center for managing Sun hardware, IBM offers the IBM Director, Compaq/HP provides Compaq/HP Insight manager managing their servers, and Dell provides Dell OpenManage for its servers. In a multi-vendor environment, IT administrators require a single integrated console from where they can monitor the heterogeneous hardware components that they are responsible for. Furthermore, the administrators require the ability to correlate between the performance of the hardware and the user view of the IT services that use the hardware, so that problems can be identified as being caused by the hardware or by the software.

eG Enterprise offers integrated monitoring of multi-vendor hardware from a central console. eG agents for Sun Solaris and AIX use native operating system commands and hooks to monitor the status of the hardware on these servers. For other operating systems (Windows, Linux, and HPUX), the eG agents can obtain hardware status information from IBM Director agents, Compaq/HP Insight Agents and Dell OpenManage agents. The eG agent interfaces with the IBM, Compaq/HP and Dell solutions using SNMP – periodically, the eG agent can poll specific MIB variables from the IBM, Compaq/HP and Dell agents to track the status of the server hardware. While agent-based monitoring is required for monitoring Sun Solaris and AIX hardware, since IBM, Compaq/HP and Dell servers are managed using SNMP, hardware monitoring for these servers can also be done in an agentless manner (i.e., without installing eG agents on the servers being managed). Prior to eG Enterprise Suite v6, the eG agents cannot collect the hardware status information whenever the target server was down or unavailable. From v6, the eG agent is configured to communicate with the remote server management processor/management card of the corresponding server and retrieve the necessary hardware statuis information. If the server to be monitored is an IBM server, then the eG agent communicates with the Integrated Management Module (IMM) and collects the required metrics. Likewise, the eG agent communicates with the HP/Dell servers and Solaris servers through Integrated Lights Out (ILO) management processor and Integrated Lights Out Manager (ILOM) respectively.

Some of the key questions that administrators can answer using the hardware monitoring capabilities of the eG Enterprise suite are:

- Is the server hardware working well?

- What is the status of the cooling units/fans of a server?
- What is the current temperature of a server? Is it within norms?
- Are all power supplies of a server available? If not, which ones have failed?
- What is the current voltage of the power supplies on the server?
- How many memory devices are available on a server and are they all working well?
- How many memory errors have been detected? Is there a faulty memory module on the system?
- Is a server's drive array subsystem working properly?
- Are the different physical and logical drives on a server working well? If not, what is their current condition?

The chapters below discuss at length, the hardware monitoring capabilities of eG Enterprise across different Windows and Unix platforms.

Note:

Hardware monitoring requires only a basic agent license.

Hardware Monitoring using Native OS Commands

eG agents for Sun Solaris and AIX servers use native operating system commands and hooks to monitor the status of the hardware on these servers. The below sections mention in detail the hardware monitoring of Solaris and AIX servers in detail.

2.1 Hardware Monitoring on Solaris Environments

Every component monitored by eG Enterprise is represented as a set of hierarchical layers, with every layer mapped to a logical group of tests that are executed on the component. The hardware tests related to Solaris servers are mapped to the **Operating System** layer of the target component.

All these tests are disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the component-type for which these tests are to be enabled as the **Component type**, set *Performance* as the **Test type**, choose the tests from the **DISABLED TESTS** list, and click on the **>>** button to move the tests to the **ENABLED TESTS** list. Finally, click the **Update** button.

The hardware tests and the measures they report are discussed hereunder.

2.1.1 CpuStatus Test

The CpuStatus test indicates whether the processors in a system are being used or not. This test works on Solaris only.

Purpose	Indicates whether the processors of a system are working or not		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every processor of the Solaris system being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Availability:** Indicates whether this processor is available for use or not.	Percent	If the value of this measure is 100, it indicates that the processor is available for use. A value of 0, on the other hand, indicates that the processor is not available for use.

2.1.2 MemoryStatus Test

The MemoryStatus test monitors the usage of the various memory partitions or banks in a system. This test works on Solaris platforms only.

Purpose	Monitors the usage of the various memory partitions or banks in a system		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every memory bank in the Solaris system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether this memory partition is available for use or not.	Percent	If the value of this measure is 100, it denotes that the memory partition/bank is available for use. A value of 0 is indicative of the memory bank not being used.

2.1.3 DiskStatus Test

The DiskStatus test monitors the usage of a system's disks. This test works on Solaris platforms only.

Purpose	Monitors the availability of a system's disks
Target of the test	A Sun Solaris server
Agent deploying the test	An internal agent
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured

Outputs of the test	One set of results for every disk on the Solaris system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether the disk partition is being used or not.	Percent	If the value of this measure is 100, it denotes the availability of the disk. The value 0 indicates that the disk is not being used.

2.1.4 FanStatus Test

The FanStatus test monitors the availability of the fans in a system. This test works on Sun Solaris only.

Purpose	Monitors the availability of fans in the target system		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every fan on the Solaris system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether this fan is being used or not.	Percent	If the value of this measure is 100, it indicates that the fan is available and is being used. A value of 0, on the other hand, indicates that the fan is not being used.

2.1.5 SystemFaults Test

The SystemFaults test measures the number of system faults that have occurred. This test works on Solaris platforms only.

Purpose	Measures the number of system faults that have occurred
Target of the test	A Sun Solaris server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every Solaris system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Number of faults: Indicates the number of system faults that have occurred.	Number	A high value of system faults is indicative of malfunctioning hardware. If this value is unusually high, immediate attention is required to diagnose the problem.

2.1.6 Temperature Test

The Temperature test measures the current temperature of the individual processors, the memory units, and other hardware units in a system. This test works on Solaris platforms only.

Purpose	Measures the current temperature of the individual processors, the memory units, and other hardware units of a system		
Target of the test	A Solaris host		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every hardware unit in the Solaris system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Temperature: Indicates the temperature of this hardware unit (in degree Celsius).	DegreeC	A sudden increase in temperature can impact the functioning of a server and must be immediately attended to.

2.1.7 Hardware-PowerSupply Test

This test monitors the availability of the various power supply units of a system. This test works on Solaris only.

Purpose	Monitors the availability of the various power supply units in a system
Target of the	A Sun Solaris server

test			
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every power supply unit in the Solaris system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether this power supply unit is being used or not.	Percent	If the value of this measure is 100, it indicates that the power supply unit is being used. A value of 0 indicates that the power supply unit is not available for use.

2.1.8 CurrentSensors Test

This test indicates whether / not the current sensors on a Solaris server are currently operational or not.

Purpose	Indicates whether / not the current sensors on a Solaris server are currently operational or not		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every current sensor on the Solaris host being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Sensor status: Indicates whether this current sensor is operational or not.	Boolean	While the value 1 indicates that the sensor is currently operational, the value 0 indicates that it is not.

2.1.9 CurrentVoltage Test

This test indicates the current status of the voltage sensors on a Solaris server.

Purpose	Indicates the current status of the voltage sensors on a Solaris server		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every voltage sensor on the Solaris host being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Sensor status: Indicates whether this voltage sensor is operational or not.	Boolean	While the value 1 indicates that the sensor is currently operational, the value 0 indicates that it is not.

2.1.10 TemperatureSensors Test

This test indicates the current status of the temperature sensors on a Solaris server.

Purpose	Indicates the current status of the temperature sensors on a Solaris server		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every temperature sensor on the Solaris host being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Sensor status: Indicates whether this sensor is operational or not.	Boolean	While the value 1 indicates that the sensor is currently operational, the value 0 indicates that it is not.

2.1.11 LedSensors Test

This test indicates the current status of the Light emitting diodes (LED) on a Solaris server.

Purpose	Indicates the current status of the Light emitting diodes on a Solaris server		
Target of the test	A Sun Solaris server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured		
Outputs of the test	One set of results for every LED sensors on the Solaris host being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	LED status: Indicates whether this LED is active or not.	Boolean	While the value 1 indicates that the LED is currently operational, the value 0 indicates that it is not.

2.2 Hardware Monitoring on AIX Environments

To monitor the hardware status of AIX servers, the eG agent uses native AIX commands/hooks on the AIX server to haul out the performance data. To execute the AIX commands/hooks, the eG agent should be installed on the AIX server as a root user.

Every component monitored by eG Enterprise is represented as a set of hierarchical layers, with every layer mapped to a logical group of tests that are executed on the component. The hardware tests related to Solaris servers are mapped to the **Operating System** layer of the target component.

All these tests are disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the component-type for which these tests are to be enabled as the **Component type**, set *Performance* as the **Test type**, choose the tests from the **DISABLED TESTS** list, and click on the **>>** button to move the tests to the **ENABLED TESTS** list. Finally, click the **Update** button.

The hardware tests and the measures they report are discussed hereunder.

2.2.1 Hardware-Temperature Test

This test monitors the thermal status of the hardware of a server.

Purpose	Monitors the thermal status of the hardware of a server. A sudden change in temperature of the server may indicate a problem that needs immediate attention.
Target	An AIX server
Agent deploying this test	Internal agent

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

<table>
<tr><td></td><td colspan="3">

Note

Note that the SNMP-related parameters are not relevant while monitoring hardware on AIX servers; in such a case therefore, you can specify *none* against **SNMPPORT** and **SNMPCOMMUNITY** strings, and leave the **SNMPVERSION** as **v1**.

