Monitoring Dell EqualLogic

eG Enterprise v6.0

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 2003, and Windows 2000 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

Table of Figures

Chapter 1

Monitoring the Dell EqualLogic PS Series SAN Storage

The Dell EqualLogic PS Series of iSCSI storage arrays is built on a patented peer storage architecture and offers enterprise-class performance and reliability, automation, and virtualization of storage for simplified storage management.

Designed to meet the requirements of the data center, EqualLogic engineered fault tolerance into the PS Series hardware design. Its components are fully redundant and hot swappable with dual controllers, standard dual fan trays, and dual power supplies standard. The hot-swappable controller module features dual-core 64-bit processors with a HyperTransport™ I/O bus and twin 64-bit double data rate (DDR) channels. Each control module is equipped with 1GB of battery-backed DRAM. Each disk drive is interconnected with its own independent, hot-swappable serial channel and secured mechanically with an inertial dampening chassis that helps eliminate drive vibrations. Self-tuning controller caches are battery-backed and mirrored across controllers.

EqualLogic PS Series arrays support Serial Attached SCSI (SAS) and Serial ATA (SATA) disk drives. Enterprise-class RAID protection governs hot-swappable disk drives, including RAID-5, RAID-10, and RAID-50 support.

Owing to its fault-tolerant hardware architecture and the high level of data protection and performance it delivers, the EqualLogic SAN is used extensively in providing reliable storage services to enterprises where mission-critical applications are operational. If the storage device were to fail or under-perform in such environments, it is bound to result in the loss of critical data, which in turn can bring these critical applications and their dependent services to a virtual standstill. To avoid such a catastrophy, it is essential to monitor the SAN storage device continuously.

eG Enterprise offers a specialized *Dell EqualLogic* monitoring model that monitors the core functions and components of the storage device, and proactively alerts administrators to issues in its overall performance and its critical operations, so that the holes are plugged before any data loss occurs.

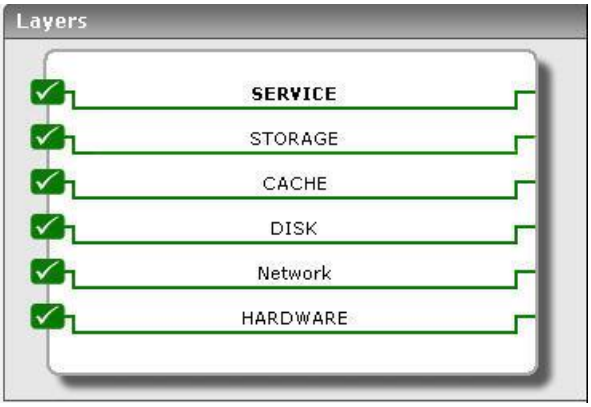

Figure 1.1: The layer model of the Dell EqualLogic SAN storage

Each layer of this model is mapped to tests that monitor a critical component of the device such as the disks, the caches, the storage processors, etc. To collect the required metrics from the device, eG periodically polls the SNMP MIB of the device. The key pre-requisite for monitoring the storage device therefore, is to enable **SNMP-enable** the storage device.

Once this is done, the eG agent will extract useful statistics from the storage system and report it to the eG manager.

Using these metrics, the following critical performance queries can be answered:

- Is the storage device available over the network?
- Is the device responding quickly to client requests or are requests to the device experiencing significant latencies?
- How many controllers and disks does the device's chassis contain?
- Are the fans in the storage device operating at normal speeds? Is any fan in an abnormal state?
- Have any hardware failures occurred recently? If so, which hardware failed?
- Are all power supply units in the storage device functioning smoothly, or has any unit failed?
- Is any fan in the power supply unit not operational now?
- Are the temperature sensors in the device registering normal temperatures, or is any sensor in an abnormal state currently?
- Does the storage device have adequate disk space resources, or has too much disk space being consumed?
- Are all disks in the storage device healthy, or are there any unhealthy disks?
- Do any disks have errors?
- Has the RAID failed?
- Are sufficient spare disks available to take the place of ones that may fail?
- Is the controller cache adequately sized?
- Does the group's storage pool have enough disk space resources? Has the pool been over-utilized?
- How many snapshots in the group are currently in use?
- How many volumes in the group are currently in use?

