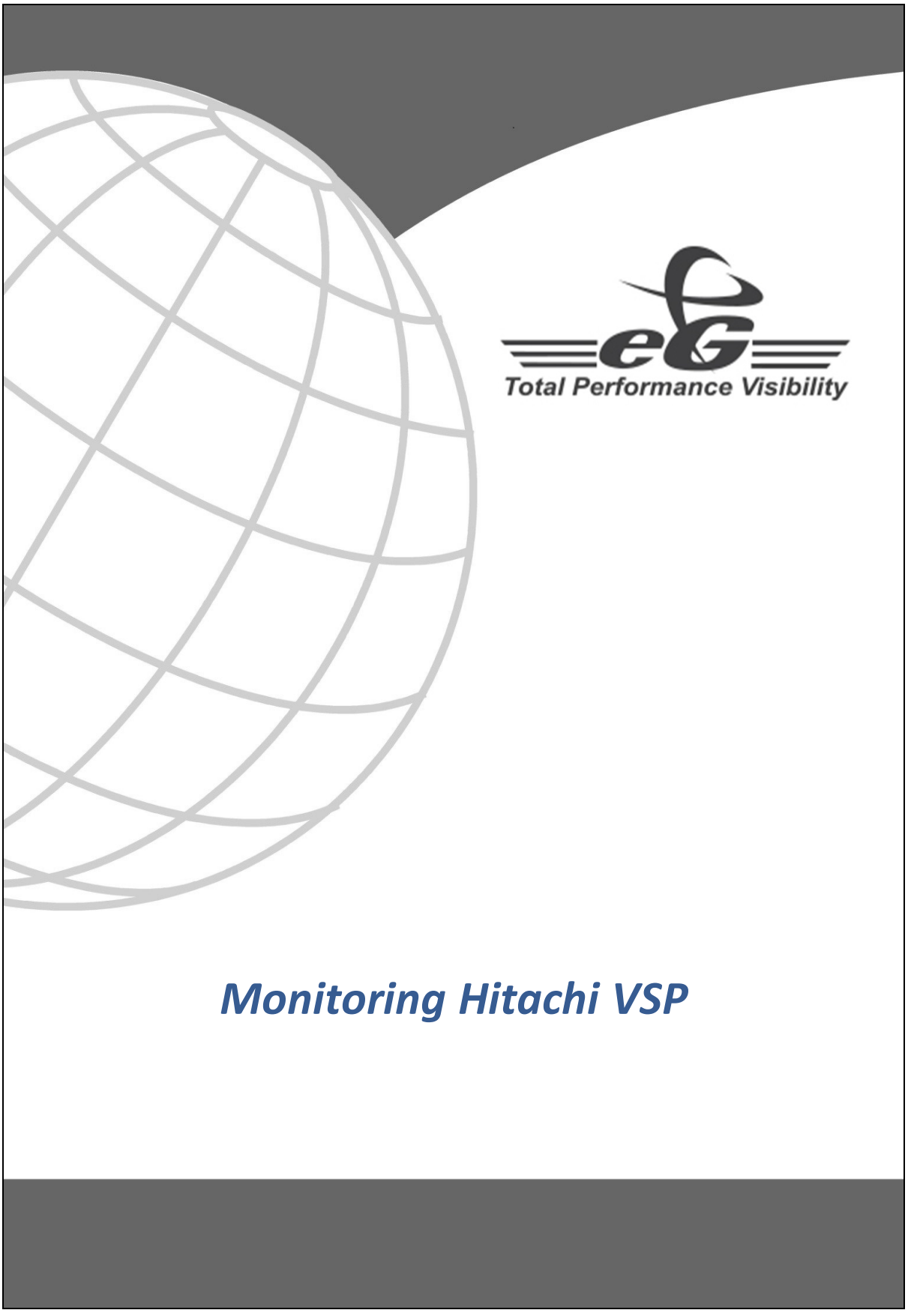

Monitoring Hitachi VSP

Table of contents

Table of Figures

1

Administering the eG Manager to monitor a Hitachi VSP Storage Device

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover the Hitachi VSP storage device. You need to manually add the server using the **COMPONENT** page (see Figure 1.1) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.

