Monitoring the Hitachi Storage Devices

eG Enterprise Version 6.0

Table of Contents

Table of Figures

Chapter

1

Introduction

Hitachi Data Systems delivers complete storage solutions to both large and small enterprises. The hardware and software products offered by Hitachi Data Systems are the foundation for its Services Oriented Storage Solutions, which provides dynamic tiered storage, common management, data protection, and archiving — enabling organizations to align their storage infrastructure with their unique business requirements.

The key storage product offerings of the Hitachi Data Systems include the Hitachi Adaptable Modular Storage (AMS) family and the Hitachi Universal Storage Platform (USP) family. Apart from providing efficient storage services, these solutions also offer effective load balancing services, thereby significantly improving application performance. Non-availability of the storage device, or issues such as abnormal I/O activity, ineffective cache usage, and excessive usage of LUNs, can not only undermine the ability of the storage device to function normally, but can ultimately affect the performance of the dependent mission-critical applications. It is therefore imperative that the availability and operations of these storage solutions are monitored 24x7.

eG Enterprise offers two specialized monitoring models for each of the storage solutions mentioned above – the *HitachiModularSan* model for monitoring the Hitachi AMS, and the *Hitachi USP SAN* model for monitoring the Hitachi USP SAN. The chapters that follow discuss each of these models in great detail.

Chapter

2

Monitoring the Hitachi AMS

The Hitachi Adapter Modular Storage is the only midrange storage product with symmetric active-active controllers that provide integrated, automated hardware-based front-to-back-end I/O load balancing. It is ideal for the most demanding application requirements with ever changing workload requirements and delivers enterprise-class performance, capacity and functionality.

Any deficiencies in the performance of the Hitachi AMS can therefore affect the quality of the user experience with the dependent aplications. Continuous monitoring of the Hitachi AMS is therefore essential.

The *HitachiModularSan* monitoring model provided by eG Enterprise monitors the I/O activity and disk usage on the storage device at frequent intervals, and proactively alerts administrators to abnormalities (if any), so that performance issues are rapidly identified and resolved, and the business-critical application the device supports function without a glitch.
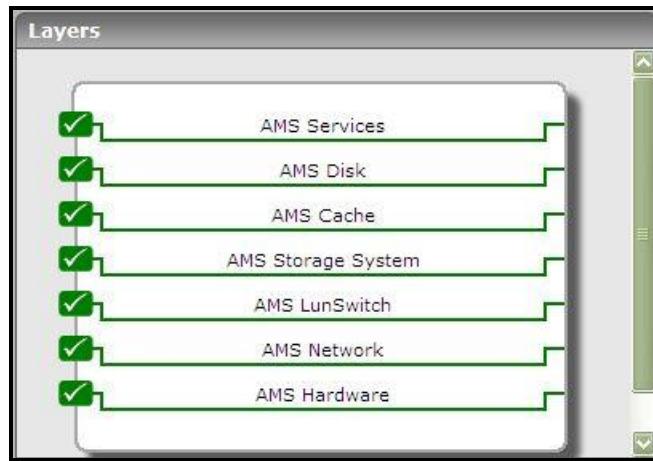
Figure 2.1: The layer model of an Hitachi AMS device

2.1 How does eG Enterprise Monitor Hitachi AMS?

Every layer of Figure 2.1 is mapped to a variety of tests which collect critical statistics pertaining to the performance of a Hitachi AMS storage unit.

For collecting these performance statistics, the eG agent uses both the following information sources:

➢ The *Performance Monitor* software that is installed with the storage device;

➢ 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 client utility named the *Storage Navigator Modular (AMS)* must be available on the eG agent host.

The tests that need to access the *Performance Monitor* should then be configured with the path to the *Storage Navigator*. This way, whenever that test is run, the eG agent executing the test automatically invokes the storage navigator client 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 collect 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** and as an **external agent** for monitoring the Hitachi AMS.

2.2 Pre-requisites for Monitoring the Hitachi AMS

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 AMS, 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;

➢ SNMP traps should be enabled on the device and configured to send traps to the external agent host;

➢ The Hitachi *Performance Monitor* software should be available;

➢ The *Storage Navigator Modular (AMS) Version 7.0 or later* should be available on the remote agent host;

➢ The *Storage Navigator Modular (AMS) Version 7.0 or later* should be able to connect to the storage unit being monitored, without requiring any user permissions.

> ➤ The eG agent can monitor only those storage units that are registered with the *Storage Navigator Modular (AMS) Version 7.0 or later*; if a target unit is neither discovered nor registered with the SNClient, do the following:

> - Login to the host on which the Storage Navigator Modular operates.

> - Go to the command prompt and switch to the directory: *C:\Program Files\Storage Navigator Modular CLI*

> - From this directory, run the following command to discover unregistered storage units:

>   **auunitaddauto -ip 192.168.40.1 192.168.40.255**

> - All discovered storage units will then be listed as follows:

```
Searching... 192.168.40.255   Detected Count : 1
The subsystem of the following was discovered.
No.  Name              Controller0     Controller1     Type      Construction   Serial No
1    DF700M_75010626   192.168.40.41   192.168.40.42   DF700M    Dual           75010626
```

> - The command will now prompt you confirm whether you want to register the discovered subsystem with the Storage Navigator Modular. Type **y** here to register one/more of the discovered storage units.

```
Are you sure you want to register the discovered subsystem? (y/n [y]) : y
```

> - Next, specify the **No.** of the discovered subsystem to register it.

```
Please specify the number of the subsystem to register: 1
```

> - If registration is successful, the following message will appear:

```
DF700M_75010626 has been registered.
The subsystems have been registered successfully
```

> ➤ Micro program 0710/A or later is required;

The metrics so collected and reported by the eG agent enable administrators to find quick and accurate answers to the following performance queries:

> ➤ Are any drives operating very slowly? Which ones are these?

> ➤ Is I/O load to the drives uniformly balanced? Has any drive been over-utilized?

> ➤ Are any port types disabled on the device? Which ones are these?

> ➤ Is any port over-loaded?

> ➤ Are any processors over-utilized? Which ones are these?

> ➤ Are the caches healthy? Is data been written to the caches at a steady rate, or are too many writes still pending? Which queue is over-loaded with pending requests to cache -is it the clean queue, middle queue, or the physical queue?

