Monitoring Hitachi USP SAN

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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. This is exactly what eG Enterprise does!

Chapter 2: How to Monitor Hitachi USP SAN Device Using eG Enterprise?

eG Enterprise monitors the Hitachi USP SAN device in an agent-less manner. To monitor the Hitachi USP SAN Device, configure a 'single agent' to function both as a **remote agent** and as an **external agent** in the environment. This agent uses the following approaches for collecting metrics from the Hitachi USP SAN 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.

2.1 Pre-requisites for Monitoring the Hitachi USP SAN

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:

1. The SNMP service should be enabled on the device;
2. The eG SNMP trap receiver service should be installed on the external agent host;

3. The storage device should be configured to send SNMP traps to the external agent host;
4. The *Hitachi Performance Monitor software* should be available;
5. The **Java export** utility should be available on the remote agent host;
6. The eG agent should be configured with the credentials of a special user account, which is specifically created for use with the export utility; this account should fulfill the following conditions:
    - Should not possess the 'write' permission;
    - Can be of any user type; however, to ensure that the eG agent collects statistics pertaining to all storage partitions, it is recommended that this user is of type storage administrator;

2.2 Managing the Hitachi USP SAN Server

The eG Enterprise cannot automatically discover the Hitachi USP SAN Server. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a Hitachi USP SAN component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select Hitachi USP SAN as the **Component type**. Then, click the **Add New Component** button. This will invoke 2.2.

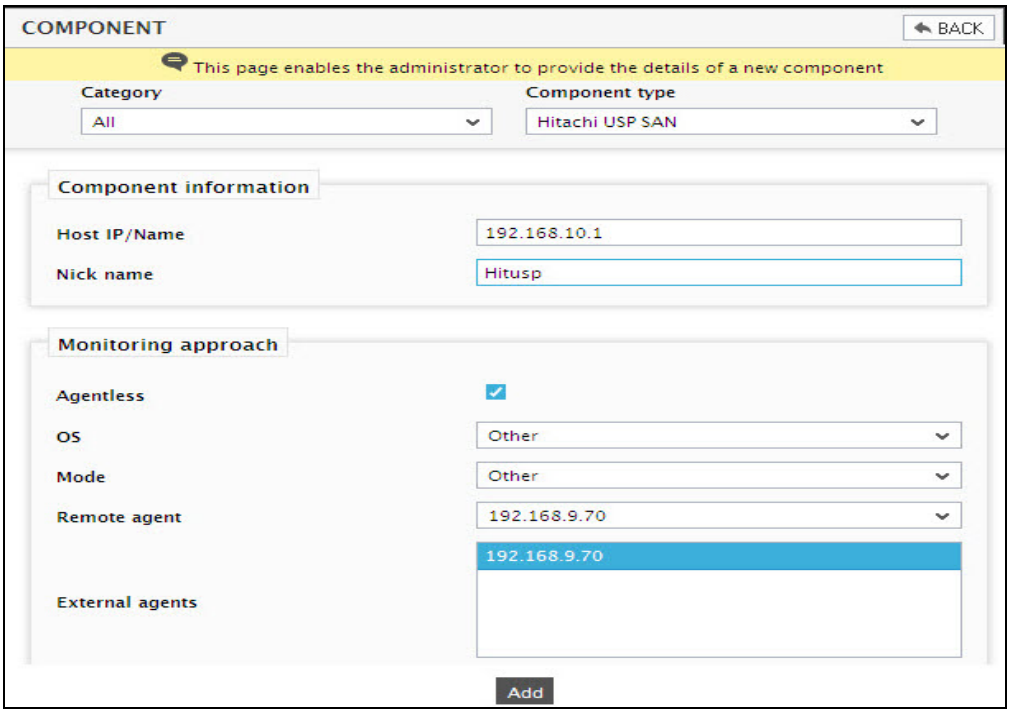


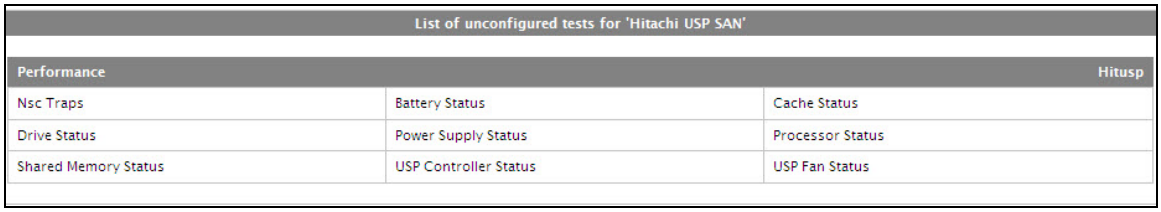
Figure 2.1: Adding a Hitachi USP SAN server

4. After specifying the **Host IP**, **Nick name** of the Hitachi USP SAN server, select **Other** as the **OS** and **SNMP** as the **MODE**. Then, click the **Add** botton to register the changes.