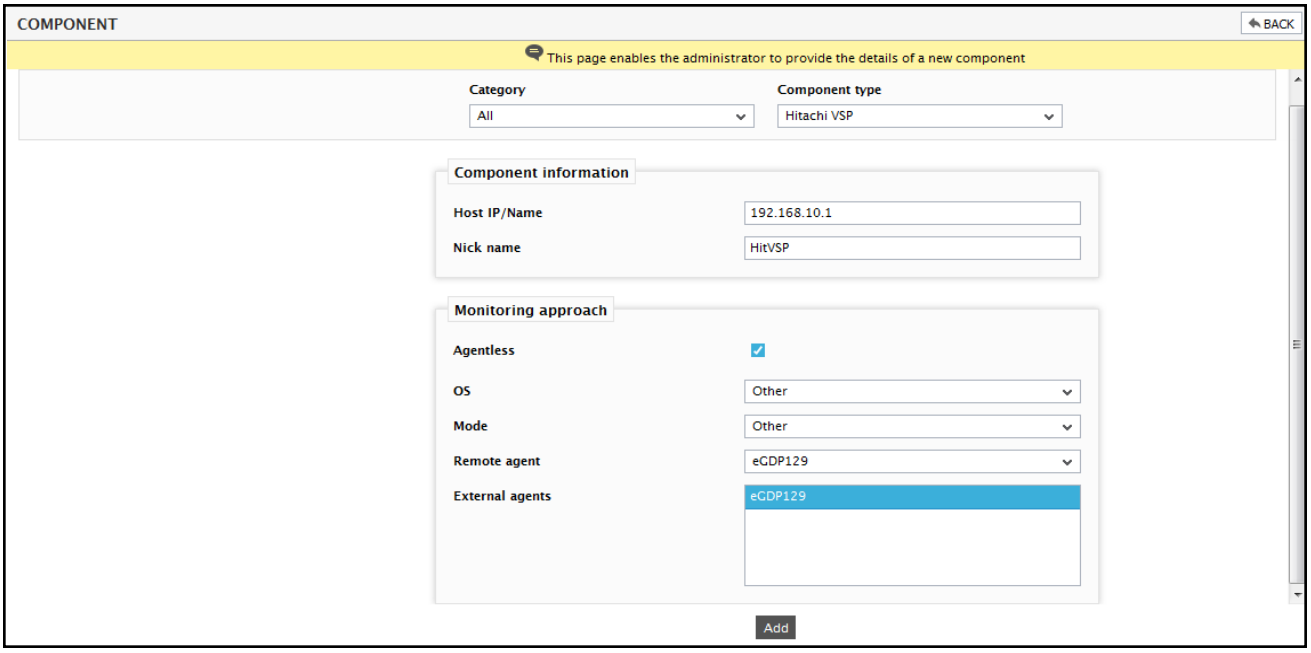

Figure 1.1: Adding the Hitachi VSP storage device

3. Specify the **Host IP** and the **Nick name** of the Hitachi VSP storage device in Figure 1.1. Then click the **Add** button to register the changes.
4. Finally, signout of the eG administrative interface.

2

Monitoring the Hitachi VSP

The Hitachi Virtual Storage Platform is a high-capacity, high performance data storage system that offers a wide range of storage and data services, software, logical partitioning, and simplified and unified data replication across heterogeneous storage systems. Its large-scale, enterprise-class virtualization layer combined with dynamic provisioning, Dynamic Tiering, and thin provisioning software, delivers virtualization of internal and external storage into one pool.

Using this system, you can deploy applications within a new framework, leverage and add value to current investments, and more closely align IT with business objectives. VSP storage systems provide the foundation for matching application requirements to different classes of storage and deliver critical services including:

- Business continuity services
- Content management services (search, indexing)
- Non-disruptive data migration
- Thin provisioning
- Dynamic Tiering
- High availability
- Security services
- I/O load balancing
- Data classification
- File management services

New technological advances improve reliability, serviceability and access to disk drives and other components when maintenance is needed. Each component contains a set of LEDs that indicate the operational status of the component.

Failure of hardware components crucial to the functioning of the VSP storage device (such as processors, batteries, fans, power supply units etc.), minimal cache usage, and excessive direct disk accesses, can significantly impact the performance of the device, thereby affecting the quality of the mission-critical services supported by the device. 24x7 monitoring of the device can greatly help in proactively identifying potential anomalies, and promptly averting them.

eG Enterprise offers a specialized Hitachi VSP monitoring model that monitors the Hitachi VSP device inside-out, and promptly alerts administrators to issues affecting their performance, so that the required remedial action can be taken before its too late.

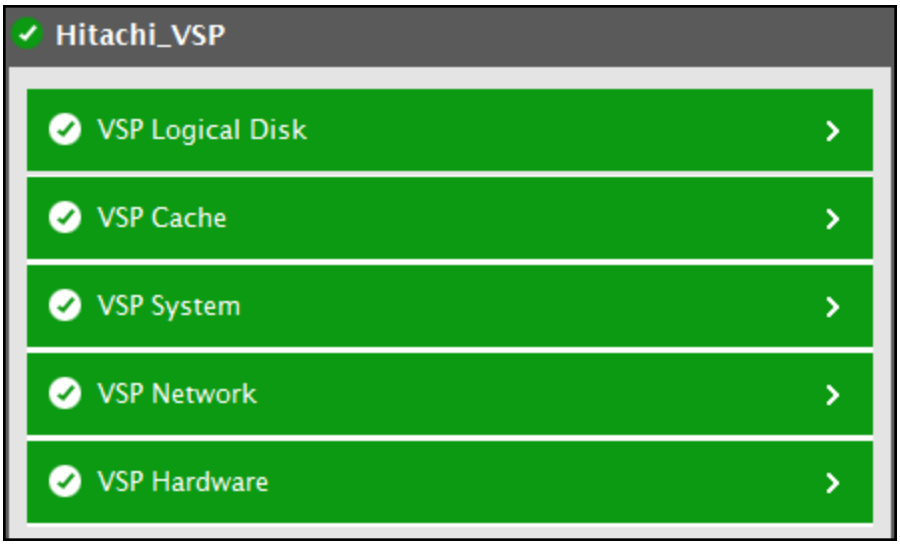

Figure 2.1: The layer model of the Hitachi VSP storage device

2.1 How does eG Enterprise monitor the Hitachi VSP device?

Each layer of Figure 2.1 above is mapped to a variety of tests which report useful performance statistics related to the storage device. These tests use both the following approaches to collecting metrics from the Hitachi VSP device:

- By accessing the Performance Monitor application available with the storage device;
- Using SNMP-based access to the SNMP MIB of the device;

The Performance Monitor is a controller-based software application that acquires information on the performance of RAID groups, logical units, and other elements of the disk subsystem while tracking the utilization rates of resources such as hard disk drives and processors. To periodically run the Performance Monitor application and to extract the metrics of interest from the storage device, a Java export utility must be available on the eG agent host.

The tests that need to access the Performance Monitor for metrics should then be configured with the path to the Java export utility. This way, whenever that test is run, the eG agent executing the test automatically invokes the Java export utility via CLI, which then connects to the storage device, accesses the Performance Monitor on the device, and extracts the desired metrics.

A few other tests executed by the eG agent collects the statistics of interest using SNMP-based access to the MIB statistics of the storage device. For these tests to work, you first need to SNMP-enable the storage device.

While you need to configure a remote agent for accessing the Performance Monitor software and collecting metrics, an external agent is necessary for performing the SNMP-based monitoring.

Note:

If need be, you can configure a single agent to function both as a *remote agent* as well as an *external agent* for monitoring the Hitachi VSP.