> ➤ Is there too much I/O activity on any LUN on the device? Is enough data been written to the LUNS, or does any LUN have a very low write hit ratio?

> ➤ How is I/O load distributed across all the RAID groups on the device? Is any group overloaded?

> ➢ Is heavy data traffic flowing through any backend loop? Which one is it?

> ➢ What is the current status of the critical hardware components of the storage device, such as, the battery, the enclosure controller, the disk, the fan, the tray, the power supply point, and the cache memory?

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

2.3 The AMS Hardware Layer

The tests mapped to the **AMS Hardware** layer monitor the speed and usage of the drives on the storage subsystem, and also capture the trap messages sent out by the hardware components on the storage device.
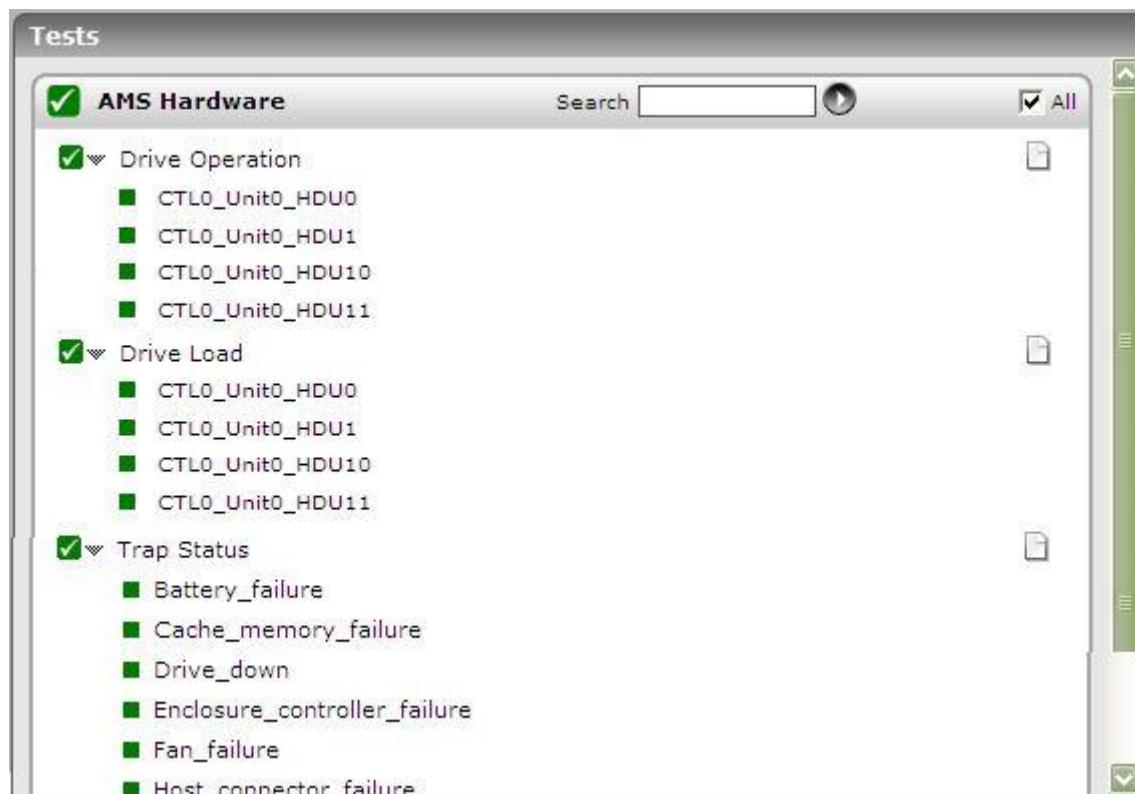
Figure 2.2: The tests mapped to the AMS Hardware layer

2.3.1 Drive Operation Test

For each drive on the storage device, this test reports the speed of the drive and the rate of tag creation on the dive.

Purpose	Reports the speed of the drive and the rate of tag creation on the drdive
Target of the test	A Hitachi AMS storage device

Agent deploying the test	A remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed
	
	2. **Host** – The IP address of the storage device
	
	3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client:
	
	    startnsmen
	
	    auunitref
	
	    The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name.
	
	4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*.
	
	5. **snclientlocation** – Specify the full path to the install directory of the storage navigator.
	
	6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.

Outputs of the test	One set of results for each drive on the Hitachi AMS device being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Operating rate: Indicates the speed, in percentage, with which this drive processes read/write requests.	Percent	A high value for this measure indicates that a large number of read/write operations have been performed on this drive. Comparing the value of this measure across drives will enable you to detect issues in load balancing across drives, accurately identify overloaded drives, and initiate relevant remedial measures.
	Tag count: Indicates the maximum number of tags made on this drive per second.	Number	

2.3.2 Drive Load Test

To periodically verify whether the I/O load is balanced across all drives on a storage device, and to promptly detect problems with load balancing, use the HitachiDrive test.

Purpose	Periodically verifies whether the I/O load is balanced across all drives on a storage device, and promptly detects problems (if any) with load balancing

Target of the test	A Hitachi AMS storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client: **startnsmen** **auunitref** The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name. 4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*. 5. **snclientlocation** – Specify the full path to the install directory of the storage navigator. 6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for each drive on the storage device monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	IO rate: Indicates the number of I/O operations performed on this drive per second.	IOPS	If this measure reports a high value or if the value of the measure increases consistently, it is indicative of unusually high I/O activity on this drive. Comparing the value of this measure across drives can accurately indicate which drive is currently experiencing heavy workloads. Observing the variations in this measure over a period of time will enable you to figure out bottlenecks in load balancing.
	Read rate: Indicates the number of read operations performed on this drive per second.	IOPS	

	Write rate: Indicates the number of write commands issued on this drive per second.	IOPS	
	Data transfer rate: Indicates the transfer size of read/write commands per second.	KB/sec	
	Read transfer rate: Indicates the transfer size of read commands per second.	KB/sec	
	Write transfer rate: Indicates the transfer size of write commands per second.	KB/sec	
	Online verify command count: Indicates the number of online verify commands executed on this drive per second.	Number/Sec	

2.3.3 Trap Status Test

This test captures the SNMP trap messages sent out by the hardware components (such as battery, cache memory, drive, enclosure controller, fan, host controller, other enclosures, and power supply units) on the storage device, and thus enables administrators to promptly detect potential hardware failures.