- Is the storage device overloaded with connections from initiators?
- Is the storage device experiencing any read/write latencies?
- Do the controllers supported by the storage device have enough battery backup? Does any controller have a low voltage or a missing battery?
- Is any controller's processor experiencing abnormal temperatures?
- Of the controllers in the storage device, which one is the primary controller and the secondary controller?
- Is the storage device healthy?
- Is the temperature of the member array good or bad?
- Is the member array experiencing any disk space shortage?

The sections that will follow discuss each of the layers of Figure 1.1 in great detail.

1.1 The Hardware Layer

Using the test mapped to this layer, you can proactively capture the potential failue of the core hardware components of the Dell EqualLogic PS Series SAN device.

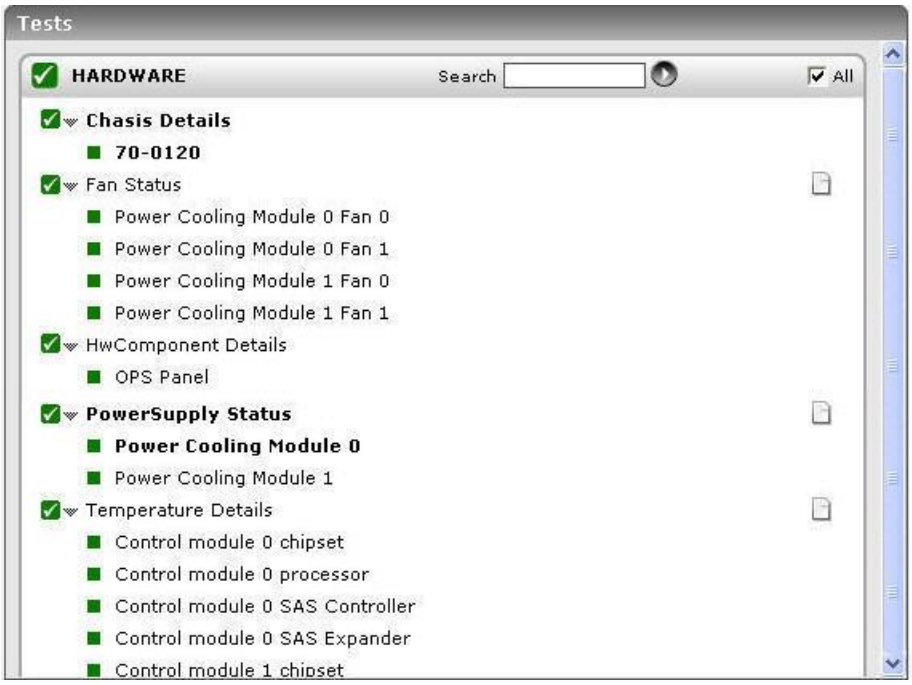

Figure 1.2: The test associated with the Hardware layer

1.1.1 EQ Chassis Test

The chassis refers to the rigid framework that contains disks, controllers, NICs, spindles, fans, and power supplies of the SAN device. Using this test, you can determine the number of disks and controllers inside the chassis being monitored.

Purpose	Reports the number of disks and controllers inside the chassis being monitored
Target of the test	A Dell EqualLogic PS Series SAN
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 Dell EqualLogic chassis being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Number of controllers: Indicates the number of controllers currently in the chassis.	Number	
	Number of disks: Indicates the number of disks currently in the chassis.	Number	

1.1.2 EQ Fans Test

This test reports the speed of each fan and the status of each fan sensor in the storage device.

Purpose	Reports the speed of each fan and the status of each fan sensor in the storage device
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 equalizer 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 fan in the storage device 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>Speed:
Indicates the current speed of this fan.</td><td>Rpm</td><td>Abnormally high and low values for this measure are a cause for concern.</td></tr>
<tr><td></td><td>Current state:
Indicates the current state of the fan.</td><td></td><td>This measure reports one of the following values as the status of this fan:
Unknown
Normal
Warning
Critical
The numeric values that correspond to the above-mentioned states are as follows:<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Critical</td><td>3</td></tr></table>Note:
By default, this measure reports the above-mentioned states while indicating the status of the fan. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only - i.e., 0 to 3.</td></tr>
</table>

1.1.3 EQ Hardware Test

This test promptly alerts you to the failure of critical hardware components of the SAN device, such as panels, fans, and power supplies.