   Note:

   Though the **Mode** is set to **SNMP** while adding a new component, the eG agent will be able to collect metrics from the target environment through the specified CLI path.

5. When you attempt to sign out, a list of unconfigured tests appears as shown in Figure 2.2.



List of unconfigured tests for 'Hitachi USP SAN'

Performance		Hitusp
Nsc Traps	Battery Status	Cache Status
Drive Status	Power Supply Status	Processor Status
Shared Memory Status	USP Controller Status	USP Fan Status

Figure 2.2: List of Unconfigured tests to be configured for the Hitachi USP SAN server

6. To know how to configure these tests, refer to **Monitoring the Hitachi USP**.
7. Finally, signout of the administrative interface.

Chapter 3: Monitoring the Hitachi USP

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.

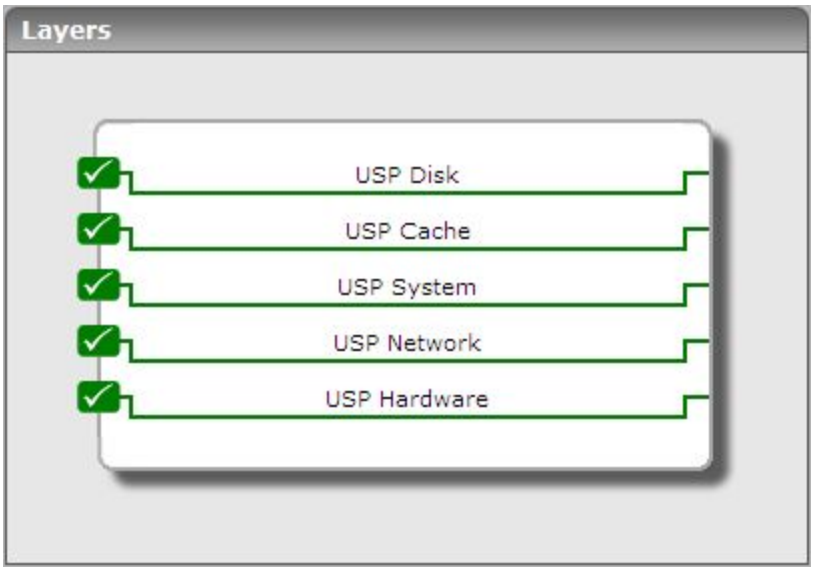


Figure 3.1: The layer model of the Hitachi USP storage device

Once the pre-requisites discussed in Section **2.1** 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.

3.1 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.

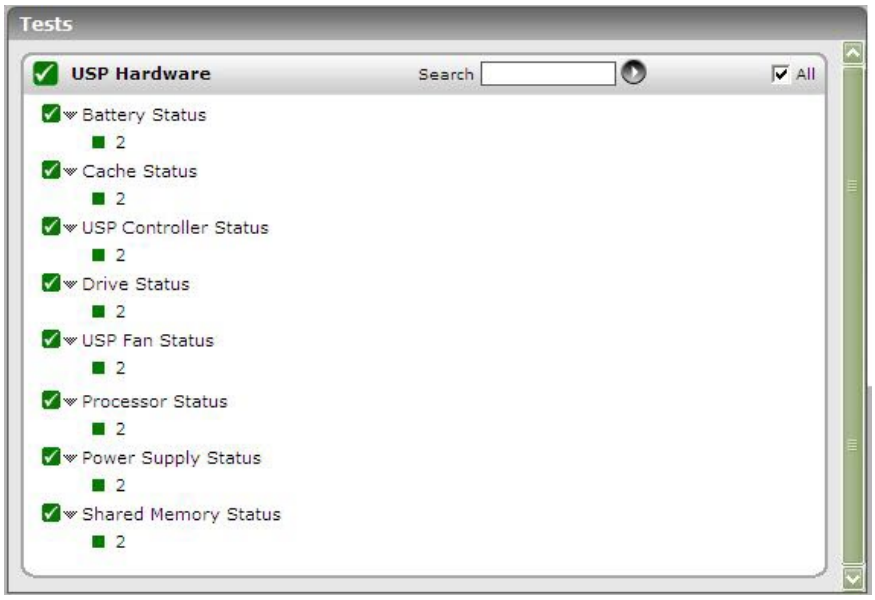


Figure 3.2: The tests mapped to the USP Hardware layer

3.1.1 Battery Status Test

This test 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

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP

Parameter	Description
	transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			• 2 – acuteError • 3 – seriousError • 4 – moderateError • 5 – serviceError

3.1.2 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.