Purpose	Captures the SNMP trap messages sent out by the hardware components (such as battery, cache memory, drive, enclosure controller, fan, host controller, other enclosures, and power supply units) on the storage device, and thus enables administrators to promptly detect potential hardware failures
Target of the test	A Hitachi AMS storage device

Agent deploying the test	An external agent
Configurable parameters for the test	1. **Test period** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **sourceaddress** - Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. 4. **oidvalue** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder: {{TABLE1}} In this case the **oidvalue** parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface. An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**. Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be *HOST* and not *Host_system*, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **oidvalue** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be: *Trap5: .1.3.6.1.4.1.9156.1.1.5-any*. 5. **showoid** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.

Where TABLE1 is:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

6. **trapoids** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified **sourceaddress**es. To make sure that the agent considers only specific traps received from the **sourceaddress**, then provide a comma-separated list of OIDs in the **trapoids** text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.

7. **DD Frequency** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against **dd frequency**.

8. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   o The eG manager license should allow the detailed diagnosis capability

   o Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Outputs of the test	One set of results for each of the traps configured for the storage device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Number of messages: Indicates the number of failure messages for each of the traps that are configured for the storage device being monitored.	Number	The detailed diagnosis of this measure, if enabled, will reveal the details reported by the SNMP agent via traps – the details include the time at which the SNMP trap was received, the IP address of the trap sender, the trap type, and the contents of the trap. If the **showoid** parameter is set to **true**, then the contents of the trap (i.e., the **Trap Details** column) will display the OID and its value. If the flag is set to **false** instead, only the values will be displayed in the **Trap details** column and not the OIDs.

2.4   The AMS Network Layer

Using the tests mapped to the **AMS Network** layer, you can determine the current control status of the port types on the storage device, and also identify ports experiencing unusually high I/O loads.
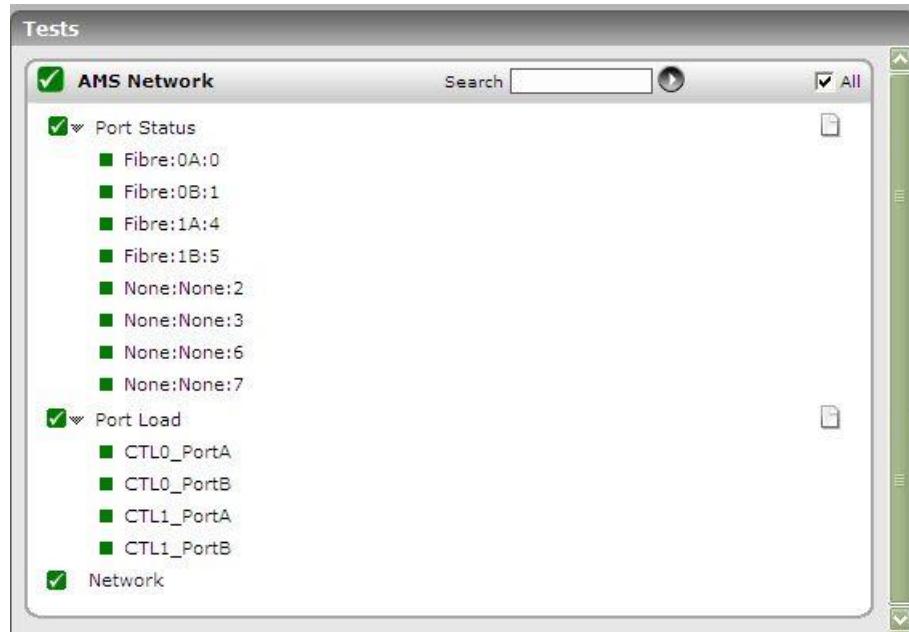
Figure 2.3: The tests mapped to the AMS Network layer

2.4.1 Port Status Test

This test auto-discovers the port types on a storage device, and reports the current control status of each type.

Purpose	Auto-discovers the port types on a storage device, and reports the current control status of each type
Target of the test	A Hitachi AMS storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for each port type on the storage device being monitored

Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Control status: Indicates the control status of this port type.	Number	If this measure reports the value 1, it indicates that this port type is enabled. The value 0 on the other hand indicates that this port type is disabled.

2.4.2 Port Load Test

Assess the load on every enabled port on the storage device using the HitachiPort test.

Purpose	Assesses the load on every enabled port on the storage device
Target of the test	A Hitachi AMS device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client: **startnsmen** **auunitref** The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name. 4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*. 5. **snclientlocation** – Specify the full path to the install directory of the storage navigator. 6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for every port on the storage device monitored
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**IO rate:** Indicates the number of I/O operations performed on this port per second.	IOPS	If this measure reports a high value or if the value of the measure increases consistently, it is indicative of unusually high I/O activity on this port. Comparing the value of this measure across ports can accurately indicate which port is currently experiencing heavy workloads. Observing the variations in this measure over a period of time will enable you to figure out bottlenecks in load balancing.
	Read rate: Indicates the number of read operations performed on this port per second.	IOPS	
	Write rate: Indicates the number of write commands issued on this port per second.	IOPS	
	Read hit: Indicates the percentage of read requests that were served from the cache.	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 the read requests have been serviced by direct disk accesses, which in turn would increase the processing overheads.
	Write hit: Indicates the percentage of write requests that were served from the cache.	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 the write requests have been serviced by direct disk accesses, which in turn would increase the processing overheads.
	Data transfer rate: Indicates the transfer size of read/write commands per second.	KB/sec	

	Read transfer rate: Indicates the transfer size of read commands per second.	KB/sec	
	Write transfer rate: Indicates the transfer size of write commands per second.	KB/sec	

2.5   The AMS LunSwitch Layer

The test mapped to this layer reports the security mode and control status of each LUN switch on the storage device being monitored.

Figure 2.4: The tests mapped to the AMS LunSwitch layer

2.5.1 Lun Switch Details Test

LUN is a **Logical Unit Number**. It can be used to refer to an entire physical disk, or a subset of a larger physical disk or disk volume. The physical disk or disk volume could be an entire single disk drive, a partition (subset) of a single disk drive, or disk volume from a RAID controller comprising multiple disk drives aggregated together for larger capacity and redundancy.

This test auto-discovers the LUN security switches on the storage device, and for every switch, reports the current security mode and control status.