2.2 Pre-requisites for monitoring the Hitachi VSP

To ensure that the eG agent is able to use both the Performance Monitor and the SNMP MIB (of the device) effectively for collecting metrics from the Hitachi VSP, the following pre-requisites should be fulfilled:

- The SNMP service should be enabled on the device;
- The eG SNMP trap receiver service should be installed on the external agent host;
- The storage device should be configured to send SNMP traps to the external agent host;
- The Hitachi Performance Monitor software should be available;
- The Java export utility should be available on the remote agent host;

  Note:

  For the eG Enterprise to monitor the Hitachi VSP and collect the required metrics, the version of the Java export utility on the remote agent host and the target Hitachi VSP storage navigator should be the same.
- The eG agent should be configured with the credentials of a special user account, which is specifically created for use with the export utility; this account should fulfill the following conditions:
  - Should not possess the 'write' permission;
  - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type storage administrator;

Once the aforesaid pre-requisites are fulfilled, the eG agent will be able to collect the desired metrics from the VSP storage device; these metrics enable administrators to find quick and accurate answers to the following performance queries:

- Is the storage device available over the network?
- Are the critical hardware components of the device, such as – battery, cache, controller,
- drive, fan, processor, power supply, shared memory - are operating normally?
- Are all the RAID stores of the VSP storage device functioning without a glitch? Is any RAID store experiencing a hardware failure currently? Which RAID store is it, and which is the hardware component that is malfunctioning - is it the battery, the fan, the processor, cache, drive, shared memory, or power supply point?
- Is I/O load balanced across all the ports in SAN environment? Has any port been over-used?
- Which port is slow in responding to I/O requests?
- Are the channel, disk, and DRR processors on the storage device being utilized optimally?
- Do the caches have adequate memory space for storing data written to them, or are too many writes pending to the cache?
- How are the cache memory to cache switch access paths utilized? Is any path choking currently?
- Is the I/O load uniformly balanced across the logical volumes, LUNs, and parity groups on the storage device? Are any of these components over-utilized currently? Which one is it?

The sections that will follow discuss each layer of Figure 2.1 elaborately.

2.3 The VSP Hardware Layer

The tests mapped to the USP Hardware layer monitors the health of the hardware components (batteries, controllers, fans, power supply units etc) of the storage device, and alerts administrators to potential hardware failures.

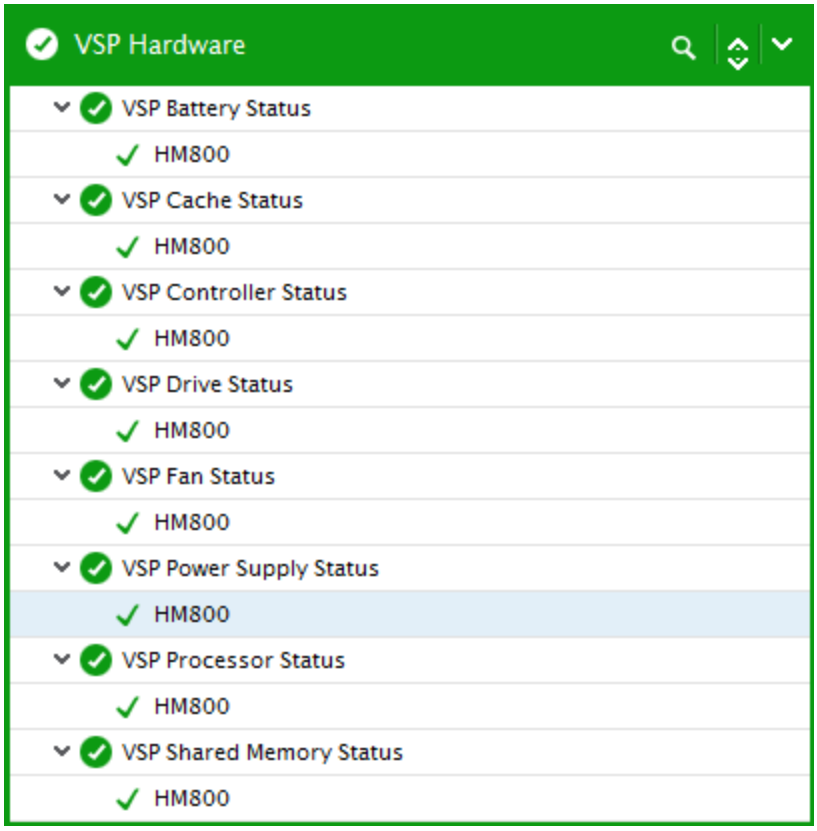

Figure 2.2: The tests mapped to the VSP Hardware Layer

2.3.1 VSP Battery Status Test

The Virtual Storage Platform is designed so that it cannot lose data or configuration information if the power fails. The battery system is designed to provide enough power to completely destage all data in the cache if two consecutive power failures occur and the batteries are fully charged. If the batteries do not contain enough charge to provide sufficient time to destage the cache when a power failure occurs, the cache operates in write through mode. When a power failure occurs and continues for 20 milliseconds or less, the storage system continues normal operation. If the power failure exceeds 20 milliseconds, the storage system uses power from the batteries to back up the cache memory data. If the charge in the batteries is not enough to withstand frequent power failures, then too much of data will be lost resulting in performance degradation of the target Hitachi VSP storage device. To avoid such loss of data, it is necessary for the administrators to monitor the status of the batteries round the clock! The **VSP Battery Status** test helps administrators in this regard!

This test reports the current status of the batteries used by each RAID store on the Hitachi VSP storage device.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1 is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.
5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.

10. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.
14. **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
15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Battery status:	Indicates the current status of the batteries of this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>noError</td><td>1</td></tr>
<tr><td>acuteError</td><td>2</td></tr>
<tr><td>seriousError</td><td>3</td></tr>
<tr><td>moderateError</td><td>4</td></tr>
<tr><td>serviceError</td><td>5</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the batteries of this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.
</td></tr>
</table>

2.3.2 VSP Cache Status Test

The Hitachi VSP(Virtual Storage Platform) places all read and write data in the cache. The amount of fast-write data in cache is dynamically managed by the cache control algorithms to provide the optimum amount of read and write cache, depending on the workload read and write I/O characteristics. The Hitachi VSP is designed so that it cannot lose data or configuration information from the cache if the power fails. The cache is protected from data loss up for up to ten minutes by the cache destage batteries while the data is copied to the cache SSD (flash memory) on the cache boards. The cache may lose data due to reasons such as frequent power failure, corruption of the cache, memory overflow of the cache etc. To avoid such loss of data from the cache, it is necessary to keep track on the status of the cache and if errors are detected, administrators should identify the criticality of such errors! The **VSP Cache Status** test helps administrators to keep a vigil on the cache!