Target of the test : A Hitachi USP storage device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the

Parameter	Description
	required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameter	Description
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

3.1.3 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.

Target of the test : A Hitachi USP storage device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

Parameter	Description
	Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			are discussed below: • 1 – noError • 2 – acuteError • 3 – seriousError • 4 – moderateError • 5 – serviceError

3.1.4 Drive Status Test

This test 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

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote

Parameter	Description
	SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameter	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

3.1.5 USP Fan Status Test

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

Target of the test : A Hitachi USP storage device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP

Parameter	Description
	transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			• 2 – acuteError • 3 – seriousError • 4 – moderateError • 5 – serviceError

3.1.6 Processor Status Test

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

Target of the test : A Hitachi USP storage device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the

Parameter	Description
	required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameter	Description
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

3.1.7 Power Supply Status Test

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

Target of the test : A Hitachi USP storage device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP

Parameter	Description
	transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

Measurement	Description	Measurement Unit	Interpretation
			• 2 – acuteError • 3 – seriousError • 4 – moderateError • 5 – serviceError

3.1.8 Shared Memory Status Test

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

Target of the test : A Hitachi USP storage device

Agent deploying the test : An external agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB

Parameter	Description
	using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.

Parameter	Description
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

3.2 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

The **Network** test mapped to this layer is discussed in the *Monitoring Unix and Windows Servers* document. The section that will follow will talk about the PortUsage test alone.

3.2.1 Port Usage Test

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

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every port on the Hitachi USP device monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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

Parameter	Description
	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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

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

3.3 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

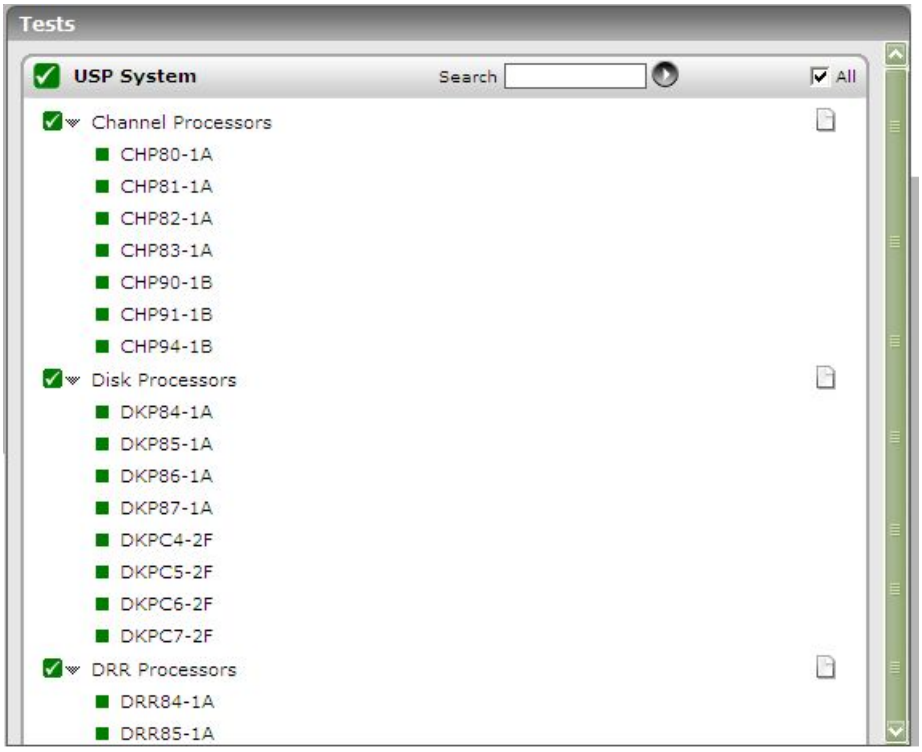


Figure 3.4: The tests mapped to the USP System layer

3.3.1 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).

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every channel processor on the Hitachi USP device monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

Measurement	Description	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

Measurement	Description	Measurement Unit	Interpretation
			ports with CHPs that are less utilized, so as to balance front-end usage;

3.3.2 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).

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every disk processor on the Hitachi USP device monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.

Parameter	Description
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 5 seconds.

Measurements made by the test

Measurement	Description	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;

3.3.3 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).

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every disk processor on the Hitachi USP device monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 5 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
DRR processor usage	Indicates the percentage of time for which this DRR processor was in use.	Percent	A high value or a value close to 100% is indicative of a high write penalty condition. In such a case, you are advised to consult with your Hitachi Data Systems representative for for further information. By comparing the value of this

Measurement	Description	Measurement Unit	Interpretation
			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.