Purpose	Promptly alerts you to the failure of critical hardware components of the storage device, such as panels, fans, and power supplies
Target of the test	A Dell EqualLogic PS Series SAN
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 equalizer 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 fan in the storage device 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 hardware.</td><td></td><td>This measure reports one of the following values as the hardware status:
Unknown
Not Present
Failed
Good
The numeric values that correspond to the above-mentioned states are as follows:<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Not Present</td><td>1</td></tr><tr><td>Failed</td><td>2</td></tr><tr><td>Good</td><td>3</td></tr></table>Note:
By default, this measure reports the above-mentioned states while indicating the status of a hardware. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only - i.e., 0 to 3.</td></tr>
</table>

1.1.4 EQ Power Supplies Test

This test auto-discovers the power supply units in the storage device, and reports the current state of each unit and the operating state of the fan in each unit.

Purpose	Auto-discovers the power supply units in the storage device, and reports the current state of each unit and the operating state of the fan in each unit
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 equalizer 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 power supply unit in the storage device 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>Current status:
Indicates the current state of this power supply unit.</td><td></td><td>This measure reports one of the following values as the status of the power supply unit:
On
No Ac Power
Failed
No Data
The numeric values that correspond to the above-mentioned states are as follows:<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>On</td><td>1</td></tr><tr><td>No Ac Power</td><td>2</td></tr><tr><td>Failed</td><td>3</td></tr><tr><td>No Data</td><td>4</td></tr></table>Note:

By default, this measure reports the above-mentioned states while indicating the status of a power supply unit. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only - i.e., 1 to 4.</td></tr>
</table>

	Fan status: Indicates the current operational state of the fan in this power supply unit.		This measure reports one of the following values as the operating status of the fan in the power supply unit: • Not Applicable • Fan is Operational • Fan is not Operational The numeric values that correspond to the above-mentioned states are as follows: <table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Not Applicable</td><td>0</td></tr><tr><td>Fan is Operational</td><td>1</td></tr><tr><td>Fan is not Operational</td><td>2</td></tr></table> **Note:** By default, this measure reports the above-mentioned states while indicating the fan status. However, in the graph of this measure, these states will be represented using their corresponding numeric equivalents only - i.e., 0 to 2.

1.1.5 EQ Temperature Test

This test reports the current state and temperature of each temperature sensor in the storage device.

Purpose	Reports the current state and temperature of each temperature sensor in the storage device
Target of the test	A Dell EqualLogic PS Series SAN
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 equalizer 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 temperature sensor in the storage device 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>Temperature:
Indicates the current temperature of this sensor.</td><td>Celcisu</td><td>A very high value is cause for concern.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Status:
Indicates the current state of this sensor.</td>
<td></td>
<td>This measure reports one of the following values as the current state of the temperature sensor:
• Unknown
• Normal
• Warning
• Critical
The numeric values that correspond to the above-mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Critical</td><td>3</td></tr></table>
Note:

By default, this measure reports the above-mentioned states while indicating the sensor status. However, in the graph of this measure, these states will be represented using their corresponding numeric equivalents only - i.e., 0 to 3.</td>
</tr>
</table>

1.2 The Network Layer

Monitor the availability of the EqualLogic SAN over the network using the test mapped to this layer.

Figure 1.3: The test mapped to the EMC Network layer

Since the test mapped to this layer has already been dealt with in the other documents, let us proceed to the next layer.

1.3 The Disk Layer

Using the tests mapped to this layer, you can isolate the following problem conditions instantly:

- Quickly detect disk space contentions in the storage device;
- Rapidly identify unhealthy disks in the device;
- Promptly capture RAID failures

Figure 1.4: The test mapped to the Disks layer

1.3.1 EQ Disk Usage Test

Adequate space should be available in the storage device to ensure the uninterrupted functioning of the mission-critical applications that are using the storage services provided by the device. If the device runs out of space, then administrators should be intimated of the space crunch promptly so that, disk space in the device can be enhanced before service levels start taking a turn for the worse! This test periodically checks the space usage in the device and proactively alerts administrators to potential disk space contentions so that, amends are made before application performance deteriorates.