Purpose	Auto-discovers the LUN security switches on the storage device, and for every switch, reports the current security mode and control status
Target of the test	A Hitachi AMS storage device

Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every LUN switch on the storage device		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Switch security mode: Indicates the current security mode of the LUN switch.	Number	If the value of this measure is 1, it indicates that the security mode of the LUN switch is *On*. If the value of this measure is 0, it indicates that the security mode of the LUN switch is *Off*.
	Switch control status: Indicates the current control status of the LUN switch.	Number	If the value of this measure is 1, it indicates that the control status of the LUN switch is *On*. If the value of this measure is 0, it indicates that the control status of the LUN switch is *Off*.

2.6   The AMS Storage System Layer

Continuously observe processor usage and proactively detect any contention for CPU resources with the help of the test mapped to the **AMS Storage System** layer.
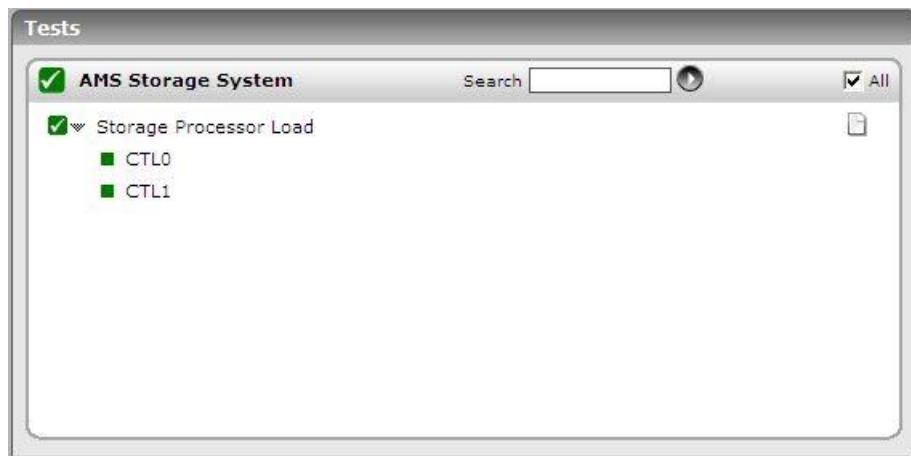
Figure 2.5: The test mapped to the AMS Storage System layer

2.6.1 Storage Processor Load Test

This test auto-discovers the processors supported by the storage device, and reports the extent to which each processor was utilized.

Purpose	Auto-discovers the processors supported by the storage device and reports the extent to which each processor was utilized
Target of the test	A Hitachi AMS storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client: **startnsmen** **auunitref** The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name. 4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*. 5. **snclientlocation** – Specify the full path to the install directory of the storage navigator. 6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for each processor supported by the storage device monitored
Measurements made by the test	<table><tr><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr><tr><td>**Usage:** Indicates the percentage of CPU resources of this processor currently utilized.</td><td>Percent</td><td>A high value for this measure or a value close to 100% could either indicate excessive usage of the processor or that one/more processes are contending for limited CPU resources.</td></tr></table>

2.7   The AMS Cache Layer

Optimal usage of the cache minimizes direct disk accesses, thus reducing unnecessary processing overheads and improving the overall performance of the storage device. To determine whether the cache is effectively utilized or not, take the help of the tests mapped to the **AMS Cache** layer.
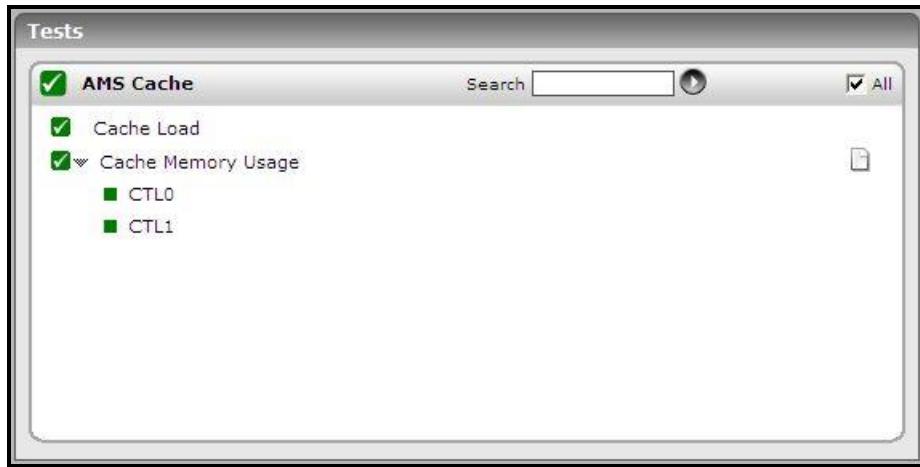
Figure 2.6: The tests mapped to the AMS Cache layer

2.7.1 Cache Load Test

This test reports the rate at which data is written to the cache memory.

Purpose	Reports the rate at which data is written to the cache memory
Target of the test	A Hitachi AMS storage device
Agent deploying the test	An external agent

| Configurable parameters for the test	1. **Testperiod** – How often should the test be executed
	2. **Host** – The IP address of the UPS
	3. **snmpport** – The port at which the UPS exposes its SNMP MIB. The default is 161.
	4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
	5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear.
	6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter.
	7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**.
	8. **confirm password** – Confirm the **authpass** by retyping it here.

	9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
	
	  ➢ **MD5** – Message Digest Algorithm
	
	  ➢ **SHA** – Secure Hash Algorithm

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

	11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types:
	
	  ➢ **DES** – Data Encryption Standard
	
	  ➢ **AES** – Advanced Encryption Standard

	12. **encryptpassword** – Specify the encryption password here.
	13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for each cache supported by the storage device monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	WriteDataRate: Indicates the rate at which data is written to the cache memory of the storage device.	Bytes/sec	

2.7.2 Cache Memory Usage Test

This test reports how well the objects in the cache have been utilized.