15. **REPORTINDEGC** - This flag is set to **Yes** by default, indicating that this test will report the *Current temperature* of the sensor in Celsius (by default). If you want the *Current temperature* to be reported in Fahrenheit instead, set this flag to **No**.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of records for each temperature probe of the system</td></tr>
<tr><td rowspan="3"><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Current temperature:</b>
Indicates the current reading of the temperature sensor.</td><td>Degree</td><td>The descriptor for this test indicates the temperature sensor name in the case of Dell servers. For HP/Compaq servers, the descriptor is of the form "chassis number.temperature sensor".</td></tr>
<tr><td><b>Temperature status:</b>
Indicates whether the temperature sensor is showing abnormality.</td><td>Number</td><td>A value of 1 indicates normalcy. A value of 2 indicates a minor problem, a value of 3 indicates a major problem, and a value of 4 indicates a critical problem.</td></tr>
</table>

2.2.2 Hardware-Fan Test

This test monitors the status of each of the cooling units/fans on a server.

Purpose	Monitors the status of each of the cooling units/fans on a server
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent, or an AIX server
Agent deploying this test	Internal/remote agent (internal agent only for AIX)

Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the encryptflag is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE**e list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD –** Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. **Note** Note that the SNMP-related parameters are not relevant while monitoring hardware on AIX servers; in such a case therefore, you can specify *none* against **SNMPPORT** and **SNMPCOMMUNITY** strings, and leave the **SNMPVERSION** as **v1**.		
Outputs of the test	One set of records for each fan		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current fan speed: Indicates the current speed of the cooling unit/fan in revolutions per min.	RPM	
	Fan status: Indicates whether the cooling unit/fan is working properly.	Number	A value of 1 indicates normalcy. A value of 2 indicates a minor problem, a value of 3 indicates a major problem, and a value of 4 indicates a critical problem.

2.2.3 Hardware-Voltage Test

This test monitors the status of each of the power supply units on a server.

Purpose	Monitors the status of each of the power supply units on a server
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent, or an AIX server
Agent deploying this test	Internal/remote agent (internal agent only for AIX)
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the

default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP **v3** converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the encryptflag is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
11. **ENCRYPTTYPE** – If the encryptflag is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP **v3** supports the following encryption types:

    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
12. **ENCRYPTPASSWORD** – Specify the encryption password here.
13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

	Note Note that the SNMP-related parameters are not relevant while monitoring hardware on AIX servers; in such a case therefore, you can specify *none* against **SNMPPORT** and **SNMPCOMMUNITY** strings, and leave the **SNMPVERSION** as **v1**.		
Outputs of the test	One set of records for each power supply unit		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current voltage: Indicates the current voltage of the power supply.	Volts	
	Voltage status: Indicates whether the current voltage value is normal or not.	Number	A value of 1 indicates normalcy. A value of 2 indicates a minor problem, a value of 3 indicates a major problem, and a value of 4 indicates a critical problem.

Hardware Monitoring using IBM Director/Dell OpenManager or Compaq Insight Management

To monitor the hardware status of Windows/Linux/HPUX servers, the eG agents integrate with IBM Director, Dell OpenManage or Compaq Insight Management. Agents for IBM Director, Dell OpenManage or Compaq Insight Management have to be installed on the servers to be monitored. In the case of AIX servers though, while most of the tests use native AIX commands/hooks on the AIX server to haul out the performance data, a couple of tests require the installation of Dell OpenManage or Compaq Insight Management on the server. To execute the AIX commands/hooks, the eG agent should be installed on the AIX server as a root user.

Once the third-party tools are installed, the eG agents then use SNMP to communicate with the hardware monitoring solutions (see Figure 1). The metrics so collected vary depending upon the Hardware status information relating to power supplies, fans, temperature, etc. are collected in this manner and reported via the eG monitoring console. This integration of the eG Enterprise suite with third-party agents allows administrators to leverage their existing investment into these hardware monitoring solutions. Furthermore, with this integration in place, the status of the entire infrastructure can be monitored - right from the hardware to the operating system and the individual processes and applications running on each server.

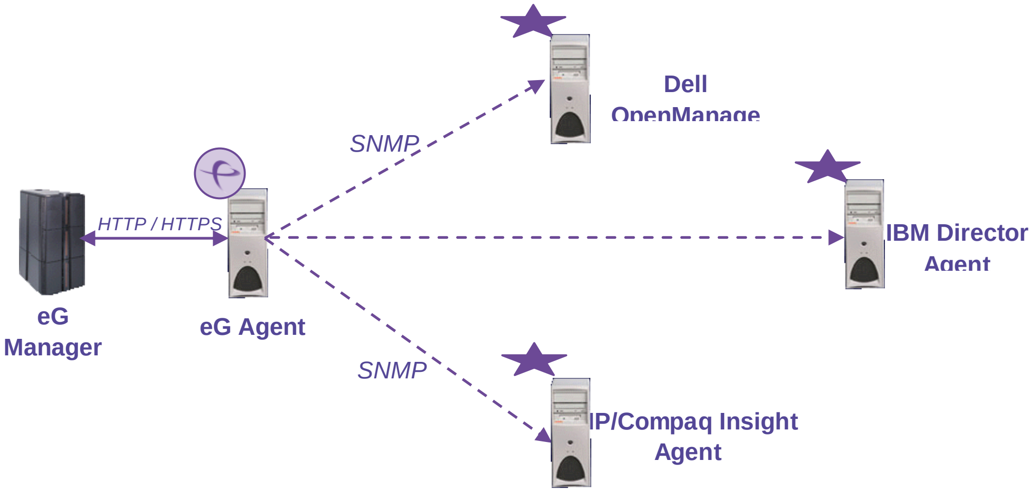

Figure 1: Integrating eG Enterprise will Dell Open Manage and HP/Compaq Insight Agents

The tests that the eG agent executes on the IBM Director/Dell OpenManage/Compaq Insight Management host are mapped to the **Operating System** layer. All these tests are disabled by default. To enable the tests, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the component-type for which these tests are to be enabled as the **Component type**, set *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

The matrix below indicates the platforms on which each of the hardware tests execute.

Test Name	Intel/AMD (32-bit or 64-bit) Machines running Windows / Linux / HPUX Operating Systems and Hosting IBM Director Agents	Intel/AMD (32-bit or 64-bit) Machines running Windows / Linux / HPUX Operating Systems and Hosting HP Insight Agents	Intel/AMD (32-bit or 64-bit) Machines running Windows / Linux / HPUX Operating Systems and Hosting Dell OpenManage Agents	IBM RS6000 Machines running AIX Operating Systems
Hardware - Status	X	✓	✓	X
Hardware - Overview	✓	✓	✓	X
Hardware – Temperature	✓	✓	✓	✓
Hardware – Fan	✓	✓	✓	✓
Hardware – Voltage	✓	✓	✓	✓
Hardware – ArrayControl	X	✓	✓	X
Hardware - Drive	X	✓	✓	X
Hardware - Processor	X	X	✓	X
Hardware - PowerSupply	X	X	✓	X
Hardware - Memory	X	X	✓	X
Hardware - Battery	X	X	✓	X
Hardware - Amperage	X	X	✓	X
Dell Hardware - ArrayControl	X	X	✓	X
Dell Hardware - Drive	X	X	✓	X

3.1 Hardware-Status Test

This test monitors the overall status of the hardware of a server and also serves as an effective health indicator for the following system components:

- Chassis
- Power supply units

- Voltage probes
- Cooling units
- Temperature probes
- Memory devices

Purpose	Monitors the overall status of the hardware of a server
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled,** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: - **MD5** – Message Digest Algorithm - **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted,

	select the **YES** option. 11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of outputs for the host monitored		
Measurements of the *test*	**Measurement**	**Measurement Unit**	**Interpretation**
	System status: Monitors the overall status of the system.	Number	A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system.
	Chassis status: Monitors the status of each chassis of the system. This measure is available for Dell Servers only.	Number	
	Power supply status: Represents the overall state of all the power supply units on this server.	Number	A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system.
	Voltage status: Represents the combined state of all voltage probes on this system.	Number	Multiple values may be provided if there are multiple chassis on the system. A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system. This value is available only for Dell servers.

	Amperage status: Represents the combined amperage status of all amperage probes on this system.	Number	Multiple values may be provided if there are multiple chassis on the system. A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system. This value is available only for Dell servers.
	Cooling unit status: Represents the combined status of all the cooling devices/fans of the system.	Number	Multiple values may be provided if there are multiple chassis on the system. A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system.
	Temperature status: Represents the combined status of all temperature probes of the system.	Number	Multiple values may be provided if there are multiple chassis on the system. A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system.
	Memory device status: Represents the combined status of all memory devices of the system.	Number	Multiple values may be provided if there are multiple chassis on the system. A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system.
	Chassis intrusion status: Represents the combined status of all intrusion detection devices on the system.	Number	Multiple values may be provided if there are multiple chassis on the system. A value of 1 indicates normalcy. A value of 2 indicates a non-critical issue, while a value of 3 indicates a critical issue with the system.

3.2 Hardware-Overview Test

The Hardware-Overview test complements the Hardware-Status test. This test checks for any correctable memory errors, tracks the drive status of a server, and also verifies if there are any errors with the automatic recovery capability of a server.