This test reports whether the cache used by each RAID store on the storage device is currently experiencing any errors, and if so, how critical the error is.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed

2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.
5. **SNMPPORT** – The port through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
10. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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

13. **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.
14. **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
15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Cache status:	Indicates the current status of the cache used by this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** noError – 1 acuteError – 2 seriousError – 3 moderateError – 4 serviceError – 5 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current state of the cache

Measurement	Description	Measurement Unit	Interpretation
			used by this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.

2.3.3 VSP Controller Status Test

Every RAID store on the Hitachi VSP storage device contains an internal bus called the controller. This test reports the current status of the controller associated with each RAID store on the storage device.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.
5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.

9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
10. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.
14. **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
15. **ENCRYPTPASSWORD** – Specify the encryption password here.
16. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Internal controller status:	Indicates the current status of the controller of this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** noError: 1 acuteError: 2 seriousError: 3 moderateError: 4 serviceError: 5 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current state of the controller of this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.

2.3.4 VSP Drive Status Test

This test reports the current drive status of each RAID store on the storage device.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*.

This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.

5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
10. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.

14. **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
15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Drive status:	Indicates the current status of the drive used by this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** noError – 1 acuteError – 2 seriousError – 3 moderateError – 4 serviceError – 5 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current state of the drive used by this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.

2.3.5 VSP Fan Status Test

This test reports the current status of the fan used by each RAID store on the storage device.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.
5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the

specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.

10. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.
14. **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
15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Fan status:	Indicates the current status of the fan used by this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>noError</td><td>1</td></tr>
<tr><td>acuteError</td><td>2</td></tr>
<tr><td>seriousError</td><td>3</td></tr>
<tr><td>moderateError</td><td>4</td></tr>
<tr><td>serviceError</td><td>5</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the fan used by this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.
</td></tr>
</table>

2.3.6 VSP Power Supply Status Test

This test reports the current status of the power supply unit used by each RAID store on the storage device.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1 is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.

5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
10. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.
14. **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

15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Power supply status:</td><td>Indicates the current status of the power supply unit used by this RAID store.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>noError</td><td>1</td></tr><tr><td>acuteError</td><td>2</td></tr><tr><td>seriousError</td><td>3</td></tr><tr><td>moderateError</td><td>4</td></tr><tr><td>serviceError</td><td>5</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of the power supply unit used by this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.</td></tr>
</table>

2.3.7 VSP Processor Status Test

This test reports the current status of the processor that each RAID store on the storage device supports.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.
4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.
5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
10. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This

parameter once again appears only if the snmpversion selected is **v3**.

11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.
14. **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
15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Processor status:	Indicates the current status of the processor used by this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** noError / 1

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>acuteError</td><td>2</td></tr><tr><td>seriousError</td><td>3</td></tr><tr><td>moderateError</td><td>4</td></tr><tr><td>serviceError</td><td>5</td></tr></table> **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current status of the processor used by this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.

2.3.8 VSP Shared Memory Status Test

Shared memory resides by default on the first pair of cache boards in controller chassis. The usage of the shared memory increases when you install software features such as Copy-On-Write Snapshot or the Universal Replicator. The shared memory on each cache board contains 1 or 2 GB cache directory to safeguard write pending data in the cache if there is an unlikely case of double failure of the shared memory cache area. If the shared memory is running out of space or if there are too many write pendings to the shared memory, then data synchronization may take time resulting in poor accessibility of the data as well as data loss. Administrators should therefore constantly monitor the status of the shared memory. The **VSP Shared Memory Status** test helps administrators in this regard.

This test reports the current status of the shared memory of each RAID store on the storage device.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every RAID store on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The host for which the test is to be configured.
3. **PRIMARY CONTROLLER IP** - Specify the IP address of the storage controller on the target storage device in the **PRIMARY CONTROLLER IP** text box. By default, the IP address of the **HOST** will be displayed in the **PRIMARY CONTROLLER IP** text box.

4. **SECONDARY CONTROLLER IP** - By default, the **SECONDARY CONTROLLER IP** text box is set to *none*. This implies that by default, the storage device being monitored supports a single controller only. Sometimes, a storage device could be configured with two controllers i.e., say for e.g., controller 1 and controller 2, so as to provide fail-over services - in other words, if the controller 1is down, then the controller 2 will take over to provide the critical storage services. In this case, you can provide the IP address of the controller 2 in the **SECONDARY CONTROLLER IP** text box.
5. **SNMPPORT** – The port number through which the storage device exposes its SNMP MIB; the default is 161.
6. **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.
7. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION**chosen is **v3**, then this parameter will not appear.
8. **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.
9. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
10. **AUTHPASS**– Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
11. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
12. **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
13. **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.

14. **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
15. **ENCRYPTPASSWORD**– Specify the encryption password here.
16. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
17. **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.
18. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Shared memory status:	Indicates the current status of the shared memory used by this RAID store.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** noError – 1 acuteError – 2 seriousError – 3 moderateError – 4 serviceError – 5 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current status of the shared memory used by this RAID store. The graph of this measure however, represents the status of a server using the numeric equivalents only - 1 to 5.

2.4 The VSP Network Layer

Using the tests mapped to this layer, administrators can instantly detect the failure of a network connection to the storage device, monitor the I/O traffic handled by the ports on the device, and accurately identify the busy ports / ports experiencing excessive activity.