Purpose	Periodically checks the space usage in the device and proactively alerts administrators to potential disk space contentions so that, amends are made before application performance deteriorates
Target of the test	A Dell EqualLogic SAN device
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 storage device being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total storage: Indicates the total disk space currently available in the device.	GB	
	Used storage: Indicates the total disk space currently in use.	GB	Ideally, the value of this measure should be low. If this value grows close to that of the **Total storage** measure, then you may want to consider to add more storage to the storage device, or free space in the storage device by deleting unnecessary data.
	Snap storage: Indicates the total disk space currently allocated for volume snapshots.	GB	Snapshots are typically used for quick recovery and offloading backup operations. If the storage device appears to be running out of space, then, the value of this measure will indicate if the volume snapshots have in any way contributed to the space crunch.
	Replication storage: Indicates the total disk space currently allocated for volume replication.	GB	EqualLogic's Auto-Replication remotely replicates data from one PS Group to another over a standard IP network over long distances, helping provide high levels of data protection and disaster tolerance. In the event of a space contention on the storage device, the value of this measure will enable you to ascertain whether volume replicas are occupying too much space in the storage device.

1.3.2 EQ Disks Test

This test auto-discovers the disks in the storage device, and reports the size, status, errors, and the level of I/O activity on each disk. With the help of this test, you can accurately identify unhealthy disks and disks that are prone to errors. You can also use this test to determine whether I/O load is uniformly distributed across all disks, and in the process isolate irregularities in load-balancing.

Purpose	Auto-discovers the disks in the storage device, and reports the size, status, errors, and the level of I/O activity on each disk
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 disk in the storage device being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Disk size: Indicates the size of this disk.	GB	
	Disk status: Indicates the current state of this disk.		This measure reports one of the following values as the current state of a disk: • Online • Spare • Failed • Offline • Alt-Sig • TooSmall • History of Failures • Unsupported • Unhealthy • Replacement

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>The numeric values that correspond to the above-mentioned states are as follows:

<table>
<tr><th>State</th><th>Numeric Value</th></tr>
<tr><td>Online</td><td>1</td></tr>
<tr><td>Spare</td><td>2</td></tr>
<tr><td>Failed</td><td>3</td></tr>
<tr><td>Offline</td><td>4</td></tr>
<tr><td>Alt-Sig</td><td>5</td></tr>
<tr><td>TooSmall</td><td>6</td></tr>
<tr><td>History of Failures</td><td>7</td></tr>
<tr><td>Unsupported</td><td>8</td></tr>
<tr><td>Unhealthy</td><td>9</td></tr>
<tr><td>Replacement</td><td>10</td></tr>
</table>

Note:

By default, this measure reports the above-mentioned states while indicating the disk status. However, in the graph of this measure, these states will be represented using their corresponding numeric equivalents only - i.e., 0 to 10.</td>
</tr>
<tr>
<td></td>
<td>Disk errors:
Indicates the number of errors that have occurred in this disk during the last measurement period.</td>
<td>Number</td>
<td>Ideally, the value of this measure should be 0.</td>
</tr>
<tr>
<td></td>
<td>Bytes read:
Indicates the number of bytes of data read from this disk during the last measurement period.</td>
<td>MB</td>
<td>These measures are good indicators of the I/O load on a disk.</td>
</tr>
</table>

	Bytes write: Indicates the number of bytes of data written to this disk during the last measurment period.	MB	

1.3.3 EQ Raid Test

The disks in EqualLogic are automatically protected with RAID (RAID 10, RAID 5, or RAID 50) and hot spares. This test monitors this protective shield by periodically checking the status of the RAID and the number of hot spares available, and promptly reporting RAID failures.