Purpose	Monitors the overall health of a server's hardware, checks for any correctable memory errors, and also verifies if there are any errors with the automatic recovery capability of a server
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled,** 3. **SNMPPORT** - The port number through which the server exposes its **SNMP MIB**. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in

use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.

8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.

9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

   - **MD5** – Message Digest Algorithm
   - **SHA** – Secure Hash Algorithm

10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the encryptflag is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:

    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard

12. **ENCRYPTPASSWORD** – Specify the encryption password here.

13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Outputs of the test	One set of records for every monitored system		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Overall status: Represents the overall status of the server hardware.	Number	A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.
	Memory status: Indicates the status of the correctable memory error log feature of a system.	Number	A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.
	Memory errors: This metric represents the number of correctable memory error log events that occurred during the last measurement period.	Number	
	Auto recovery status: This metric represents the overall condition of the automatic server recovery feature of a system.	Number	A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.
	Drive status: This metric represents the overall condition of the server's drive array subsystem.	Number	A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.

3.3 Hardware-Temperature Test

This test monitors the thermal status of the hardware of a server.

Purpose	Monitors the thermal status of the hardware of a server. A sudden change in temperature of the server may indicate a problem that needs immediate attention.
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent
Agent deploying this test	Internal/remote agent

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

	Current temperature of the sensor in Celsius (by default). If you want the *Current temperature* to be reported in Fahrenheit instead, set this flag to **No**. 16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of records for each temperature probe of the system		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current temperature: Indicates the current reading of the temperature sensor.	Degree	The descriptor for this test indicates the temperature sensor name in the case of Dell servers. For HP/Compaq servers, the descriptor is of the form "chassis number.temperature sensor".
	Temperature status: Indicates whether the temperature sensor is showing abnormality.	Number	A value of 1 indicates normalcy. A value of 2 indicates a minor problem, a value of 3 indicates a major problem, and a value of 4 indicates a critical problem.

3.4 Hardware-Fan Test

This test monitors the status of each of the cooling units/fans on a server.

Purpose	Monitors the status of each of the cooling units/fans on a server
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the snmpversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the

SNMPVERSION chosen is **v3**, then this parameter will not appear.

6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
   - **MD5** – Message Digest Algorithm
   - **SHA** – Secure Hash Algorithm
10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
12. **ENCRYPTPASSWORD** – Specify the encryption password here.
13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Outputs of the test	One set of records for each fan in the target server to be monitored		
Measurements	**Measurement**	**Measurement Unit**	**Interpretation**

of the test	**Current fan speed:** Indicates the current speed of the cooling unit/fan in revolutions per min.	RPM	
	Fan status: Indicates whether the cooling unit/fan is working properly.	Number	A value of 1 indicates normalcy. A value of 2 indicates a minor problem, a value of 3 indicates a major problem, and a value of 4 indicates a critical problem.

3.5 Hardware-Voltage Test

This test monitors the status of each of the power supply units on a server.

Purpose	Monitors the status of each of the power supply units on a server
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3

converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

- **MD5** – Message Digest Algorithm
- **SHA** – Secure Hash Algorithm

10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
12. **ENCRYPTPASSWORD** – Specify the encryption password here.
13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Outputs of the test	One set of records for each power supply unit		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current voltage: Indicates the current voltage of the power supply.	Volts	
	Voltage status: Indicates whether the current voltage value is normal or not.	Number	A value of 1 indicates normalcy. A value of 2 indicates a minor problem, a value of 3 indicates a major problem, and a value of 4 indicates a critical problem.

3.6 Hardware-ArrayControl Test

The Hardware-ArrayControl test monitors the overall health of the controllers of drive arrays on a system.

Purpose	Monitors the status of each of the controllers of drive arrays on a server

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

	13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of records for each array controller on the monitored system		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Controller condition: Represents the condition of an array controller.	Number	This value represents the overall condition of the controller and any associated logical drives, physical drives, and array accelerators. A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.
	Board condition: Indicates the status of the array controller's board and any array accelerators.	Number	A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.

3.7 Hardware-Drive Test

This test monitors the overall health of logical and physical drives of a disk array.

Purpose	Monitors the overall health of logical and physical drives of a disk array
Target	A server with IBM Director, Dell OpenManage or HP/Compaq Insight agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The default value is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework

is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP **v3** converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
   - **MD5** – Message Digest Algorithm
   - **SHA** – Secure Hash Algorithm
10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
12. **ENCRYPTPASSWORD** – Specify the encryption password here.
13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Outputs of the test	One set of records for every logical/physical drive on the monitored system				
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**		
	Condition: Represents the condition of a logical or physical drive.	Number	For a logical drive, this value represents the overall condition of the logical drive and any associated physical drives. For a physical drive, this value represents its overall condition. A value of 1 indicates normalcy. A value of 2 indicates a degraded condition, while a value of 3 indicates a critical condition.		
	Status: This value indicates the status of a physical or logical drive.	Number	The following values are valid for the physical drive status:		
			Value	**Description**	**Explanation**
			1	Other	Indicates that the instrument agent does not recognize the drive. You may need to upgrade your instrument agent and/or driver software.
			2	ok	Indicates the drive is functioning properly.
			3	failed	Indicates that the drive is no longer operating and should be replaced
			4	predictiveFailure	Indicates that the drive has a predictive failure error and should be replaced.
			For a logical drive, the following values are valid:		
			Value	**Description**	**Explanation**
			2	OK	Indicates that the logical drive is in normal operation mode.

			3	Failed	Indicates that more physical drives have failed than the fault tolerance mode of the logical drive can handle without data loss.
			4	Unconfigure d	Indicates that the logical drive is not configured.
			5	Recovering	Indicates that the logical drive is using Interim Recovery Mode. In Interim Recovery Mode, at least one physical drive has failed, but the logical drive's fault tolerance mode lets the drive continue to operate with no data loss.
			6	Ready Rebuild	Indicates that the logical drive is ready for Automatic Data Recovery. The physical drive that failed has been replaced, but the logical drive is still operating in Interim Recovery Mode.

			7	Rebuilding	Indicates that the logical drive is currently doing Automatic Data Recovery. During Automatic Data Recovery, fault tolerance algorithms restore data to the replacement drive.
			8	Wrong Drive	Indicates that the wrong physical drive was replaced after a physical drive failure.
			9	Bad Connect	Indicates that a physical drive is not responding.
			10	Overheating	Indicates that the drive array enclosure that contains the logical drive is overheating. The drive array is still functioning, but should be shutdown.
			11	Shutdown	Indicates that the drive array enclosure that contains the logical drive has overheated. The logical drive is no longer functioning.

			12	Expanding	Indicates that the logical drive is currently doing Automatic Data Expansion. During Automatic Data Expansion, fault tolerance algorithms redistribute logical drive data to the newly added physical drive.
			13	Not Available	Indicates that the logical drive is currently unavailable. If a logical drive is expanding and the new configuration frees additional disk space, this free space can be configured into another logical volume. If this is done, the new volume will be set to not available.
			14	Queued For Expansion	Indicates that the logical drive is ready for Automatic Data Expansion. The logical drive is in the queue for expansion.

3.8 Hardware-Processor Test

This test monitors the current status and speed of the processors supported by a system. **This test executes only on IBM Dell Servers**.

Purpose	Monitors the current status and speed of the processors supported by a system
Target	A server with Dell OpenManage agent

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

<table>
<tr><td></td><td colspan="3">14. <b>TIMEOUT</b> - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
15. <b>DATA OVER TCP –</b> 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 server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of records for every processor supported by the monitored system</td></tr>
<tr><td rowspan="2"><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status:</b>
Indicates the current status of this processor.</td><td>Number</td><td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>0</td></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Non Critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non Recoverable</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current status of a processor. However, in the graph of this measure, processor status is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr><td></td><td><b>State:</b>
Indicates the current state of this processor.</td><td>Number</td><td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Enabled</td><td>3</td></tr>
<tr><td>Idle</td><td>4</td></tr>
<tr><td>Bios Disabled</td><td>5</td></tr>
<tr><td>User Disabled</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of a processor. However, in the graph of this measure, processor state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td></td><td><b>Speed:</b>
Indicates the current speed of this processor.</td><td>MHz</td><td>A very low value for this measure indicates that the processor is slow. If the value of this measure is 0, it indicates that the speed could not be determined.
Comparing the value of this measure across processors will point you to that processor that is very slow currently.</td></tr>
</table>

3.9 Hardware-PowerSupply Test

With the help of this measure, you can promptly detect the potential failure of any of the power supply units of a server. **This test executes only on IBM Dell servers**.

Purpose	Promptly detect the potential failure of any of the power supply units of a server
Target	A server with Dell OpenManage agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.** 3. **SNMPPORT** - The port number through which the server exposes its SNMP MIB. The

default value is 161.

4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP **v3** protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.

7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.

8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.

9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

   - **MD5** – Message Digest Algorithm
   - **SHA** – Secure Hash Algorithm

10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:

    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard

12. **ENCRYPTPASSWORD** – Specify the encryption password here.