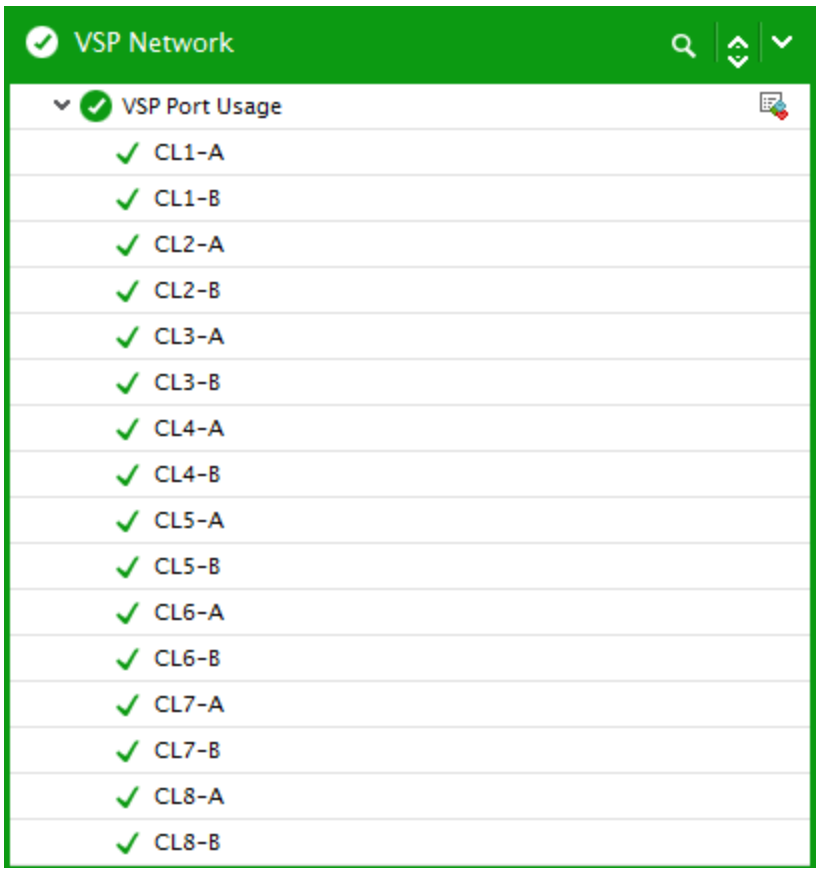

Figure 2.3: The tests mapped to the VSP Network layer

Since the *Network* test mapped to this layer has already been discussed in the *Monitoring Generic Servers* document, the section that will follow will discuss about the *VSP Port Usage* test alone.

2.4.1 VSP Port Usage Test

This test provides information on I/O rates for all the host bus adapters connected to each Storage unit Port.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every port on the target Hitachi VSP device being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed**HOST** – The host for which the test is to be

configured.

2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **TIMEOUT -** Specify the duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
I/O operations rate:	Indicates the rate at which read- write operations are performed on this port.	IOPS	A high value of this measure is generally indicative of high I/O activity on a port. Comparing the value of this measure across ports will enable you to isolate busy ports, and detect load imbalances.
Data traffic:	Indicates the rate at which data is transferred over this port.	KB/Sec	
Response time:	Indicates the responsiveness of this port to read-write requests.	Microseconds	Ideally, the value of this measure should be low. If the value of this measure is very high or is increasing steadily, then, you might want to check whether the I/O operations rate measure too reports a high value. If so, it is a clear indication that since the I/O activity is high, the hosts are taking a longer time to access the disks, thereby increasing the response time.

2.5 The VSP System Layer

This layer monitors how well the following components of a storage device have been utilized, and enables accurate identification of over-utilized components.

- The Data Recovery and Reconstruction (DRR) processors
- The Disk Processors
- The Channel Adapters