Purpose	Periodically checks the status of the RAID and the number of hot spares available, and promptly reports RAID failures
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 storage device monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>test</td>
<td>Status:
Indicates the current state of the RAID.</td>
<td></td>
<td>This measure reports one of the following values as the current state of the RAID:
• ok
• Degraded
• Verifying
• Reconstructing
• Failed
• Catastrophic Loss
• Expanding
• Mirroring
The numeric values that correspond to the above-mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>ok</td><td>1</td></tr><tr><td>Degraded</td><td>2</td></tr><tr><td>Verifying</td><td>3</td></tr><tr><td>Reconstructing</td><td>4</td></tr><tr><td>Failed</td><td>5</td></tr><tr><td>Catastrophic Loss</td><td>6</td></tr><tr><td>Expanding</td><td>7</td></tr><tr><td>Mirroring</td><td>8</td></tr></table>Note:
By default, this measure reports the above-mentioned states while indicating the RAID status. However, in the graph of this measure, these states will be represented using their corresponding numeric equivalents only - i.e., 1 to 8.</td>
</tr>
</table>

	Number of spares: Indicates the number of disks that are currently allotted as spares in the RAID.	Number	If a drive fails in a RAID array that includes redundancy--meaning all of them except RAID 0--it is desirable to get the drive replaced immediately so the array can be returned to normal operation. There are two reasons for this: fault tolerance and performance. If the drive is running in a degraded mode due to a drive failure, until the drive is replaced, most RAID levels will be running with no fault protection at all: a RAID 1 array is reduced to a single drive, and a RAID 3 or RAID 5 array becomes equivalent to a RAID 0 array in terms of fault tolerance. At the same time, the performance of the array will be reduced, sometimes substantially. An extremely useful RAID feature that helps alleviate this problem is the use of *hot spares*. Additional drives are attached to the controller and left in a "standby" mode. If a failure occurs, the controller can use the spare drive as a replacement for the bad drive. Moreover, with a controller that supports hot sparing, rebuild will be *automatic*. If the controller detects that a drive has gone down, it disables it, and immediately rebuilds the data onto the hot spare.

1.4 The Cache Layer

You will be able to determine the mode of each cache controller and also figure out which cache is badly sized with the help of the test associated with this layer.

Figure 1.5: The test mapped to the Cache layer

1.4.1 EQ Cache Test

Each PS Series array is composed of controllers with mirrored battery-backed caches. Cache memory in the controller enhances read and write performance, improving overall storage throughput. Streaming data can be queued into the cache to dramatically accelerate read performance. This test monitors each controller cache in the storage device and reports its size and mode.

Purpose	Monitors each controller cache in the storage device and reports its size and mode
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 equalizer 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 cache in the storage device 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>Cache size:
Indicates the current size of this cache.</td><td>GB</td><td>Ideally, the value of this measure should be high. If the cache is not adequately sized, read/write performance will suffer.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Cache mode:
Indicates the current mode of this cache.</td>
<td></td>
<td>This measure reports one of the following values as the cache mode:
• Unknown
• Write Through
• Write Back

When write-through cache is turned on, the RAID controller writes data straight through the cache - directly to the disks - before informing the host that the write was committed.

For performance-critical applications, the cache memory can be used to accelerate write speeds with a configuration called write-back cache. In this mode, data is considered committed, or successfully received, as soon as the controller writes back to the host that the information has been received in cache memory.

The numeric values that correspond to the above-mentioned modes are as follows:

<table>
<tr><th>Mode</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0</td></tr>
<tr><td>Write Through</td><td>1</td></tr>
<tr><td>Write Back</td><td>2</td></tr>
</table>

Note:

By default, this measure reports the above-mentioned modes while indicating the cache modes. However, in the graph of this measure, these modes will be represented using their corresponding numeric equivalents only - i.e., 0 to 2.</td>
</tr>
</table>

1.5 The Storage Layer

A PS Series group is comprised of a single PS Series array or multiple arrays working together. This layer monitors the space usage in the group storage pool, and also reports the number of snapshots and volumes in the group that are currently online or are in use.

Figure 1.6: The tests mapped to the Storage layer

1.5.1 EQ Group Pools Test

The EqualLogic iSCSI SAN's unique peer storage architecture consolidates all storage resources into an easy-to-manage tiered storage pool, securely accessed by servers across a standard Ethernet network.