13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

14. timeout - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default,

<table>
<tr><td></td><td colspan="3">this flag is set to **No**.</td></tr>
<tr><td>**Outputs of the test**</td><td colspan="3">One set of records for every power supply unit supported by the monitored system</td></tr>
<tr><td rowspan="2">**Measurements of the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td>**Status:**
Indicates the current status of this power supply unit.</td><td></td><td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>0</td></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Non Critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non Recoverable</td><td>6</td></tr>
</table>
Note:
This measure reports the **Measure Values** listed in the table above to indicate the current status of a power supply unit. However, in the graph of this measure, status is indicated using only the **Numeric Values** listed in the above table.</td></tr>
</table>

<table>
<tr>
<td rowspan="2"></td>
<td><b>Sensor state:</b>
Indicates the current state of this power supply sensor.</td>
<td></td>
<td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Present</td><td>1</td></tr>
<tr><td>PsFailure Detected</td><td>2</td></tr>
<tr><td>Predictive Failure</td><td>4</td></tr>
<tr><td>PsACLost</td><td>8</td></tr>
<tr><td>acLostOrOutOfRange</td><td>16</td></tr>
<tr><td>acOutOfRangeButPresent</td><td>32</td></tr>
<tr><td>Configuration Error</td><td>64</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of a sensor. However, in the graph of this measure, sensor state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td><b>Output:</b>
Indicates the maximum sustained output wattage of the power supply, in tenths of watts.</td>
<td>Watts</td>
<td></td>
</tr>
</table>

3.10 Hardware-Memory Test

This test auto-discovers the memory devices on a Dell server, and reports the current state , size, and speed of each device. **This test executes only on IBM Dell servers**.

Purpose	Auto-discovers the memory devices on a Dell server, and reports the current state , size, and speed of each device
Target	A server with Dell OpenManage agent
Agent deploying this test	Internal/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. **Ensure that the HOST is SNMP-enabled.**

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

<table>
<tr><td></td><td colspan="3">server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of records for every memory device supported by the monitored server</td></tr>
<tr><td rowspan="2"><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>State:</b>
Indicates the current state of this memory device.</td><td></td><td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Enabled</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>enabledAndNotReady</td><td>3</td></tr>
<tr><td>Not Ready</td><td>5</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of a memory device. However, in the graph of this measure, the device state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Status:</b>
Indicates the current status of this memory device.</td>
<td></td>
<td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>0</td></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Non Critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non Recoverable</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of a memory device. However, in the graph of this measure, device status is indicated using only the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Device size:</b>
Indicates the size of this memory device.</td>
<td>GB</td>
<td>If the value of this measure is 0, it indicates that no memory has been installed on the corresponding device.
Compare the value of this measure across devices to identify the device that has been installed with the maximum memory.</td>
</tr>
<tr>
<td></td>
<td><b>Speed:</b>
Indicates the speed of this memory device.</td>
<td>Nanosecs</td>
<td>A very low value is indicative of a very slow device. If the value of this measure is 0, it indicates that the speed could not be determined.
Compare the value of this meausre acrss devices to know which device isthe fastest, and which the slowest.</td>
</tr>
</table>

3.11 Hardware-Battery Test

Using this test, you can promptly identify batteries that are in a critical state and those that are not ready yet. **This test executes only on IBM Dell servers**.

Purpose	Points to batteries that are in a critical state and those that are not ready yet
Target	A server with Dell OpenManage agent

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

<table>
<tr><td></td><td colspan="3">14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.</td></tr>
<tr><td>**Outputs of the test**</td><td colspan="3">One set of records for every memory device supported by the monitored server</td></tr>
<tr><td rowspan="2">**Measurements of the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td>**State:**
Indicates the current state of this battery.</td><td></td><td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Enabled</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>enabledAndNotReady</td><td>3</td></tr>
<tr><td>Not Ready</td><td>5</td></tr>
</table>
Note:
This measure reports the **Measure Value**s listed in the table above to indicate the current state of a battery. However, in the graph of this measure, the battery state is indicated using only the **NumericS Value**s listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Status:</b>
Indicates the current status of this battery.</td>
<td></td>
<td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>0</td></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Non Critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non Recoverable</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current status of a battery. However, in the graph of this measure, battery status is indicated using only the <b>Numeric Values</b> listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Battery reading:</b>
Indicates the current reading of this battery.</td>
<td></td>
<td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Predictive failure</td><td>1</td></tr>
<tr><td>Failed</td><td>2</td></tr>
<tr><td>Present</td><td>4</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current reading level of a battery. However, in the graph of this measure, reading levels are indicated using only the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

3.12 Hardware-Amperage Test

This test reports the current state, status, and reading for each amperage probe on a Dell server. **This test executes only on IBM Dell servers.**

Purpose	Reports the current state, status, and reading for each amperage probe
Target	A server with Dell OpenManage agent

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

<table>
<tr><td></td><td colspan="3">14. <b>TIMEOUT</b> - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
15. <b>DATA OVER TCP –</b> 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 server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of records for every memory device supported by the monitored server</td></tr>
<tr><td rowspan="2"><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>State:</b>
Indicates the current state of this amperage probe.</td><td></td><td>The values this can measure report and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>0</td></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>enabledAndNotReady</td><td>3</td></tr><tr><td>Not Ready</td><td>5</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of an amperage probe. However, in the graph of this measure, the probe state is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Status:</b>
Indicates the current status of this amperage probe.</td>
<td></td>
<td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Ok</td><td>3</td></tr>
<tr><td>Non Critical Upper</td><td>4</td></tr>
<tr><td>Non Critical Lower</td><td>5</td></tr>
<tr><td>Non Recoverable Upper</td><td>6</td></tr>
<tr><td>Critical Upper</td><td>7</td></tr>
<tr><td>Critical Lower</td><td>8</td></tr>
<tr><td>Non Recoverable Lower</td><td>9</td></tr>
<tr><td>Failed</td><td>10</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of an amperage probe. However, in the graph of this measure, the probe status is indicated using only the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Amperage probe reading:</b>
Indicates the current reading of an amperage probe of type other than <i>amperageProbeTypeIsDiscrete</i>.</td>
<td>Amps</td>
<td></td>
</tr>
</table>

3.13 Dell Array Controllers Test

This test reports the current operational and error state of each of the array controllers on Dell hardware, and also reports the current configuration of each array controller, such as its type, cache size, and memory size.

Purpose	Reports the current operational and error state of each of the array controllers on Dell hardware, and also reports the current configuration of each array controller, such as its type, cache size, and memory size
Target	A server with Dell OpenManage agent

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

<table>
<tr><td></td><td colspan="3">14. <b>TIMEOUT</b> - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
15. <b>DATA OVER TCP –</b> 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 server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of records for every array controller on a Dell server</td></tr>
<tr><td><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Type:</b>
Indicates the type of this array controller.</td><td></td><td>The values this can measure report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>SCSI</td><td>1</td></tr>
<tr><td>PV660F</td><td>2</td></tr>
<tr><td>PV662F</td><td>3</td></tr>
<tr><td>IDE (Integrated / Intelligent Drive Electronics)</td><td>4</td></tr>
<tr><td>SATA (Serial Advanced Technology Attachment)</td><td>5</td></tr>
<tr><td>SAS (Serial Attached SCSI)</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the array controller type. However, in the graph of this measure, the type is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
</table>

<table>
<tr><th></th><th></th><th></th><th></th></tr>
<tr><td></td><td><b>State:</b>
Indicates the current operational state of this array controller.</td><td></td><td>The values this measure can report and their numeric equivalents are available 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>Ready</td><td>1</td></tr>
<tr><td>Failed</td><td>2</td></tr>
<tr><td>Online</td><td>3</td></tr>
<tr><td>Offline</td><td>4</td></tr>
<tr><td>Degraded</td><td>6</td></tr>
</table>

<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of an array controller. However, in the graph of this measure, the operational state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td></td><td><b>Rebuild rate:</b>
Indicates the percentage of compute cycles dedicated to rebuilding failed array disks in this array controller.</td><td>Percent</td><td>During a rebuild, the complete contents of an array disk are reconstructed. The rebuild rate, configurable between 0% and 100%, represents the percentage of the system resources dedicated to rebuilding failed array disks. At 0%, the rebuild will have the lowest priority for the controller, will take the most time to complete, and will be the setting with the least impact to system performance. A rebuild rate of 0% does not mean that the rebuild is stopped or paused.
At 100%, the rebuild will be at the highest priority for the controller, will minimize the rebuild time, and will be the setting with the most impact to system performance.</td></tr>
<tr><td></td><td><b>Cache size:</b>
Indicates the current amount of memory in the cache of this array controller.</td><td>MB</td><td></td></tr>
</table>

<table>
<tr><td></td><td><b>No of physical devices:</b>
Indicates the number of physical devices on this controller channel including both disks and the controller.</td><td>Number</td><td></td></tr>
<tr><td></td><td><b>No of logical devices:</b>
Indicates the number of virtual disks on this controller.</td><td>Number</td><td></td></tr>
<tr><td></td><td><b>Memory size:</b>
Indicates the size of this controller's memory.</td><td>MB</td><td></td></tr>
<tr><td></td><td><b>Controller status:</b>
Indicates the status of the controller itself without the Propagation of any contained component status.</td><td></td><td>The values this measure can report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>OK</td><td>3</td></tr>
<tr><td>Non-critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non-recoverable</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current status of an array controller. However, in the graph of this measure, the operational state is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

3.14 Dell Drives Test

This test reports the current state of the logical and physical drives of a disk array, and also promptly alerts administrations to current or potential contention for disk space on a disk array.