Purpose	Reports how well the objects in the cache have been utilized
Target of the test	A Hitachi AMS storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client: **startnsmen** **auunitref** The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name. 4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*. 5. **snclientlocation** – Specify the full path to the install directory of the storage navigator. 6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for every cache on the storage device

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Write pending rate: Indicates the percentage of writes to this cache that are currently pending.	Percent	A high value could be a cause for concern, as it could indicate a bottleneck while writing to the cache.
	Clean queue usage rate: Indicates the percentage of the this cache's clean queue currently utilized.	Percent	Since all pending read/write requests to a cache typically reside in a queue, excessive queue usage (i.e., a high value for this measure) is often an indication that too many requests are yet to be processed by the cache and hence, are still in queue. This could be a result of a processing bottleneck on the cache or a cache overload. You might have to investigate further to diagnose the root-cause of this anomaly.
	Middle queue usage rate: Indicates the percentage of this cache's middle queue currently utilized.	Percent	
	Physical queue usage rate: Indicates the percentage of the cache's physical queue currently utilized.	Percent	On the other hand, if the values of these measures are low, it is a sign of good cache health.
	Total queue usage rate: Indicates the percentage of the cache queue currently utilized.	Percent	

2.8   The AMS Disk Layer

The tests associated with the **AMS Disk** layer monitors the I/O load on the LUNs and RAID groups on the storage device being monitored.

Figure 2.7: The tests mapped to the SanDisk layer

2.8.1 Lun Load Test

This test monitors the I/O activity on each LUN on the storage device, and reveals the LUN that is experiencing the maximum throughput.

Purpose	Monitors I/O activity on each LUN on the storage device, and reveals the LUN that is experiencing the maximum throughput
Target of the test	A Hitachi AMS storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed
	2. **Host** – The IP address of the storage device
	3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client:
	startnsmen
	auunitref
	The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name.
	4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*.
	5. **snclientlocation** – Specify the full path to the install directory of the storage navigator.
	6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for each LUN on the storage device monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	IO rate: Indicates the number of read/write commands executed on this LUN per second.	IOPS	If this measure reports a high value or if the value of the measure increases consistently, it is indicative of unusually high I/O activity on this LUN. Comparing the value of this measure across LUNs can accurately indicate which LUN is currently experiencing heavy workloads. Observing the variations in this measure over a period of time will enable you to figure out bottlenecks in load balancing.
	Read rate: Indicates the number of read operations performed on this LUN per second.	IOPS	
	Write rate: Indicates the number of write commands issued on this LUN per second.	IOPS	

	Read hit: Indicates the percentage of read requests that were served from this LUN.	Percent	Ideally, the value of this measure should be high. A low value is a cause for concern, as it could indicate that a majority of the read requests have failed. .
	Write hit: Indicates the percentage of data written to this LUN.	Percent	Ideally, the value of this measure should be high. A low value is a cause for concern, as it indicates that data is not getting written to the LUN; this could be owing to an I/O bottleneck, which might have to be investigated.
	Data transfer rate: Indicates the transfer size of read/write commands per second.	KB/sec	
	Read transfer rate: Indicates the transfer size of read commands per second.	KB/sec	
	Write transfer rate: Indicates the transfer size of write commands per second.	KB/sec	
	Tag count: Indicates this LUN's current tag count.	Number	

2.8.2 Raid Group Load Test

"RAID" – the Redundant Array of Independent Disks - is now used as an umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives. RAID's various designs all involve two key design goals: increased data reliability or increased input/output performance. When multiple physical disks are set up to use RAID technology, they are said to be *in* a *RAID* array/group. This array distributes data across multiple disks, but the array is seen by the computer user and operating system as one single disk.

For every RAID group auto-discovered on a Hitachi AMS storage device, this test monitors the I/O load on the group.

Purpose	Monitors the I/O load on each RAID group

Target of the test	A Hitachi AMS storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **Testperiod** – How often should the test be executed 2. **Host** – The IP address of the storage device 3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client: **startnsmen** **auunitref** The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name. 4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*. 5. **snclientlocation** – Specify the full path to the install directory of the storage navigator. 6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for each RAID group on the storage device monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	IO rate: Indicates the number of read/write commands executed on this RAID group per second.	IOPS	If this measure reports a high value or if the value of the measure increases consistently, it is indicative of unusually high I/O activity on this RAID group. Comparing the value of this measure across groups can accurately indicate which RAID group is currently experiencing heavy workloads. Observing the variations in this measure over a period of time will enable you to figure out bottlenecks in load balancing.
	Read rate: Indicates the number of read operations performed on this RAID group per second.	IOPS	

	Write rate: Indicates the number of write commands issued on this RAID group per second.	IOPS	
	Read hit: Indicates the percentage of read requests that were served from this RAID 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.
	Write hit: Indicates the percentage of data written to this RAID group.	Percent	Ideally, the value of this measure should be high. A low value is a cause for concern, as it indicates that not all data is getting written to this RAID group; this could be owing to an I/O bottleneck, which might require further investigation.
	Data transfer rate: Indicates the transfer size of read/write commands per second.	KB/sec	
	Read transfer rate: Indicates the transfer size of read commands per second.	KB/sec	
	Write transfer rate: Indicates the transfer size of write commands per second.	KB/sec	

2.9   The AMS Services Layer

Whenever the storage device experiences heavy workloads, the additional load on the device is transferred to the disk via multiple backend loops. Using the test mapped to the **AMS Services** layer, the load on each of these backend loops can be monitored.
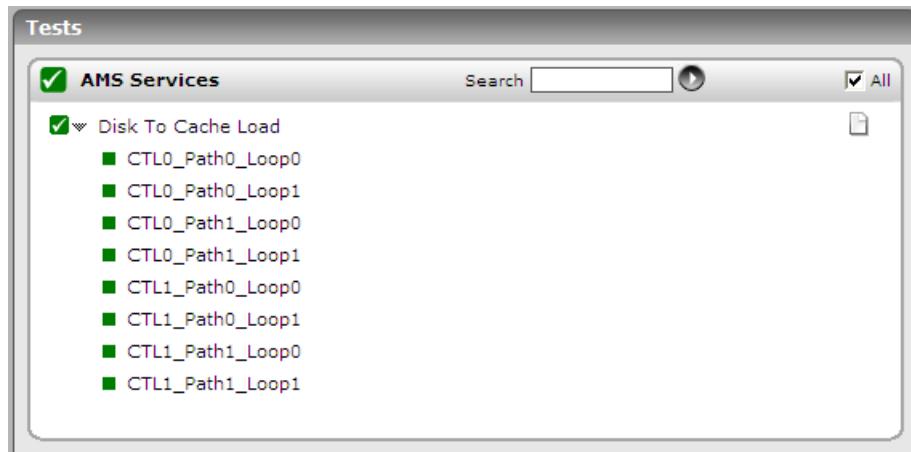
Figure 2.8: The test mapped to the AMS Services Layer

2.9.1 Disk To Cache Load Test

Whenever the storage device experiences heavy workloads, the additional load on the device is transferred to the disk via multiple backend loops. Periodic monitoring of the I/O activity on the loops is essential to identify loops that are heavily loaded, and loops where data is moving slowly or is choking. This test auto-discovers the backend loops that are operational on a storage device, and reports load statistics pertaining to each loop.