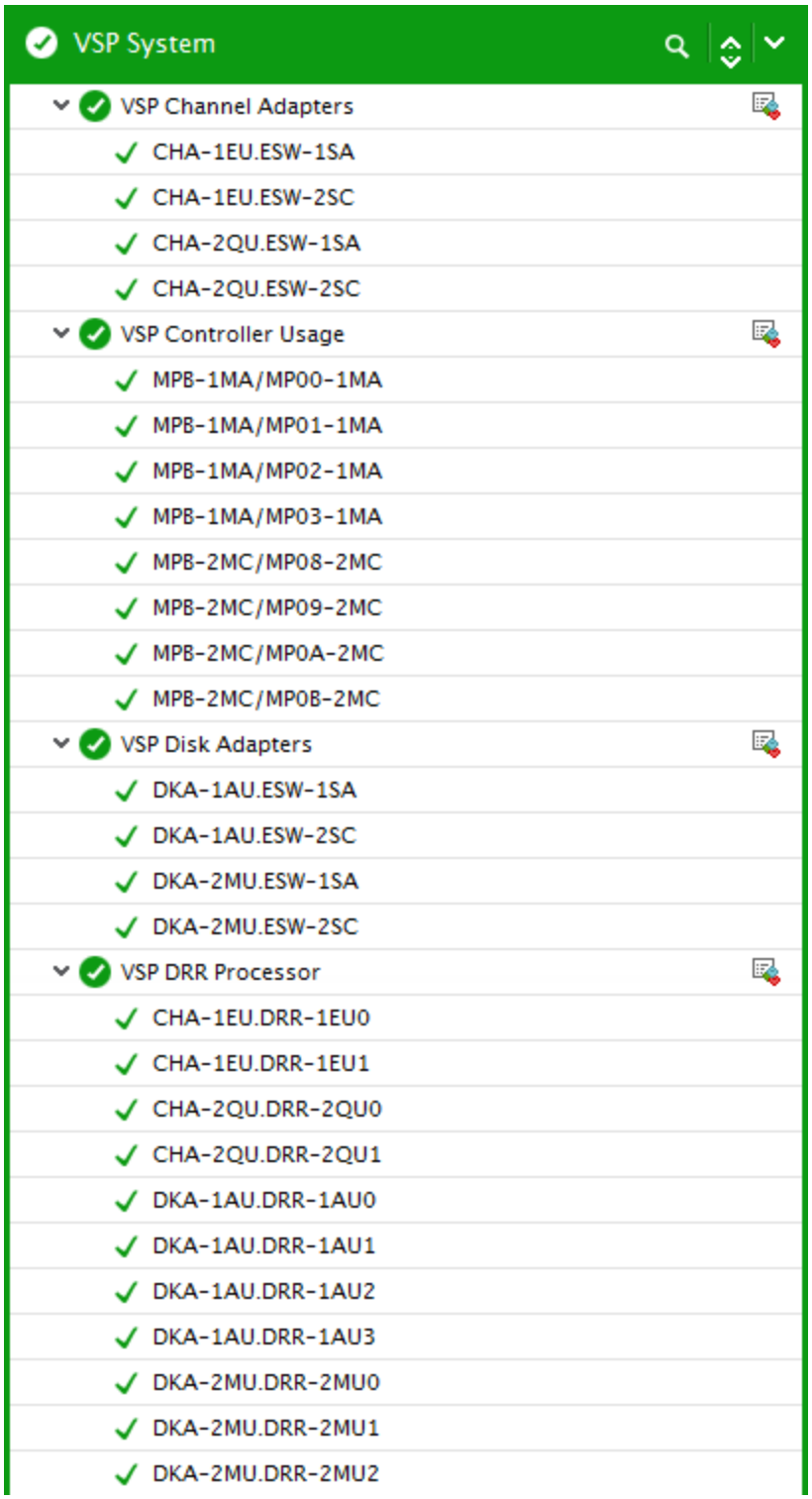

Figure 2.4: The tests mapped to the VSP System layer

2.5.1 VSP Channel Adapters Test

A Hitachi VSP may comprise of multiple Channel adapters. The Channel adapter (CHA) processes a command from a host or other storage system to a local storage system and controls data transfer to the Hitachi VSP. The host and other storage system are connected to a fibre port on the CHA via the fibre channel. Sending and receiving commands to and from another storage system via the channel adapter enables data copy and backup between storages. For the data to be copied swiftly to the storage of the Hitachi VSP, it is essential for the Channel adapters to respond to the requests in a quick manner. If the Channel adapters are busy or unable to process the requests as and when the requests are received, then the data backup between the storage systems may not synchronize leading to data loss which inturn would result in critical failures. To avoid such critical failures, it is essential for the administrators to monitor each Channel adapter of the target Hitachi VSP and figure out the responsiveness and utilization of the Channel adapters. The **VSP Channel Adapters Test** helps administrators to proactively determine the responsiveness of the channel adapters.

This test monitors the usage and responsiveness of each channel adapter, and reveals over-utilized channel adapters (if any).

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every channel adapter on the target Hitachi VSP device being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **TIMEOUT -** Specify the time duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Channel adapter usage:	Indicates the percentage of time for which this channel adapter was in use.	Percent	A high value or a value close to 100% is indicative of excessive usage of the channel processor. By comparing the value of this measure across adapters, you can accurately detect imbalances in load distribution, and rapidly identify the affected channel adapters. To ensure that load is balanced, you might want to consider the following: • Install additional CHAs, or; • Move devices defined on already overloaded ports to ports with CHPs that are less utilized, so as to balance front-end usage;
Data traffic:	Indicates the rate at which data is transferred over this channel adapter port.	KB/Sec	
Response time:	Indicates the responsiveness of this channel adapter port to read-write requests.	Microseconds	Ideally, the value of this measure should be low. If the value of this measure is very high or is increasing steadily, then, you might want to check whether the I/O operations rate measure too reports a high value. If so, it is a clear indication that since the I/O activity is high, the hosts are taking a longer time to access the disks, thereby increasing the response time.

2.5.2 VSP Controller Usage Test

This test monitors the usage of each controller available in the Hitachi VSP storage device, and reveals over-utilized controllers (if any).

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every controller on the target Hitachi VSP device being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **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 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Usage:	Indicates the percentage of time for which this controller was in use.	Percent	A high value or a value close to 100% is indicative of excessive usage of the controllers. By comparing the value of this measure across controllers, you can accurately detect imbalances in load distribution, and rapidly identify the affected controllers.

2.5.3 VSP Disk Adapters Test

A disk adapter controls the transfer of data between the drives and cache. If data is not being transferred successfully or if administrators experience slowness in data transfer, then it indicates that one of the disk adapters is not functioning or is being over-utilized leading to errors in data transmission. In order to maintain a smooth and error free data transmission, it is essential on the part of the administrators to monitor the usage of the disk adapters. The **VSP Disk Adapters** test helps administrators in this regard!

This test monitors the usage of each disk adapter, and reveals over-utilized adapters (if any).

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every disk adapter on the target Hitachi VSP device being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **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 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Disk adapter usage:	Indicates the percentage of time for which this disk adapter was in use.	Percent	A high value or a value close to 100% is indicative of excessive usage of the disk adapters. By comparing the value of this measure across adapters, you can accurately detect imbalances in load distribution, and rapidly identify the affected disk processors. To ensure that load is balanced, you might want to consider the following: • Install additional HDDs (hard disk drives) or DKAs, and then, using Volume Migration, migrate the high- write- usage volumes (especially sequential writes) to the new parity groups; or;

Measurement	Description	Measurement Unit	Interpretation
			• Use Volume Migration to migrate logical volumes from high-usage parity groups to low-usage parity groups;

2.5.4 VSP DRR Processors Test

A Data Recovery and Reconstruction Processor (DRR) is a microprocessor (located on the DKAs and channel adapters) that is used to generate parity data for RAID-5 or RAID-6 parity groups. The DRR uses the formula “old data + new data + old parity” to generate new parity.

This test monitors the usage of each DRR processor on the storage device, and reveals the over-utilized processors (if any).

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every disk processor on the target Hitachi VSP device being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the ‘write’ permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **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 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
DRR processor usage:	Indicates the percentage of time for which this DRR processor was in use.	Percent	A high value or a value close to 100% is indicative of a high write penalty condition. In such a case, you are advised to consult with your Hitachi Data Systems representative for for further information. By comparing the value of this measure across processors, you can accurately detect imbalances in load distribution, and rapidly identify the affected DRR processors. To ensure that load is balanced within the subsystem, you might want to consider relocating volumes using Volume Migration.