A PS Series group is comprised of a single PS Series array or multiple arrays working together. When an array is configured as a group member, its RAID-protected disk space is added to the group's storage pool.

Sufficient storage resources should always be available in the pool so that, applications depending upon the pool can function without a glitch. A sudden or consistent erosion of disk space in the pool can have disastrous effects on application performance. This test enables you to keep track of the space usage on the group's storage pool so that, you can detect and fix a space drain before it is too late.

Purpose	Enables you to keep track of the space usage on the group's storage pool so that, you can detect and fix a space drain before it is too late
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 storage device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total space: Indicates the total amount of space in the group storage pool currently.	GB	
	Used space: Indicates the total space in the group storage pool that is currently in use.	GB	
	Reserved space: Indicates the total space in the group storage pool that is currently reserved for snapshot data.	GB	
	Free space: Indicates the current unused space in the pool.	GB	
	Free percentage: Indicates the percentage of space in the pool that is currently unused.	Percent	Ideally, the value of this measure should be high. A very low percentage of free space is indicative of excessive space utilization in the storage pool. If the space in the pool is not increased, then applications using the pool will experience slowdowns.

1.5.2 EQ Group Snapshots

A snapshot represents a frozen image of a volume. The source of a snapshot is called an "original." When a snapshot is created, it looks exactly like the original at that point in time. As changes are

made to the original, the snapshot remains the same and looks exactly like the original at the time the snapshot was created. Snapshots allow administrators to perform online backups and can be scheduled at regular time intervals. If data loss occurs, archived information can be rapidly retrieved to restore data and return to normal operations.

This test monitors how snapshots in the PS Series group are used.

Purpose	Monitors how snapshots in the PS Series group are used
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 storage device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total snapshots: Indicates the total number of snapshots in the group, currently.	Number	
	In use snapshots: Indicates the number of snapshots in the group that currently have iSCSI connections.	Number	
	Online snapshots: Indicates the number of snapshots in the group that are currently available for iSCSI connections.	Number	

1.5.3 EQ Group Volumes

Administrators create volumes from the available space in the PS Series group storage pool. a volume can be spread across multiple disks and multiple group members — this is done automatically by the virtualization built into the arrays. The group exports volumes as iSCSI targets protected with security, including authentication and authorization, for both discovery and access. upon connection, hosts see volumes as local disks.

This test reports the usage of volume in the PS Series group storage pool.

Purpose	Reports the usage of volume in the PS Series group storage pool
Target of the	A Dell EqualLogic SAN storage

test	
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 storage device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total snapshots: Indicates the total number of snapshots available in the group, currently.	Number	
	In use volumes: Indicates the number of volumes in the group that currently have active iSCSI connections.	Number	
	Online volumes: Indicates the number of volumes in the group that are currently available for iSCSI connections.	Number	
	Total connections: Indicates the total number of iSCSI connections that are currently established to the volumes in this group.	Number	

1.6 The Service Layer

With the help of the tests mapped to this layer, you can do the following:

- Isolate connection loads and I/O latencies experienced by the device;
- Identify the array controllers in an abnormal state;
- Detect the unhealthy state of the device;
- Monitor the space usage in the group member array and report over-utilization

Figure 1.7: The tests mapped to the Service layer

1.6.1 EQ Connections Test

This test monitors the connection and I/O load on the storage device, and reports how well the device handles the load. In the process, the test reports the latencies experienced by the device while performing read/write operations, thus shedding light on probable processing bottlenecks.

Purpose	Monitors the connection and I/O load on the storage device, and reports how well the device handles the load. In the process, the test reports the latencies experienced by the device while performing read/write operations, thus shedding light on probable processing bottlenecks.
Target of the test	A Dell EqualLogic PS Series storage device
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 storage device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Current connections: Indicates the number of iSCSI connections currently made from initiators to this storage device.	Number	An initiator is a client of an SCSI interface, via IP, that issues commands to request services from components, logical units of a server known as a target. A SCSI transport maps the client-server SCSI protocol to a specific interconnect. An initiator is one endpoint of a SCSI transport and a target is the other endpoint. The value of this measure is a good indicator of the connection load on the storage device.
	Read latency: Indicates the time taken for a read operation on the storage device during the last measurement period.	Secs	Very high values for these measures are indicative of the existence of road-blocks to rapid reading/writing by the storage device. By observing the variations in these measures over time, you can understand whether the latencies are sporadic or consistent. Consistent delays in reading/writing could indicate that there are persistent bottlenecks (if any) in the storage device to speedy I/O processing.
	Write latency: Indicates the time taken for a write operation on the storage device during the last measurement period.	Secs	
	Read avg latency: Indicates the average time taken by this storage device to perform reads, since storage device startup.	Secs	