Purpose	Reports the current state of the logical and physical drives of a disk array, and also promptly alerts administrations to current or potential contention for disk space on a disk array
Target	A server with Dell OpenManage agent

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

	14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of records for every disk array on a Dell server		
Measurements	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td><b>of the test</b></td>
<td><b>Status:</b>
Indicates the current status of this disk array.</td>
<td></td>
<td>The values this can measure report and their numeric equivalents are available 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>Ready</td><td>1</td></tr>
<tr><td>Failed</td><td>95</td></tr>
<tr><td>Online</td><td>3</td></tr>
<tr><td>Offline</td><td>96</td></tr>
<tr><td>Degraded</td><td>6</td></tr>
<tr><td>Recovering</td><td>7</td></tr>
<tr><td>Removed</td><td>11</td></tr>
<tr><td>Resynching</td><td>15</td></tr>
<tr><td>Regenerating</td><td>16</td></tr>
<tr><td>FailedRedundancy</td><td>18</td></tr>
<tr><td>Rebuild</td><td>24</td></tr>
<tr><td>No Media</td><td>25</td></tr>
<tr><td>Formatting</td><td>26</td></tr>
<tr><td>Diagnostics</td><td>28</td></tr>
<tr><td>Reconstructing</td><td>32</td></tr>
<tr><td>Predictive Failure</td><td>34</td></tr>
<tr><td>Initializing Controllers</td><td>35</td></tr>
<tr><td>Backgroundinit</td><td>36</td></tr>
<tr><td>Foreign</td><td>39</td></tr>
<tr><td>Clear</td><td>40</td></tr>
<tr><td>Unsupported</td><td>41</td></tr>
<tr><td>PermanentlyDegraded</td><td>52</td></tr>
<tr><td>Incompatible</td><td>53</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the status of the disk array. However, in the graph of this measure, array status is indicated using only the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

<table>
<tr><td></td><td><b>Total size:</b>
Indicates the total size of this disk array.</td><td>MB</td><td></td></tr>
<tr><td></td><td><b>Used space:</b>
Indicates the amount of space in this disk array that is being used currently .</td><td>MB</td><td>Ideally, the value of this measure should be low.</td></tr>
<tr><td></td><td><b>Free space:</b>
Indicates the amount of space in this disk array that is currently unused.</td><td>MB</td><td>Ideally, the value of this measure should be high.</td></tr>
<tr><td></td><td><b>Severity state:</b>
Indicates whether/not this disk array is currently experiencing any critical/non-recoverable failures.</td><td>wn</td><td>The values this can measure report and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>OK</td><td>3</td></tr>
<tr><td>Non-critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non-recoverable</td><td>6</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the severity state of the disk array. However, in the graph of this measure, array status is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td></td><td><b>Speed:</b>
Indicates the speed at which this disk array is currently running.</td><td>MPS</td><td>Compare the value of this measure across disk array to know which array is currently operating at an abnormal speed.</td></tr>
<tr><td></td><td><b>Free space availability:</b>
Indicates the percentage of free space in this disk array.</td><td>Perce</td><td>A very low value or a consistent decrease in this value is a cause for concern, as it indicates a steady erosion of disk space in the array.</td></tr>
</table>

Hardware Monitoring using Integrated Management Module (IMM)

The integrated management module (IMM) consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities in a single chip on the server system board. The IMM replaces the baseboard management controller (BMC) and Remote Supervisor Adapter II in IBM® System x servers. The IMM provides the following functions:

- Around-the-clock remote access and management of your server
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems
- Web-based management with standard web browsers

The eG agent communicates with the IMM and collects the necessary hardware status information without using the IBM Director agent. Every component monitored by eG Enterprise is represented as a set of hierarchical layers, with every layer mapped to a logical group of tests that are executed on the component. The hardware tests related to IBM servers are mapped to the **Operating System** layer of the target component.

All these tests are disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the component-type for which these tests are to be enabled as the **Component type**, set *Performance* as the **Test type**, choose the tests from the **DISABLED TESTS** list, and click on the **>>** button to move the tests to the **ENABLED TESTS** list. Finally, click the **Update** button.

The hardware tests and the measures they report are discussed hereunder.

4.1 IBM - IMM Processor Test

This test indicates the current health status of each processor of the IBM server.

Purpose	Indicates the current health status of each processor of the IBM server
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the IBM server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.</td></tr>
<tr><td>**Outputs of the test**</td><td colspan="3">One set of results for every processor of the IBM server being monitored</td></tr>
<tr><td rowspan="2">**Measurements made by the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td>**Status:**
Indicates the current health status of this processor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Abnormal</td><td>0</td></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>Normal</td><td>2</td></tr></table>
Note:
This measure reports the **Measure Value**s listed in the table above to indicate the current health status of this processor. However, in the graph, this measure is indicated using the **Numeric Value**s listed in the above table.</td></tr>
</table>

4.2 IBM - IMM Temperature Test

This test reports the current health and temperature of each temperature unit. This way, administrators can identify the temperature units that are functioning abnormally.

Purpose	reports the current health and temperature of each temperature unit
Target of the test	An IBM server
Agent deploying the	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for every temperature unit of the IBM server being monitored</td></tr>
<tr><td><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Temperature:</b>
Indicates the current temperature of this temperature unit.</td><td>Celcius</td><td>A sudden increase in temperature can impact the functioning of a server and must be immediately attended to.</td></tr>
<tr><td></td><td><b>Status:</b>
Indicates the current health of this temperature unit.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Abnormal</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Normal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this temperature unit. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

4.3 IBM - IMM Voltage Test

This test monitors the current health and the voltage at which each voltage module of the IBM server is operating. Using this test, administrators are proactively alerted to fluctuations in the voltage of the voltage modules before any severe damage occurs on the IBM server.

Purpose	Monitors the current health and the voltage at which each voltage module of the IBM server is operating
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for every power supply unit of the IBM server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Voltage:</b>
Indicates the current voltage at which this voltage module is operating.</td><td>Volts</td><td></td></tr>
<tr><td></td><td><b>Status:</b>
Indicates the current health of this voltage module.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Abnormal</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Normal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current health of this voltage module. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
</table>

4.4 IBM - IMM System Test

This test monitors the IBM server and reports the current power and operating status of the server, In addition, this test will report the time elapsed since the server was last powered on and the number of times the server was restarted.

Purpose	Monitors the IBM server and reports the current power and operating status of the server, In addition, this test will report the time elapsed since the server was last powered on and the number of times the server was restarted
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for the IBM server being monitored</td></tr>
<tr><td><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Power status:</b>
Indicates the current power status of this server.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Powered Off</td><td>0</td></tr><tr><td>Powered On</td><td>255</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current power status of this server. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td></td><td><b>PoweredOn:</b>
Indicates the time elapsed since this server was last <i>Powered On</i>.</td><td>Hours</td><td></td></tr>
<tr><td></td><td><b>Restart count:</b>
Indicates the number of times the server was restarted.</td><td>Number</td><td></td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Operation status:</b>
Indicates the current operating status of this server.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>System Power Of</td><td>0</td></tr>
<tr><td>System Power On</td><td>1</td></tr>
<tr><td>System in UEFI</td><td>2</td></tr>
<tr><td>UEFI error detected</td><td>3</td></tr>
<tr><td>BootingOS</td><td>4</td></tr>
<tr><td>OSBooted</td><td>5</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current operating status of this server. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

4.5 IBM - IMM Memory Module Test

This test auto-discovers the memory modules on an IBM server, and reports the current health and size of each module.

Purpose	Auto-discovers the memory modules on an IBM server, and reports the current health and size of each module
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for every Solaris system being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status:</b>
Indicates the current health of this memory module.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Abnormal</td><td>0</td></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>Normal</td><td>100</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current health of this memory module. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td></td><td><b>Memory capacity:</b>
Indicates the size of this memory module.</td><td>GB</td><td>If the value of this measure is 0, it indicates that no memory has been installed on the corresponding module.
Compare the value of this measure across modules to identify the module that has been installed with the maximum memory.</td></tr>
</table>

4.6 IBM - IMM Fan Test

This test monitors the current health and the speed with which each fan in the IBM server is operating.

Purpose	Monitors the current health and the speed with which each fan in the IBM server is operating
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each fan in the IBM server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status:</b>
Indicates the current health of this fan.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Abnormal</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Normal</td><td>100</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this fan. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td></td><td><b>Speed:</b>
Indicates the speed at which this fan is operating.</td><td>Percent</td><td></td></tr>
</table>

4.7 IBM - IMM Power Test

This test reports the current health of each power supply unit of the IBM server.

Purpose	Reports the current health of each power supply unit of the IBM server
Target of the test	An IBM server

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

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for every power supply unit in the IBM server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status:</b>
Indicates the current health of this power supply unit.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Abnormal</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Normal</td><td>100</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this power supply unit. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

4.8 IBM - IMM Events Test

This test reports the number of events of each type that were generated by the target server.