2.6 The VSP Cache layer

Using the tests mapped to this layer, you can determine the following:

- Bottlenecks in data writes to the cache;
- Bottlenecks in data transfer from the cache switches to cache memory;

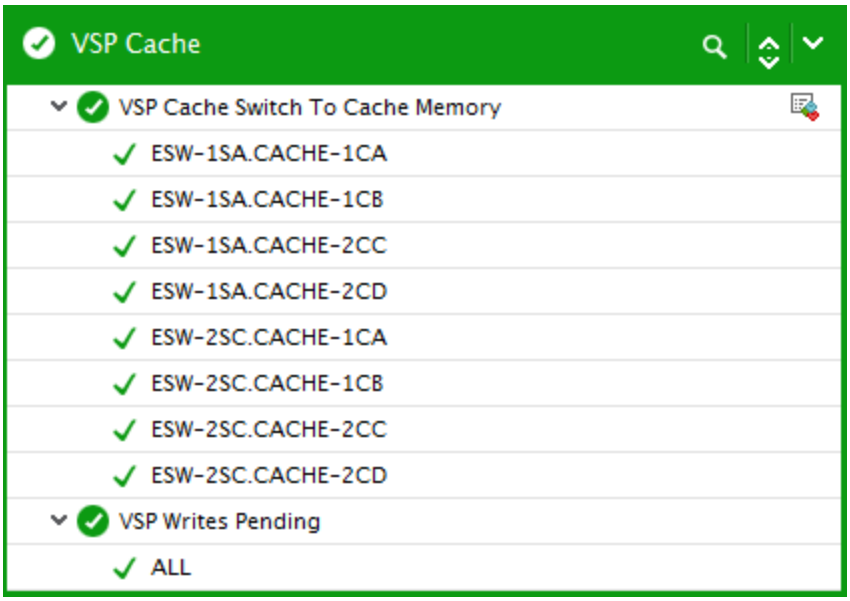

Figure 2.5: The tests mapped to the VSP Cache layer

2.6.1 VSP Cache Switch to Cache Memory Test

An access path is a path through which data and commands are transferred within a disk subsystem. Since data is written to the cache memory via a cache switch, the cache switch to cache memory route is also an access path. If there are too many writes still pending to the cache memory, you might want to know how the data transfer in this path is progressing to determine whether a slowdown in the path could have contributed to the high write-pending rate. The **VSP Cache Switch to Cache Memory** test monitors the usage of each cache switch to cache memory access path to facilitate such an analysis.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every cache switch to cache memory access path on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **TIMEOUT -** Specify the time duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Usage:	Indicates the percentage usage of this cache switch to cache memory access path.	Percent	A very high value or a value close to 100% for this measure could indicate that the access path is over-utilized, probably owing to a slow data write rate to the cache. Comparing the value of

Measurement	Description	Measurement Unit	Interpretation
			this measure across paths could indicate which path(s) is choking. Data could be transferred slowly over a path if cache does not have enough space to accommodate the data. Such an event could occur if the cache is unable to write data to the disk quickly; a slowdown in writes to disk can severely hamper the cache's ability to make space for data waiting to be written, thus crowding the access path.

2.6.2 VSP Writes Pending Test

This test reports the percentage of data that is yet to be written to the cache, and thus sheds light on a potential cache overload or a slowdown while writing data from the cache to the disk.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every cache logical partition on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed.
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **TIMEOUT -** Specify the duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
Writes pending:	Indicates the ratio of write-pending data to cache memory capacity.	Percent	A high value of this measure or a value close to 100% is a cause for concern, as it indicates that too much data is yet to be written to the cache. This essentially means that the cache does not have enough space to accommodate the pending data. Such an event could occur if the cache is unable to write data to the disk quickly; a slowdown in writes to disk can severely hamper the cache's ability to make space for data waiting to be written, thus rendering the write data pending for a long time.

2.7 The VSP Disk Layer

The tests mapped to this layer monitor the level of I/O activity on the logical volumes, parity groups, and LUNs on the storage device.

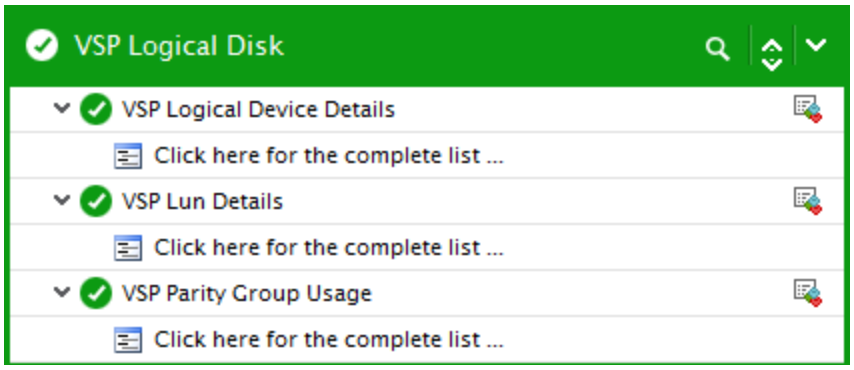

Figure 2.6: The tests mapped to the VSP Logical Disk layer

2.7.1 VSP Logical Device Details Test

This test monitors the I/O activity on each logical volume (LDEV) on the storage device, and subsequently helps administrators identify irregularities in load balancing across the volumes.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every logical volume on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **TIMEOUT -** Specify the duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
I/O operations rate:	Indicates the number of read- write operations performed on this logical volume per second.	IOPS	A high value for this measure is indicative of high I/O activity on the logical volume. Comparing the value of this measure across logical volumes can accurately reveal which volumes are extremely busy, and also enable administrators to easily detect irregularities in load distribution across the volumes. To uniformly balance load across volumes, you should consider installing additional hardware (e.g., HDDs, disk adapters, cache), or you can use volume migration to migrate high-usage volumes to higher HDD classes and/or to lower-usage parity groups.