	Write avg latency: Indicates the average time taken by this storage device to perform writes, since device startup.	Secs	
	Read operation count: Indicates the rate at which the storage device performed reads.	Ops/Sec	
	Write operation count: Indicates the rate at which the storage device performed writes.	Ops/Sec	
	Transmitted data: Indicates the rate at which data is transmitted by the storage device.	KB/Sec	
	Received data: Indicates the rate at which data is received by the storage device.	KB/Sec	

1.6.2 EQ Controllers Test

The Dell EqualLogic PS Series supports dual controllers, which are redundant and hot-swappable. The controller module features dual-core 64-bit processors with a HyperTransport™ I/O bus and twin 64-bit double data rate (DDR) channels. Each control module is equipped with 1GB of battery-backed DRAM.

To ensure that the controllers are functioning properly, the temperature of their processors and the strength of their battery backups should be periodically checked so that, abnormalities can be quickly detected and fixed. This test auto-discovers the available controllers in the PS Series array, and reports the above for each controller. In addition, this test also reveals which of the controllers is the primary controller in the redundant setup, and which is the secondary.

Purpose	This test auto-discovers the controllers supported by the PS Series array, and reports the temperature of the processors and the strength of the battery backups for each controller
Target of the	A Dell EqualLogic SAN storage

test	
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 available controller in the storage device monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>test</td>
<td>Battery status:
Indicates the current status of the battery present in this controller.</td>
<td></td>
<td>This measure reports one of the following values as the state of the battery present in a controller:
• Ok
• Failed
• Good Battery
• Low Voltage
• Low Voltage Charging
• Missing Battery
The numeric values that correspond to the above-mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Ok</td><td>1</td></tr><tr><td>Failed</td><td>2</td></tr><tr><td>Good Battery</td><td>3</td></tr><tr><td>Low Voltage</td><td>4</td></tr><tr><td>Low Voltage Charging</td><td>5</td></tr><tr><td>Missing Battery</td><td>6</td></tr></table>
Note:
By default, this measure reports the above-mentioned states while indicating the state of the battery present in a controller. However, in the graph of this measure, battery states will be represented using their corresponding numeric equivalents - i.e., 1 - 6.</td>
</tr>
<tr>
<td></td>
<td>Total uptime:
Indicates the time that elapsed since this controller was last booted.</td>
<td>Secs</td>
<td>By carefully observing the changes in the measure, you can promptly detect unexpected breaks in the availability of the controller.</td>
</tr>
</table>

<table>
<tr><td></td><td>Processor temperature:
Indicates the current temperature of the processor supported by this controller.</td><td>Celsius</td><td>Ideally, this value should be low.</td></tr>
<tr><td></td><td>Chipset temperature:
Indicates the current temperature of the chipset supported by this controller.</td><td>Celsius</td><td>A low value is desired for this measure.</td></tr>
<tr><td></td><td>Controller status:
Indicates whether the controller is the primary controller or the secondary.</td><td></td><td>This measure reports the value Primary or Secondary depending upon whether the controller is the primary controller or the secondary controller in the redundant setup.

The numeric values that correspond to the above-mentioned states are as follows:

<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Primary</td><td>1</td></tr><tr><td>Secondary</td><td>2</td></tr></table>
Note:

By default, this measure reports the above-mentioned States while indicating the status of the controller. However, the graph of this measure will be represent states using the corresponding numeric equivalents - 1 or 2 only.</td></tr>
</table>

1.6.3 EQ Health Test

This test monitors the overall health of the member array in the monitored group, and proactively alerts administrators to abnormalities.