3.4 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;

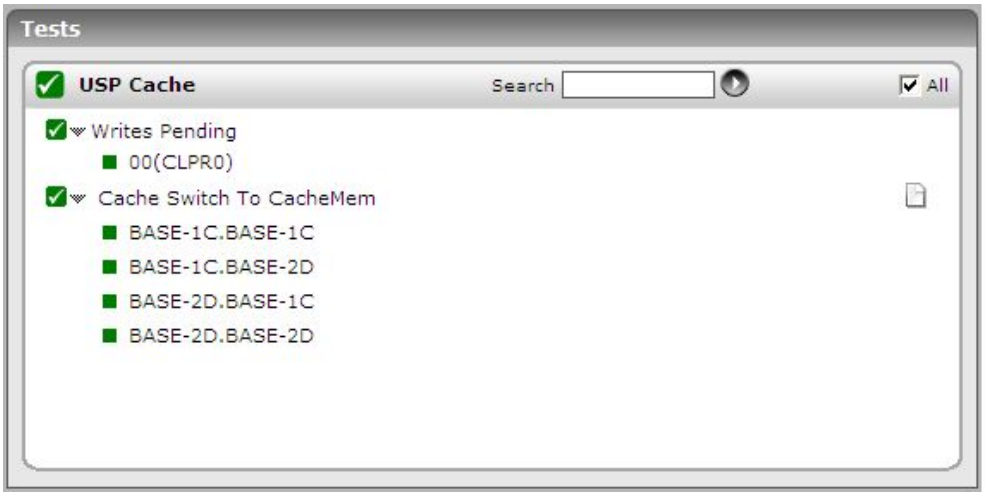


Figure 3.5: The tests mapped to the USP Cache layer

3.4.1 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.

arget of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

Measurement	Description	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

Measurement	Description	Measurement Unit	Interpretation
			written, thus rendering the write data pending for a long time.

3.4.2 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.

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.

Parameter	Description
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

Measurement	Description	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 to 100% for this measure could indicate that the access path is over-utilized, probably owing to a slow data write rate to the cache. Comparing the value of 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.

3.5 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.

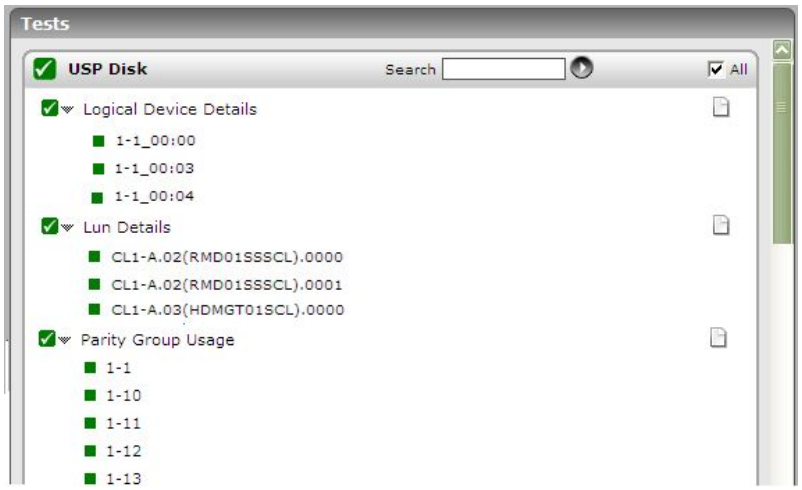


Figure 3.6: The tests mapped to the USP Disk layer

3.5.1 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.

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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;

Parameter	Description
	• 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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

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

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

3.5.2 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.

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

Measurement	Description	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	Percent	

Measurement	Description	Measurement Unit	Interpretation
	access mode.		
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.

3.5.3 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.

Target of the test : A Hitachi USP storage device

Agent deploying the test : A remote agent

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

Configurable parameters for the test

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

Parameter	Description
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host is listening. By default, this is set to *NULL*.
UserID, Password and 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.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 3 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
I/O operations rate	Indicates the number of read-write operations performed on this parity group per second.	IOPS	A high value for this measure is indicative of high I/O activity on the parity group. Comparing the value of this measure across parity groups can accurately reveal which parity groups are overloaded, and also enable administrators to easily detect irregularities in load distribution across the parity groups. To uniformly balance load across parity groups, you should consider installing additional HDDs, or you can use volume migration to migrate volumes from high-usage parity groups to low-usage parity groups.
Transactions rate	Indicates the rate at which data transfers occur on this	KB/Sec	

Measurement	Description	Measurement Unit	Interpretation
	parity group.		
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	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.