Purpose	Reports the number of events of each type that were generated by the target server
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

	16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the IBM server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each event type occurred in the IBM server being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Number of events: Indicates the number of events of this type that occurred in this server during the last measurement period.	Number	A very low value (zero) indicates that the server is in a healthy state. The detailed diagnosis of this measure if enabled, lists the time of the event, the status of the event and the message generated for the event.

4.9 IBM - IMM HardDisk Test

This test auto-discovers the hard disks of the IBM server and reports the current health of each hard disk.

Purpose	auto-discovers the hard disks of the IBM server and reports the current health of each hard disk
Target of the test	An IBM server
Agent deploying the test	An external/remote agent

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

<table>
<tr>
<td></td>
<td colspan="3">15. <b>DATA OVER TCP –</b> 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 IBM server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td>
</tr>
<tr>
<td><b>Outputs of the test</b></td>
<td colspan="3">One set of results for each hard disk of the IBM server being monitored</td>
</tr>
<tr>
<td rowspan="2"><b>Measurements made by the test</b></td>
<td><b>Measurement</b></td>
<td><b>Measurement Unit</b></td>
<td><b>Interpretation</b></td>
</tr>
<tr>
<td><b>Disk status:</b>
Indicates the current health of this hard disk.</td>
<td>Boolean</td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Abnormal</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Normal</td><td>100</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this hard disk. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

Hardware Monitoring using iLO

Integrated Lights-Out, or iLO, is a proprietary embedded server management technology by Hewlett-Packard which provides out-of-band management facilities. The iLO software can remotely perform most functions that otherwise require a visit to the servers at the data center, computer room, or remote location.

iLO allows you to do the following:

- Monitor server health. iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. iLO also monitors firmware versions and the status of fans, memory, the network, processors, power supplies, and server hard drives.
- Access a high-performance and secure Integrated Remote Console to the server from any where in the world if you have a network connection to the server.

The eG agent communicates with the iLO and collects the necessary hardware status information without using the HP/Compaq Insight agent. Every component monitored by eG Enterprise is represented as a set of hierarchical layers, with every layer mapped to a logical group of tests that are executed on the component. The hardware tests related to Solaris servers are mapped to the **Operating System** layer of the target component.

All these tests are disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the component-type for which these tests are to be enabled as the **Component type**, set *Performance* as the **Test type**, choose the tests from the **DISABLED TESTS** list, and click on the **>>** button to move the tests to the **ENABLED TESTS** list. Finally, click the **Update** button.

The hardware tests and the measures they report are discussed hereunder.

5.1 HP - ILO Fan Test

This test monitors the overall state and the speed state of each fan in the HP server.

Purpose	Monitors the overall state and the speed state of each fan in the HP server
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b> 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 HP server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each fan in the HP server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status:</b>
Indicates the overall state of this fan.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Failed</td><td>4</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the overall state of this fan. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Speed:</b>
Indicates the speed state of this fan.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Normal</td><td>2</td></tr>
<tr><td>High</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the speed state of this fan. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

5.2 HP - ILO Sensor Temperature Test

This test reports the current state and temperature of each temperature sensor using which administrators can identify the temperature units that are functioning abnormally.

Purpose	reports the current state and temperature of each temperature sensor
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b> 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 HP server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each temperature sensor of the HP server being monitored</td></tr>
<tr><td><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Temperature:</b>
Indicates the current temperature of this temperature sensor.</td><td>Celcius</td><td>A sudden increase in temperature can impact the functioning of a server and must be immediately attended to.</td></tr>
<tr><td></td><td><b>Status:</b>
Indicates the current state of this temperature sensor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Ok</td><td>2</td></tr><tr><td>Degraded</td><td>3</td></tr><tr><td>Failed</td><td>4</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of this temperature sensor. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

5.3 HP - ILO Memory Details Test

This test reports the current state and size of each memeory module of the HP server.

Purpose	Reports the current state and size of each memeory module of the HP server
Target of the	An HP server

test	
Agent deploying the test	An external/remote agent

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

	16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the HP server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for every processor of the IBM server being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr><td><b>test</b></td><td><b>Status:</b>
Indicates the current state of this memory module.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Not present</td><td>2</td></tr>
<tr><td>Present</td><td>3</td></tr>
<tr><td>Good</td><td>4</td></tr>
<tr><td>Add</td><td>5</td></tr>
<tr><td>Upgrade</td><td>6</td></tr>
<tr><td>Missing</td><td>7</td></tr>
<tr><td>Does not match</td><td>8</td></tr>
<tr><td>Not supported</td><td>9</td></tr>
<tr><td>Bad config</td><td>10</td></tr>
<tr><td>Degraded</td><td>11</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of this memory module. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td></td><td><b>Memory size:</b>
Indicates the capacity i.e., size of this memory module.</td><td>GB</td><td>If the value of this measure is 0, it indicates that no memory has been installed on the corresponding module.
Compare the value of this measure across modules to identify the module that has been installed with the maximum memory.</td></tr>
</table>

5.4 HP - ILO Memory Summary Test

This test monitors the current health and the voltage at which each voltage module of the IBM server is operating. Using this test, administrators are proactively alerted to fluctuations in the voltage of the voltage modules before any severe damage occurs on the IBM server.

Purpose	Monitors the current health and the voltage at which each voltage module of the IBM server is operating
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

	16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the HP server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for every memory unit of the HP server being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Sockets: Indicates the number of sockets of this memory unit.	Number	
	Total memory: Indicates the total size of this memory unit.	GB	
	Operating frequency: Indicates the frequency with which this memory unit operates.	MHz	
	Operating voltage: Indicates the voltage with which this memory unit operates.	Volts	

5.5 HP - ILO System Board Controller Test

This test reports the current state of the memory array controller, current state and size of the cache module in the memory array controller.

Purpose	Reports the current state of the memory array controller, current state and size of the cache module in the memory array controller
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b> 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 HP server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for the HP server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Controller status:</b>
Indicates the current state of the memory array controller.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Failed</td><td>4</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of the memory array controller. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr><td></td><td><b>Cache module status:</b>
Indicates current state of the cache module in the memory array controller.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Ok</td><td>2</td></tr><tr><td>Degraded</td><td>3</td></tr><tr><td>Failed</td><td>4</td></tr></table><b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of the cache module in the memory array controller. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td></td><td><b>Cache module memory:</b>
Indicates the size of the cache module.</td><td>KB</td><td></td></tr>
</table>

5.6 HP -ILO Logical Drive Test

This test auto-discovers the logical drives in the HP server and reports the current state, encryption state and size of each logical drive.

Purpose	Auto-discovers the memory modules on an IBM server, and reports the current health and size of each module
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the HP server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.</td></tr>
<tr><td>**Outputs of the test**</td><td colspan="3">One set of results for each logical drive of the HP server being monitored</td></tr>
<tr><td rowspan="2">**Measurements made by the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td>**Status:**
Indicates the current state of this logical drive.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Failed</td><td>4</td></tr>
</table>
Note:
This measure reports the **Measure Value**s listed in the table above to indicate the current state of this logical drive. However, in the graph, this measure is indicated using the **Numeric Value**s listed in the above table.</td></tr>
<tr><td></td><td>**Capacity:**
Indicates the size of this logical drive.</td><td>GB</td><td>Compare the value of this measure across logical drives to identify the drive that has been allocated with the maximum memory.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Encryption status:</b>
Indicates whether/not this logical drive is encrypted.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Encrypted</td><td>2</td></tr>
<tr><td>Not encrypted</td><td>3</td></tr>
</table>

<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate whether/not this logical drive is encrypted. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

5.7 HP - ILO Physical Drive Test

This test monitors the current state, size, configuration state and temperature of each hard disk available in the HP server.

Purpose	Monitors the current state, size, configuration state and temperature of each hard disk available in the HP server
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b> 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 HP server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each hard disk available in the HP server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Status:</b>
Indicates the current state of this hard disk.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Failed</td><td>4</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of this hard disk. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td></td><td><b>Capacity:</b>
Indicates the size of this hard disk.</td><td>Percent</td><td>Compare the value of this measure across hard disks to identify the disk that has been allocated with the maximum memory.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Configuration status:</b>
Indicates whether/not this hard disk is configured in the server.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Configured</td><td>2</td></tr>
<tr><td>Not configured</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate whether/not this logical drive is encrypted. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Temperature:</b>
Indicates the current temperature of this hard disk.</td>
<td>Celcius</td>
<td></td>
</tr>
</table>

5.8 HP - ILO Power Test

This test reports the current health of each power supply unit in the chassis of the HP server.