Purpose	Auto-discovers the backend loops that are operational on a storage device, and reports load statistics pertaining to each loop
Target of the test	A Hitachi AMS storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **Testperiod** – How often should the test be executed
	2. **Host** – The IP address of the storage device
	3. **unitname** – Specify the name of the storage unit to be monitored. To determine the unit name registered with the Storage Navigator Client for the AMS SAN device, run the following commands, one after another, from the *C:\Program Files\Storage Navigator Modular CLI* directory on the Storage Navigator Client:
	startnsmen
	auunitref
	The output of the command includes the **Name** of the storage unit. *DF700M_75011118* is a sample unit name.
	4. **MCtype** – Indicate the machine type. The value can be *AMS* or *WMS*. By default, this parameter is set to *AMS*.
	5. **snclientlocation** – Specify the full path to the install directory of the storage navigator.
	6. **timeout** – Indicate the duration (in minutes) for which this test should wait for a response from the storage device. By default, this is set to 5 minutes.
Outputs of the test	One set of results for each backend loop

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	IO rate: Indicates the number of read/write commands transferred to the disk per second via this loop.	IOPS	If this measure reports a high value or if the value of the measure increases consistently, it is indicative of unusually high I/O activity on this backend loop. Comparing the value of this measure across loops can accurately indicate which path is currently experiencing heavy traffic. Observing the variations in this measure over a period of time will enable you to identify roadblocks (if any).
	Read rate: Indicates the number of read operations performed on the disk via this backend loop per second.	IOPS	
	Write rate: Indicates the number of write commands issued on the disk per second via this loop.	IOPS	

	Data transfer rate: Indicates the transfer size of read/write commands per second.	KB/sec	
	Read transfer rate: Indicates the transfer size of read commands per second.	KB/sec	
	Write transfer rate: Indicates the transfer size of write commands per second.	KB/sec	
	Online verify command count: Indicates the number of online verify commands executed per second.	Number/Sec	

Chapter

3

Monitoring the Hitachi USP

The Hitachi Universal Storage Platform (USP) is an Enterprise class enclosure that provides both its own internal disk storage capabilities (up to 330TB of raw capacity) as well as the ability to pool and manage external storage platforms. External storage platforms can be connected to--and managed by--the USP software; both the external capacity and the internal capacity of the USP itself can be combined into a single storage pool that can itself be virtualized and presented to network hosts.

Failure of hardware components crucial to the functioning of the USP 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 USP SAN* model that monitors the Hitachi USP 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.
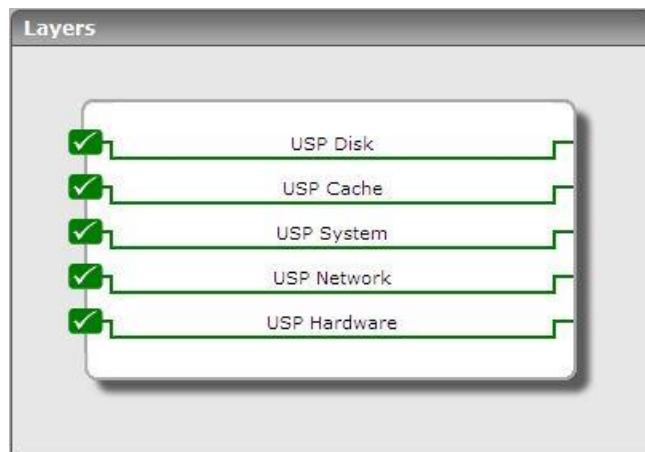

Figure 3.1: The layer model of the Hitachi USP storage device

3.1   How does eG Enterprise Monitor the Hitachi USP Device?

Each layer of Figure 3.1 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 USP 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** and as an **external agent** for monitoring the Hitachi USP.

3.2   Pre-requisites for Monitoring the Hitachi USP

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 USP, 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;

➢ 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:

  o 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 USP 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 USP 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 are too manywrites 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 3.1 elaborately.

3.3 The USP Hardware Layer

This tests mapped to the **USP Hardware** layer monitors the health of the hardware components of the storage device, and alerts administrators to potential hardware failures.
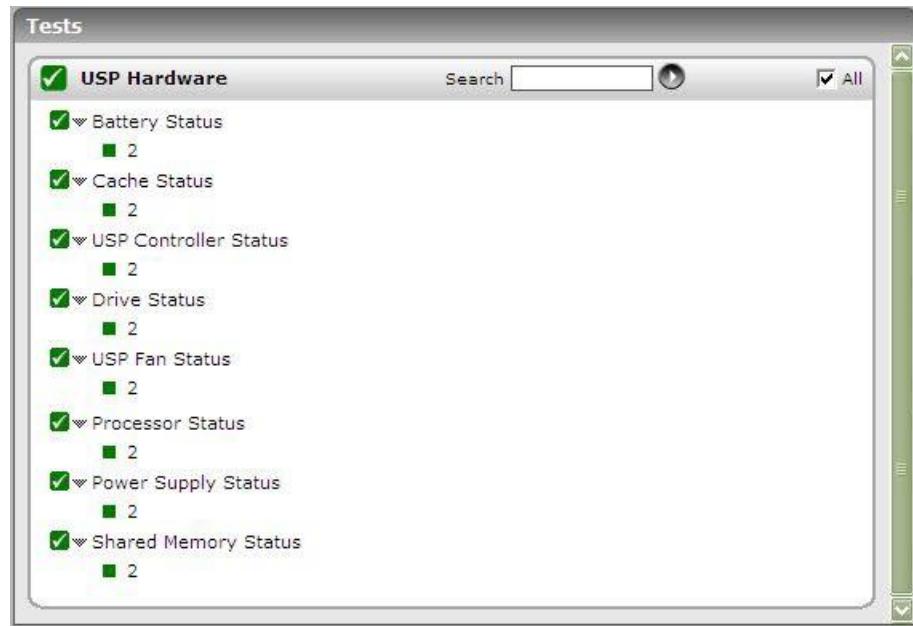
Figure 3.2: The tests mapped to the USP Hardware layer

3.3.1 Battery Status Test

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

Purpose	Reports the current status of the batteries used by each RAID store on the Hitachi USP storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Battery status: Indicates the current status of the batteries of this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.3.2 Cache Status Test

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.