Measurement	Description	Measurement Unit	Interpretation
Transactions rate:	Indicates the rate at which data transfers occur on this logical volume.	KB/Sec	
Read IOPS:	Indicates the rate at which data reads are performed on this logical volume.	IOPS	
Write IOPS:	Indicates the rate at which data is written to this logical volume.	IOPS	
Read hits:	Indicates the percentage of read requests that were served by this logical volume.	Percent	Ideally, the value of this measure should be high. A low value is a cause for concern, as it indicates that a majority of read requests have failed.
Write hits:	Indicates the percentage of data written to this logical volume.	Percent	
Cache- to- disk transfers:	Indicates the number of data transfer operations performed from the cache to this logical volume.	Number	A high value for this measure is a sign of good health. A low value or a consistently decreasing value could be a cause for concern, as it indicates that the cache is not writing enough data to the disk; this in turn could overload the cache and hamper its ability to make space for data that is waiting to be written.
Response time:	Indicates the current responsiveness of this logical volume to requests.	Microseconds	Ideally, the value of this measure should be low.
Transfers between disk and cache:	Indicates the rate at which data is transferred by this logical volume to the cache.	Number/Sec	

2.7.2 VSP Lun Details Test

A logical unit number (LUN) is a unique identifier used to designate individual or collections of hard disk devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of storage space shared over a storage area network (SAN). LUN errors, poor LUN cache usage, and abnormal I/O activity on the LUNs, if not promptly detected and resolved, can hence significantly degrade the performance of the storage device. This is why, it is important to continuously monitor the LUN performance. This can be achieved using the **VSP Lun Details** test.

This test monitors the I/O traffic and data transfers conducted by each LUN on the storage device, and helps administrators identify irregularities in load balancing across LUNs.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every LUN on the Hitachi VSP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed**HOST** – The host for which the test is to be configured.
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.
6. **TIMEOUT -** Specify the duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
I/O operations rate:	Indicates the number of read- write operations	IOPS	A high value for this measure is indicative of high I/O activity on the

Measurement	Description	Measurement Unit	Interpretation
	performed on this LUN per second.		LUN. Comparing the value of this measure across LUNs can accurately reveal which LUNs are extremely busy, and also enable administrators to easily detect irregularities in load distribution across the LUNs.
Transaction rate:	Indicates the rate at which data transfers occur on this LUN.	KB/Sec	
Sequential read hits:	Indicates the percentage of read requests served by this LUN in sequential access mode.	Percent	
Random read hits:	Indicates the percentage of read requests served by this LUN in random access mode.	Percent	
Sequential write hits:	Indicates the percentage of data written to this LUN in sequential access mode.	Percent	
Random write hits:	Indicates the percentage of data written to this LUN in random access mode.	Percent	
Cache- to- disk transfers:	Indicates the number of data transfer operations performed from the cache to this LUN.	Number	A high value for this measure is a sign of good health. A low value or a consistently decreasing value could be a cause for concern, as it indicates that the cache is not writing enough data to the disk; this in turn could overload the cache and hamper its ability to make space for data that is waiting to be written.

Measurement	Description	Measurement Unit	Interpretation
Response time:	Indicates the current responsiveness of this LUN to I/O requests.	Microseconds	Ideally, the value of this measure should be low.

2.7.3 VSP Parity Group Usage Test

A parity group is a group of hard disk drives (HDDs) that form the basic unit of storage for the Virtual Storage Platform. All HDDs in a parity group must have the same physical capacity. The parity group is also called as an *array group* or a *RAID group*. A RAID group contains both user data and parity information. This allows user data to be accessed in the event that one or more of the drives within the RAID group are not available. If one or more parity groups are inaccessible, then the load to the other parity groups may increase manifold! This sudden increase will affect the data transfer between the parity groups, increase the I/O traffic and result in irregular load on the parity groups which may sometimes lead to critical data loss thus affecting the overall performance of the storage device. To avoid such problems, administrators can use the **VSP Parity Group Usage** test.

This test monitors the I/O traffic and data transfers conducted by each parity group on the storage device, and indicates irregularities in load balancing across the parity groups.

Target of the test : A Hitachi VSP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every parity group on the Hitachi USP device monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed**HOST** – The host for which the test is to be configured.
2. **HOST** - The host for which the test is to be configured.
3. **PORT** - The port at which the device listens. By default, this is set to NULL.
4. **USERID** and **PASSWORD** – To extract metrics from the target storage device, the eG agent should be configured with the credentials of a special user account, which is specifically created for use with the *Java export utility*. This user account should fulfill the following conditions:
   - Should not possess the 'write' permission;
   - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type *storage administrator*;

   Specify the credentials of such a user in the **USERID** and **PASSWORD** text boxes.
5. **CONFIRM PASSWORD -** Confirm the password by retyping it here.

6. **TIMEOUT -** Specify the duration (in seconds) beyond which this test should time out in the **TIMEOUT** text box. The default is 3 seconds.

Measures made by the test:

Measurement	Description	Measurement Unit	Interpretation
I/O operations rate:	Indicates the number of read- write operations performed on this parity group per second.	IOPS	A high value for this measure is indicative of high I/O activity on the parity group. Comparing the value of this measure across parity groups can accurately reveal which parity groups are overloaded, and also enable administrators to easily detect irregularities in load distribution across the parity groups. To uniformly balance load across parity groups, you should consider installing additional HDDs, or you can use volume migration to migrate volumes from high-usage parity groups to low-usage parity groups.
Transactions rate:	Indicates the rate at which data transfers occur on this parity group.	KB/Sec	
Read IOPS:	Indicates the rate at which read operations are performed on this parity group.	IOPS	
Write IOPS:	Indicates the rate at which data is written to this parity group.	IOPS	
Read hits:	Indicates the percentage of read requests serviced by this parity group.	Percent	Ideally, the value of this measure should be high. A low value is a cause for concern, as it indicates that a majority of read requests have failed.

Measurement	Description	Measurement Unit	Interpretation
Write hits:	Indicates the percentage of data written to this parity group.	Percent	
Cache- to- disk transfers:	Indicates the number of data transfer operations performed from the cache to this parity group.	Number	A high value for this measure is a sign of good health. A low value or a consistently decreasing value could be a cause for concern, as it indicates that the cache is not writing enough data to the disk; this in turn could overload the cache and hamper its ability to make space for data that is waiting to be written.
Response time:	Indicates the current responsiveness of this parity group to I/O requests.	Microseconds	Ideally, the value of this measure should be low.
Transfers between disk and cache:	Indicates the rate at which data transfer operations are performed between this parity group and the cache.	Number/Sec	

3

Conclusion

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

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