Purpose	Reports the current health of each power supply unit in the chassis of the HP server
Target of the test	An HP server
Agent deploying the test	An external/remote agent

Configurable parameters for the test

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

<table>
<tr>
<td></td>
<td colspan="3">16. <b>DATA OVER TCP –</b> 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 HP server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td>
</tr>
<tr>
<td><b>Outputs of the test</b></td>
<td colspan="3">One set of results for each power supply unit of the HP server being monitored</td>
</tr>
<tr>
<td rowspan="2"><b>Measurements made by the test</b></td>
<td><b>Measurement</b></td>
<td><b>Measurement Unit</b></td>
<td><b>Interpretation</b></td>
</tr>
<tr>
<td><b>Present status:</b>
Indicates the availability of this power supply unit in the chassis of the server.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Absent</td><td>2</td></tr>
<tr><td>Present</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the availability of this power supply unit. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td><b>Status:</b>
Indicates the current state of this power supply unit.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Failed</td><td>4</td></tr>
</table>

<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of this hard disk. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Input main voltage:</b>
Indicates the input voltage of this power supply unit.</td>
<td>Volts</td>
<td></td>
</tr>
<tr>
<td></td>
<td><b>Power supply used:</b>
Indicates the input current of this power supply unit.</td>
<td>Watts</td>
<td></td>
</tr>
<tr>
<td></td>
<td><b>Maximum capacity:</b>
Indicates the maximum input current that is allowed to pass through this power supply unit.</td>
<td>Watts</td>
<td></td>
</tr>
</table>

<table>
<tr>
<td></td>
<td><b>Pluggable status:</b>
Indicates whether/not this power supply unit is hot pluggable.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Non hotpluggable</td><td>2</td></tr>
<tr><td>Hotpluggable</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate whether/not this power supply unit is hot pluggable. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

5.9 HP - ILO Drive Test

This test auto-discovers the drive enclosures of the HP server and reports the current state, fan status and temperature of each drive enclosure.

Purpose	auto-discovers the drive enclosures of the HP server and reports the current state, fan status and temperature of each drive enclosure.
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the HP server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.</td></tr>
<tr><td>**Outputs of the test**</td><td colspan="3">One set of results for each enclosure of the HP server being monitored</td></tr>
<tr><td rowspan="2">**Measurements made by the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td>**Status:**
Indicates the current state of this enclosure.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Ok</td><td>2</td></tr><tr><td>Degraded</td><td>3</td></tr><tr><td>Failed</td><td>4</td></tr></table>
Note:
This measure reports the **Measure Value**s listed in the table above to indicate the current state of this enclosure. However, in the graph, this measure is indicated using the **Numeric Value**s listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Fan status:</b>
Indicates the current state of the fans in this enclosure.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>No fan</td><td>4</td></tr>
<tr><td>Degraded</td><td>5</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of the fans in this enclosure. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Temperature status:</b>
Indicates the temperature status of this enclosure.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>No Temp</td><td>5</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the temperature status of this enclosure. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

	Drive bays: Indicates the number of bays i.e., slots in this enclosure.	Number	

5.10 HP - ILO Processors Test

This test auto-discovers the processors of the HP server and reports the current state and speed of each processor.

Purpose	auto-discovers the processors of the HP server and reports the current state and speed of each processor
Target of the test	An HP server
Agent deploying the test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the HP server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.</td></tr>
<tr><td>**Outputs of the test**</td><td colspan="3">One set of results for each processor of the being monitored</td></tr>
<tr><td>**Measurements made by the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td></td><td>**Status:**
Indicates the current state of this processor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Disabled</td><td>5</td></tr>
</table>
Note:
This measure reports the **Measure Values** listed in the table above to indicate the current state of this processor. However, in the graph, this measure is indicated using the **Numeric Values** listed in the above table.</td></tr>
<tr><td></td><td>**Speed:**
Indicates the speed of this processor.</td><td>MHz</td><td></td></tr>
<tr><td></td><td>**External frequency:**
Indicates the current speed of this processor on the processor bus.</td><td>MHz</td><td></td></tr>
</table>

5.11 HP - ILO Event Test

This test reports the number of events of each type that were generated by the target server.

Purpose	Reports the number of events of each type that were generated by the target server
Target of the test	An HP server
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the HP server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the HP server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3.** 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **INCLUDE INFO** – Specify a comma separated list of events for which this test should report metrics. Each event specified in this list box will be listed as a descriptor of this test. 16. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	17. **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 HP server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the each event type occurred in the HP server being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Event: Indicates the number of events of this type that occurred in this server during the last measurement period.	Number	A very low value (zero) indicates that the server is in a healthy state. The detailed diagnosis of this measure if enabled, lists the time of the event, the status of the event and the message generated for the event.

Hardware Monitoring using ILOM

ILOM enables you to actively manage and monitor the Solaris server independently of the operating system state, providing you with a reliable Lights Out Management (LOM) system. With ILOM, you can proactively:

- Learn about hardware errors and faults as they occur
- Remotely control the power state of your server
- View the graphical and non-graphical consoles for the host
- View the current status of sensors and indicators on the system
- Determine the hardware configuration of your system
- Receive generated alerts about system events in advance via IPMI PETs, SNMP Traps, or Email Alerts.

The eG agent communicates with the ILOM and collects the necessary hardware status information independently. Every component monitored by eG Enterprise is represented as a set of hierarchical layers, with every layer mapped to a logical group of tests that are executed on the component. The hardware tests related to Solaris servers are mapped to the **Operating System** layer of the target component.

All these tests are disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the component-type for which these tests are to be enabled as the **Component type**, set *Performance* as the **Test type**, choose the tests from the **DISABLED TESTS** list, and click on the **>>** button to move the tests to the **ENABLED TESTS** list. Finally, click the **Update** button.

The hardware tests and the measures they report are discussed hereunder.

6.1 ILOM Fan Test

This test reports the admin, operating and health states of each fan module present in the Solaris server.

Purpose	Reports the admin, operating and health states of each fan module present in the Solaris server
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with

<table>
<tr><td></td><td colspan="3">the server. This parameter is specific to SNMP <b>v1</b> and <b>v2</b> only. Therefore, if the <b>SNMPVERSION</b> chosen is <b>v3</b>, then this parameter will not appear.
7. <b>USERNAME</b> – This parameter appears only when <b>v3</b> is selected as the <b>SNMPVERSION</b>. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the <b>USERNAME</b> parameter.
8. <b>AUTHPASS</b> – Specify the password that corresponds to the above-mentioned <b>USERNAME</b>. This parameter once again appears only if the snmpversion selected is <b>v3</b>.
9. <b>CONFIRM PASSWORD</b> – Confirm the <b>AUTHPASS</b> by retyping it here.
10. <b>AUTHTYPE</b> – This parameter too appears only if <b>v3</b> is selected as the <b>SNMPVERSION</b>. From the <b>AUTHTYPE</b> 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:
➢ <b>MD5</b> – Message Digest Algorithm
➢ <b>SHA</b> – Secure Hash Algorithm
11. <b>ENCRYPTFLAG</b> – This flag appears only when <b>v3</b> is selected as the <b>SNMPVERSION</b>. By default, the eG agent does not encrypt SNMP requests. Accordingly, the <b>ENCRYPTFLAG</b> is set to <b>NO</b> by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the <b>YES</b> option.
12. <b>ENCRYPTTYPE</b> – If the <b>ENCRYPTFLAG</b> is set to <b>YES</b>, then you will have to mention the encryption type by selecting an option from the <b>ENCRYPTTYPE</b> list. SNMP v3 supports the following encryption types:
➢ <b>DES</b> – Data Encryption Standard
➢ <b>AES</b> – Advanced Encryption Standard
13. <b>ENCRYPTPASSWORD</b> – Specify the encryption password here.
14. <b>CONFIRM PASSWORD</b> – Confirm the encryption password by retyping it here.
15. <b>TIMEOUT -</b> Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
16. <b>DATA OVER TCP –</b> 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 Solaris server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each fan module of the Solaris server being monitored</td></tr>
<tr><td><b>Measurements</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
</table>

<table>
<tr>
<td rowspan="2">of the <i>test</i></td>
<td><b>Admin state:</b>
Indicates the current admin state of this fan module.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the admin state of this fan module. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td><b>Operation status:</b>
Indicates whether/not this fan module is enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not this fan module is enabled. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this fan module.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this fan module. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

6.2 ILOM Hard Disk Test

This test reports the admin, operating and health states of each hard disk present in the Solaris server.

Purpose	Reports the admin, operating and health states of each hard disk present in the Solaris server
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from

	this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3.** 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Solaris server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each hard disk of the Solaris server being monitored

<table>
<tr><th>Measurements of the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td><b>Admin state:</b>
Indicates the current admin state of this hard disk.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the admin state of this fan module. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td></td><td><b>Operation status:</b>
Indicates whether/not this hard disk is enabled.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate whether/not this fan module is enabled. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this hard disk.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this hard disk. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
</table>

6.3 ILOM Power Supply Test

This test reports the admin, operating and health states of each power supply unit present in the Solaris server.

Purpose	Reports the admin, operating and health states of each power supply unit present in the Solaris server
Target	A Solaris server
Agent deploying this test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
16. <b>DATA OVER TCP –</b> 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 Solaris server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each power supply unit of the Solaris server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Admin state:</b>
Indicates the current admin state of this power supply unit.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the admin state of this power supply unit. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Operation status:</b>
Indicates whether/not this power supply unit was enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not this fan module is enabled. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this power supply unit.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current health of this power supply unit. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

6.4 ILOM Server CPU Test

This test reports the admin, operating and health states of each processor present in the Solaris server.