Purpose	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 USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored

Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Cache status: Indicates the current status of the cache used by this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.3.3 USP Controller Status Test

Every RAID store on the USP 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.

Purpose	Reports the current status of the controller associated with each RAID store on the storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Controller status: Indicates the current status of the controller of this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➤ 1 – noError ➤ 2 – acuteError ➤ 3 – seriousError ➤ 4 – moderateError ➤ 5 – serviceError

3.3.4 Drive Status Test

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

Purpose	Reports the current drive status of each RAID store on the storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored

Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Drive status: Indicates the current status of the drive used by this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.3.5 USP Fan Status Test

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

Purpose	reports the current status of the fan used by each RAID store on the storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored

Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Fan status: Indicates the current status of the fan used by this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.3.6 Processor Status Test

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

Purpose	Reports the current status of the processor that each RAID store on the storage device supports
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored

Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Processor status: Indicates the current status of the processor used by this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.3.7 Power Supply Status Test

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

Purpose	Reports the current status of the power supply unit used by each RAID store on the storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Power supply status: Indicates the current status of the power supply unit used by this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.3.8 Shared Memory Status Test

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

Purpose	Reports the current status of the power supply unit used by each RAID store on the storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	An external agent

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

	14. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every RAID store on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Shared memory status: Indicates the current status of the shared memory used by this RAID store.	Number	This measure can report any value between and equal to 1 and 5. The values and the states they represent are discussed below: ➢ 1 – noError ➢ 2 – acuteError ➢ 3 – seriousError ➢ 4 – moderateError ➢ 5 – serviceError

3.4 The USP 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 3.3: The tests mapped to the USP 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 talk about the **PortUsage** test alone.

3.4.1 Port Usage Test

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

Purpose	Provides information on I/O rates for all the host bus adapters connected to each Storage unit Port
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed
	
	2. **Host** - The host for which the test is to be configured.
	
	3. **port** – The port at which the device listens. By default, this is set to NULL.
	
	4. **userid, password, confirm password** - The test 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*;
	
	Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box.
	
	5. **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.

Outputs of the test	One set of results for every port on the Hitachi USP device monitored
Measurements made by the test	**Measurement**	**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.

3.5   The USP 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 Processors
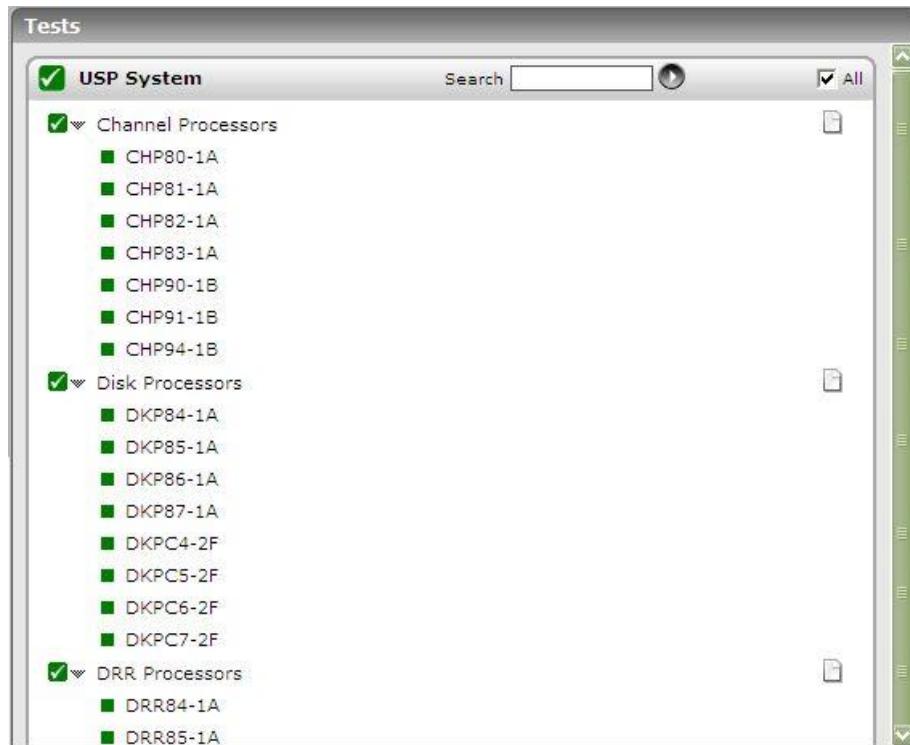
Figure 3.4: The tests mapped to the USP System layer

3.5.1 Channel Processors Test

A channel processor (CHP), which is contained in a channel adapter (CHA), processes host commands and controls data transfer between hosts and the cache. A channel adapter typically contains multiple channel processors.

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

Purpose	Monitors the usage of each channel processor, and reveals over-utilized processors (if any).		
Target of the test	A Hitachi USP storage device		
Agent deploying the test	A remote agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port at which the device listens. By default, this is set to NULL. 4. **userid, password**, **confirm password** - The test 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*; Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box. 5. **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.		
Outputs of the test	One set of results for every channel processor on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**

	Channel processor usage: Indicates the percentage of time for which this channel processor 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 processors, you can accurately detect imbalances in load distribution, and rapidly identify the affected channel processors. 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;

3.5.2 Disk Processors Test

A disk processor (DKP), which is contained in a disk adapter (DKA), controls data transfer between the cache and the disk devices. A disk adapter contains multiple disk processors (DKPs).

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

Purpose	Monitors the usage of each disk processor, and reveals over-utilized processors (if any).
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port at which the device listens. By default, this is set to NULL. 4. **userid**, **password**, **confirm password** - The test 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*; Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box. 5. **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 5 seconds.

Outputs of the test	One set of results for every disk processor on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Disk processor usage: Indicates the percentage of time for which this disk processor was in use.	Percent	A high value or a value close to 100% is indicative of excessive usage of the disk processor. By comparing the value of this measure across processors, 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; ➢ Use Volume Migration to migrate logical volumes from high-usage parity groups to low-usage parity groups;

3.5.3 DRR Processors Test

A Data Recovery and Reconstruction Processor (DRR) is a microprocessor located on the DKAs 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).