Purpose	Monitors the overall health of the member array in the monitored group, and proactively alerts administrators to abnormalities
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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.

<table>
<tr><td></td><td colspan="3">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 equalizer 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 the storage device 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>Health status:
Indicates the current status of the member array.</td><td></td><td>This measure reports one of the following values as the state of the member array:

• Unknown
• Normal
• Warning
• Error

The numeric values that correspond to the above-mentioned states are as follows:

<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Warning</td><td>2</td></tr><tr><td>Error</td><td>3</td></tr></table>
Note:

By default, this measure reports the above-mentioned States while indicating the health of the member array. However, in the graph of this measure, array health will be represented using the corresponding numeric equivalents - i.e., 0 - 3.</td></tr>
</table>

1.6.4 EQ Member Test

A PS Series group is comprised of a single PS Series array or multiple arrays working together. Each array in a group is called a member. A member is a fully-functional, high-performance, highly-available storage array with mirrored write-back caches and multiple storage network connections.

Each member is composed of redundant components - disks, controllers with mirrored write-back caches, network interfaces, power supplies, and cooling fans.

This test monitors the space usage of the each member, and promptly alerts you if disk space in any member array is over-utilized. In addition, the test reports the number of controllers and disks in each member array, and periodically checks the array temperature to report abnormalities (if any).

Purpose	Monitors the space usage of the each member, and promptly alerts you if disk space in any member array is over-utilized. In addition, the test reports the number of controllers and disks in each member array, and periodically checks the array temperature to report abnormalities (if any).
Target of the test	A Dell EqualLogic SAN storage
Agent deploying the test	A remote 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 being configured 3. **PORT** - The port at which the device listens. By default, this will be NULL. 4. **SNMPPORT** - The port number through which the Juniper DX device exposes its SNMP MIB. The default port is 161. 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 target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 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 equalizer 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 member array monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total space: Indicates the total space in this member, currently.	GB	
	Used space: Indicates the amount of space in this member currently in use.	GB	Ideally, the value of this measure should be low. If the value is very close to that of the **Total space** measure, it indicates that the member is running out of disk space. This can severely hamper the performance of applications that use the array for storage.
	Number of controllers: Indicates the number of controllers in this member array, currently.	Number	
	Number of disks: Indicates the number of disks in this member array, currently,	Number	
	Number of connections: Indicates the number of iSCSCI initiators that are currently connected to this member array.	Number	An initiator is a client of an SCSI interface, via IP, that issues commands to request services from components, logical units of a server known as a target. A SCSI transport maps the client-server SCSI protocol to a specific interconnect. An initiator is one endpoint of a SCSI transport and a target is the other endpoint. This is a good indicator of the load on the array.

<table>
<tr><td></td><td>Average temperature:
Indicates the average temperature of this member array.</td><td>Celcius</td><td>A low value is desired for this measure.</td></tr>
<tr><td></td><td>Temperature status:
Indicates the current temperature status of this member array.</td><td></td><td>This measure reports Good or Bad as the temperature status of the member.
The numeric values that correspond to the above-mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Good</td><td>100</td></tr><tr><td>Bad</td><td>0</td></tr></table>
Note:
By default, this measure reports the above-mentioned States while indicating the temperature status of the array. However, in the graph of this measure, temperature status will be represented using the corresponding numeric equivalents - i.e., 0 and 100.</td></tr>
<tr><td></td><td>Free space:
Indicates the free disk space that is currently available in this member array.</td><td>GB</td><td>A high value is desired for this measure.</td></tr>
<tr><td></td><td>Free percentage:
Indicates the percentage of space in this member array that is currently free.</td><td>GB</td><td>A high value is desired for this measure. A very low value indicates excessive utilization of the disk space in the array. This can severely hamper the performance of applications that use the array for storage.</td></tr>
</table>

Chapter 2

Conclusion

This document has clearly explained how eG Enterprise monitors the Dell EqualLogic SAN storage device. We can thus conclude that eG Enterprise is the ideal solution for monitoring such SAN devies. For more information on eG Enterprise, please visit our web site at www.eginnovations.com or write to us at sales@eginnovations.com.