Purpose	Monitors the status of each of the cooling units/fans on a server
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3.** 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the

<table>
<tr>
<td></td>
<td colspan="3">
encryption type by selecting an option from the <b>ENCRYPTTYPE</b> list. SNMP v3 supports the following encryption types:
➢ <b>DES</b> – Data Encryption Standard
➢ <b>AES</b> – Advanced Encryption Standard
13. <b>ENCRYPTPASSWORD</b> – Specify the encryption password here.
14. <b>CONFIRM PASSWORD</b> – Confirm the encryption password by retyping it here.
15. <b>TIMEOUT -</b> Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the <b>TIMEOUT</b> text box. The default is 10 seconds.
16. <b>DATA OVER TCP –</b> 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 Solaris server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.
</td>
</tr>
<tr>
<td><b>Outputs of the test</b></td>
<td colspan="3">One set of results for each processor of the Solaris server being monitored</td>
</tr>
<tr>
<td rowspan="2"><b>Measurements of the test</b></td>
<td><b>Measurement</b></td>
<td><b>Measurement Unit</b></td>
<td><b>Interpretation</b></td>
</tr>
<tr>
<td><b>Admin state:</b>
Indicates the current admin state of this processor.</td>
<td></td>
<td>
The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the admin state of this processor. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td><b>Operation status:</b>
Indicates whether/not this processor is enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not this processor is enabled. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this processor.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current health of this processor. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

6.5 ILOM Fan Sensor Test

This test reports the admin, operating and health states of each fan sensor present in the Solaris server. In addition, this test helps administrators figure out the fan that is experiencing fluctuations in speed.

Purpose	Reports the admin, operating and health states of each fan sensor present in the Solaris server. In addition, this test helps administrators figure out the fan that is experiencing fluctuations in speed.
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted,

select the **YES** option.

12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Solaris server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

<table>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each fan sensor of the Solaris server</td></tr>
<tr><td rowspan="2"><b>Measurements of the test</b></td><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td><b>Admin state:</b>
Indicates the current admin state of this fan sensor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the admin state of this fan sensor. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Operation status:</b>
Indicates whether/not this fan sensor is enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not this fan sensor is enabled. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this fan sensor.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current health of this fan sensor. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

	Speed: Indicates the current speed of the fan associated with this fan sensor.	RPM	
	Sensor latency: Indicates the average latency of this fan sensor.	millisec	

6.6 ILOM Power Sensor Test

This test reports the admin, operating and health states of each power sensor present in the Solaris server. In addition, this test reports the input current and average latence of each power sensor.

Purpose	Monitors the status of each of the controllers of drive arrays on a server
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**.

	From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Solaris server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each power sensor of the Solaris server being monitored		
Measurements	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td rowspan="2">**of the test**</td>
<td>**Admin state:**
Indicates the current admin state of this power sensor.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
Note:
This measure reports the **Measure Values** listed in the table above to indicate the admin state of this power sensor. However, in the graph, this measure is indicated using the **Numeric Values** listed in the above table.</td>
</tr>
<tr>
<td>**Operation status:**
Indicates whether/not this power sensor is enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
Note:
This measure reports the **Measure Values** listed in the table above to indicate whether/not this power sensor is enabled. However, in the graph, this measure is indicated using the **Numeric Values** listed in the above table.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this power sensor.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this power sensor. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Sensor reading:</b>
Indicates the input current to this power sensor.</td>
<td>Amps</td>
<td></td>
</tr>
<tr>
<td></td>
<td><b>Sensor latency:</b>
Indicates the average latency of this power sensor.</td>
<td>millisec</td>
<td></td>
</tr>
</table>

6.7 ILOM Temperature Sensor Test

This test reports the admin, operating, health state of each temperature sensor present in the Solaris server. Using this test, administrators can be proactively alerted to the temperature sensor that has been constantly experiencing temperature fluctuations.

Purpose	Monitors the overall health of logical and physical drives of a disk array
Target	A Solaris server
Agent deploying this test	An external/remote agent

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

<table>
<tr><td></td><td colspan="3">16. <b>DATA OVER TCP –</b> 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 Solaris server over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each temperature sensor of the Solaris server being monitored</td></tr>
<tr><td rowspan="2"><b>Measurements of the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Admin state:</b>
Indicates the current admin state of this temperature sensor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Locked</td><td>1</td></tr><tr><td>Unlocked</td><td>2</td></tr><tr><td>ShuttingDown</td><td>3</td></tr></table><b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the admin state of this temperature sensor. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

<table>
<tr>
<td></td>
<td><b>Operation status:</b>
Indicates whether/not this temperature sensor is enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not this temperature sensor is enabled. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Health status:</b>
Indicates the current health of this temperature sensor.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>1</td></tr>
<tr><td>Major</td><td>2</td></tr>
<tr><td>Minor</td><td>3</td></tr>
<tr><td>Normal</td><td>4</td></tr>
<tr><td>Warning</td><td>5</td></tr>
<tr><td>Pending</td><td>6</td></tr>
<tr><td>Cleared</td><td>7</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current health of this temperature sensor. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

	Temperature: Indicates the current temperature of this temperature sensor.	Degree Celcius	
	Sensor latency: Indicates the average latency of this temperature sensor.	millisec	

6.8 ILOM Voltage Sensor Test

This test reports the admin, operating, health state of each voltage sensor present in the Solaris server. Using this test, administrators can be proactively alerted to the voltage sensor that has been constantly experiencing voltage fluctuations.

Purpose	Monitors the current status and speed of the voltage sensors present in the solaris server
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME.** This parameter once again appears only if the snmpversion selected is **v3.** 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.

	10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Solaris server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for each voltage sensor of the Solaris server being monitored		
Measurements	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>of the test</td>
<td><b>Admin state:</b>
Indicates the current admin state of this voltage sensor.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Locked</td><td>1</td></tr>
<tr><td>Unlocked</td><td>2</td></tr>
<tr><td>ShuttingDown</td><td>3</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the admin state of this voltage sensor. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
<tr>
<td></td>
<td><b>Operation status:</b>
Indicates whether/not this voltage sensor is enabled.</td>
<td></td>
<td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>1</td></tr>
<tr><td>Enabled</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate whether/not this voltage sensor is enabled. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td>
</tr>
</table>

<table>
<tr><td rowspan="3"></td><td><b>Health status:</b>
Indicates the current health of this voltage sensor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Critical</td><td>1</td></tr><tr><td>Major</td><td>2</td></tr><tr><td>Minor</td><td>3</td></tr><tr><td>Normal</td><td>4</td></tr><tr><td>Warning</td><td>5</td></tr><tr><td>Pending</td><td>6</td></tr><tr><td>Cleared</td><td>7</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this temperature sensor. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td><b>Voltage:</b>
Indicates the current voltage of this voltage sensor.</td><td>Volts</td><td></td></tr>
<tr><td><b>Sensor latency:</b>
Indicates the average latency of this voltage sensor.</td><td>millisec</td><td></td></tr>
</table>

6.9 ILOM Server power Test

This test reports the current power consumption and maximum power that can be consumed by the target Solaris server.

Purpose	Reports the current power consumption and maximum power that can be consumed by the target Solaris server
Target	A Solaris server

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

	14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Solaris server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the target Solaris server being monitored		
Measurements of the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Actual power consumption: Indicates the actual input power comsumed by the server.	Watts	
	Max permitted power: Indicates the maximum input power that can be consumed by the server at any instance.	Watts	

6.10 ILOM Battery Test

This test reports the current status of each battery in the target Solaris server.

Purpose	Reports the current status of each battery in the target Solaris server
Target	A Solaris server
Agent deploying this test	An external/remote agent
Configurable parameters for this test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Solaris server 3. **MANAGEMENT CARD IP** – Specify the IP address of the target server's management card here. By default, the eG agent communicates with the target server through this card and collects the required metrics. 4. **SNMPPORT** – The SNMP Port number of the Solaris server (161 typically) 5. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

	6. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 7. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME.** This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Solaris server over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of records for each battery of the Solaris server to be monitored

<table>
<tr><th rowspan="2">Measurements of the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td><b>Battery status:</b>
Indicates the current state of this battery.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Critical</td><td>0</td></tr>
<tr><td>Low</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Full charged</td><td>3</td></tr>
<tr><td>Charging</td><td>6</td></tr>
<tr><td>Charging and high</td><td>7</td></tr>
<tr><td>Charging and low</td><td>8</td></tr>
<tr><td>Charging and critical</td><td>9</td></tr>
<tr><td>Undefined</td><td>10</td></tr>
<tr><td>Partially charged</td><td>11</td></tr>
<tr><td>Other</td><td>12</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of this battery. However, in the graph, this measure is indicated using the <b>Numeric Values</b> listed in the above table.</td></tr>
</table>

6.11 Benefits

Using the eG Enterprise suite, administrators can:

- Monitor the status and performance of multi-vendor, multi-platform hardware components at anytime, from anywhere, from a central web console. This ensures that administrators do not need different monitoring consoles for different types of hardware.

- Collect, consolidate, and present a wealth of performance results pertaining to the monitored hardware. This information is critical for historical analysis, trending, and proactive planning, so that server downtimes can be minimized.
- Look across hardware and software layers of a server, automatically correlate performance across these layers, and accurately identify problem areas. Administrators can thus focus their attention on the key bottlenecks and ensure better performance of the servers and applications, and thereby enhance service uptime.
- Instantly be notified of hardware and software issues, in many cases well before the actual failure occurs. Administrators can thus initiate corrective actions very early in the process, thereby ensuring minimal or no impact on the service performance seen by users.

Chapter

2

Conclusion

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

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