Purpose	Monitors the usage of each DRR processor, and reveals over-utilized processors (if any).
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed
	2. **Host** - The host for which the test is to be configured.
	3. **port** – The port at which the device listens. By default, this is set to NULL.
	4. **userid, password, confirm password** - The test 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*;
	Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box.
	5. **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 5 seconds.
Outputs of the test	One set of results for every disk processor on the Hitachi USP device monitored

Measurements made by the test	Measurement	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.

3.6 The USP 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;
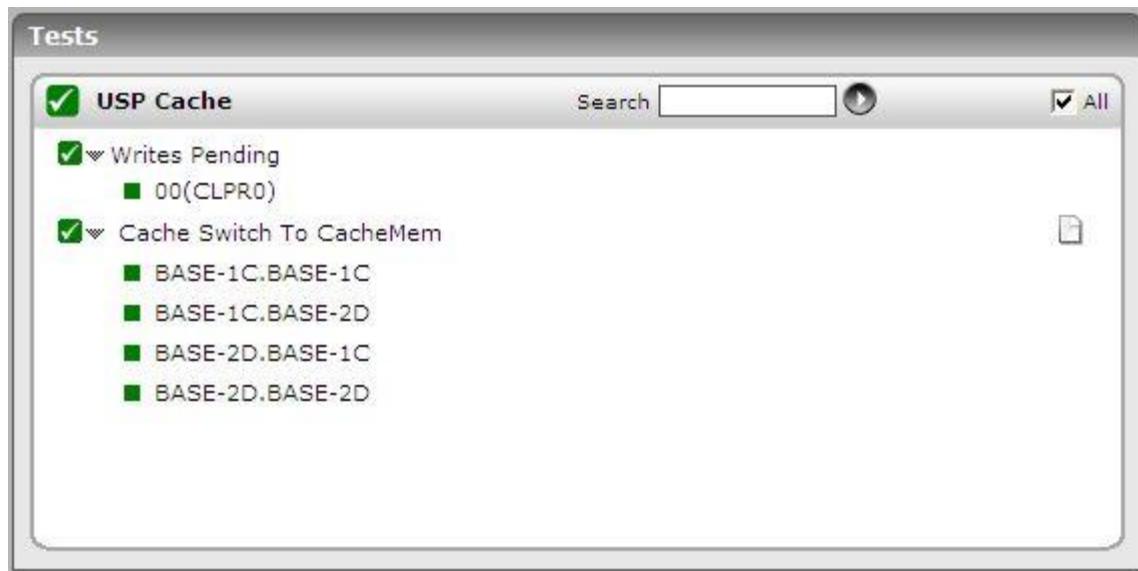
Figure 3.5: The tests mapped to the USP Cache layer

3.6.1 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.

Purpose	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 USP storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed
	
	2. **Host** - The host for which the test is to be configured.
	
	3. **port** – The port at which the device listens. By default, this is set to NULL.
	
	4. **userid, password**, **confirm password** - The test 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*;
	
	Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box.
	
	5. **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.

Outputs of the test	One set of results for every cache logical partition on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Writes pending rate: 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.

3.6.2 Cache Switch To CacheMem 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. This test monitors the usage of each cache switch to cache memory access path to facilitate such an analysis.

Purpose	Monitors the usage of each cache switch to cache memory access path and reveals how the data transfer in each path is progressing to determine whether a slowdown in any of the paths could have contributed to the high write-pending rate
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed
	2. **Host** - The host for which the test is to be configured.
	3. **port** – The port at which the device listens. By default, this is set to NULL.
	4. **userid, password, confirm password** - The test 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*;
	Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box.
	5. **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.
Outputs of the test	One set of results for every cache switch to cache memory access path on the Hitachi USP device monitored
Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Short CSWCMA: Indicates the percentage usage of this cache switch to cache memory access path.	Percent	A very high value or a value close to100% 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 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.

3.7 The USP 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 3.6: The tests mapped to the USP Disk layer

3.7.1 Logical Device Details Test

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

Purpose	Monitors the I/O activity on each logical volume (LDEV) on the storage device, and indicates irregularities in load balancing across the volumes
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port at which the device listens. By default, this is set to NULL. 4. **userid, password**, **confirm password** - The test 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*; Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box. 5. **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.

Outputs of the test	One set of results for every logical volume on the Hitachi USP device monitored		
Measurements made by the test	**Measurement**	**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.
	Transaction 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 cach	Number/Sec	

3.7.2 Lun Details Test

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

Purpose	Monitors the I/O traffic and data transfers conducted by each LUN on a storage device, and indicates irregularities in load balancing across LUNs
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed
	2. **Host** - The host for which the test is to be configured.
	3. **port** – The port at which the device listens. By default, this is set to NULL.
	4. **userid, password, confirm password** - The test 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*;
	Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box.
	5. **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.
Outputs of the test	One set of results for every LUN on the Hitachi USP device monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	I/O operations rate: Indicates the number of read-write operations performed on this LUN per second.	IOPS	A high value for this measure is indicative of high I/O activity on the 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	

	C2D transfer rate: 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.
	Response time: Indicates the current responsiveness of this LUN to I/O requests.	Microseconds	Ideally, the value of this measure should be low.

3.7.3 Parity Group Usage Test

A parity group is a group of hard disk drives (HDDs) that form the basic unit of storage for the TagmaStore USP and NSC subsystem. All HDDs in a parity group must have the same physical capacity. This test monitors the usage of the parity groups on the storage device.

Purpose	Monitors the usage of the parity groups on the storage device
Target of the test	A Hitachi USP storage device
Agent deploying the test	A remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured. 3. **port** – The port at which the device listens. By default, this is set to NULL. 4. **userid, password, confirm password** - The test 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*; Provide the credentials of this user against the **userid** and **password** parameters. Confirm the password by retyping it in the **confirm password** text box. 5. **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.
Outputs of the test	One set of results for every parity group on the Hitachi USP device monitored

Measurements made by the test	Measurement	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 percenatage 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.
	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.
	Transfer between disk and cache: Indicates the rate at which data transfer operations are performed between this parity group and the cache.	Number/Sec	

Chapter

4

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 **Hitachi Storage Devices**. 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.