
# Monitoring Hitachi AMS Storage Device

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

# Table of Contents

# Table of Figures

# Chapter 1: Introduction

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. It is therefore imperative that the availability and operations of the Hitachi AMS storage is monitored 24x7. This is where eG Enterprise helps administrators!

# Chapter 2: How to Monitor Hitachi AMS Storage Device Using eG Enterprise?

eG Enterprise monitors the Hitachi AMS storage device in an agentless manner. In order to monitor the storage device, eG Enterprise deploys a **remote agent** and an **external agent**. For collecting performance statistics, eG agent uses the following information sources:

- The **Performance Monitor** software that is installed with the storage 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.

- The **SNMP MIB** of the device;

  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 storage device.

To enable the remote or external agent to connect and communicate with the Hitachi AMS storage device, a set of pre-requisites should be fulfilled. These requirements have been discussed in Section **2.1**. Once the pre-requisites are fulfilled, start monitoring the storage device. The broad steps for monitoring the storage device using eG Enterprise are as follows:

- Managing the Hitachi AMS Storage Device
- Configuring the tests

These steps have been discussed in following sections.

## 2.1 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:

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. SNMP traps should be enabled on the device and configured to send traps to the external agent host;
4. The Hitachi Performance Monitor software should be available;
5. The Storage Navigator Modular (AMS) Version 7.0 or later should be available on the remote agent host;
6. 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.
7. 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
```

8. Micro program 0710/A or later is required;

## 2.2 Managing the Hitachi AMS SAN

The eG Enterprise cannot automatically discover the Hitachi AMS SAN. 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 AMS 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 AMS SAN* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

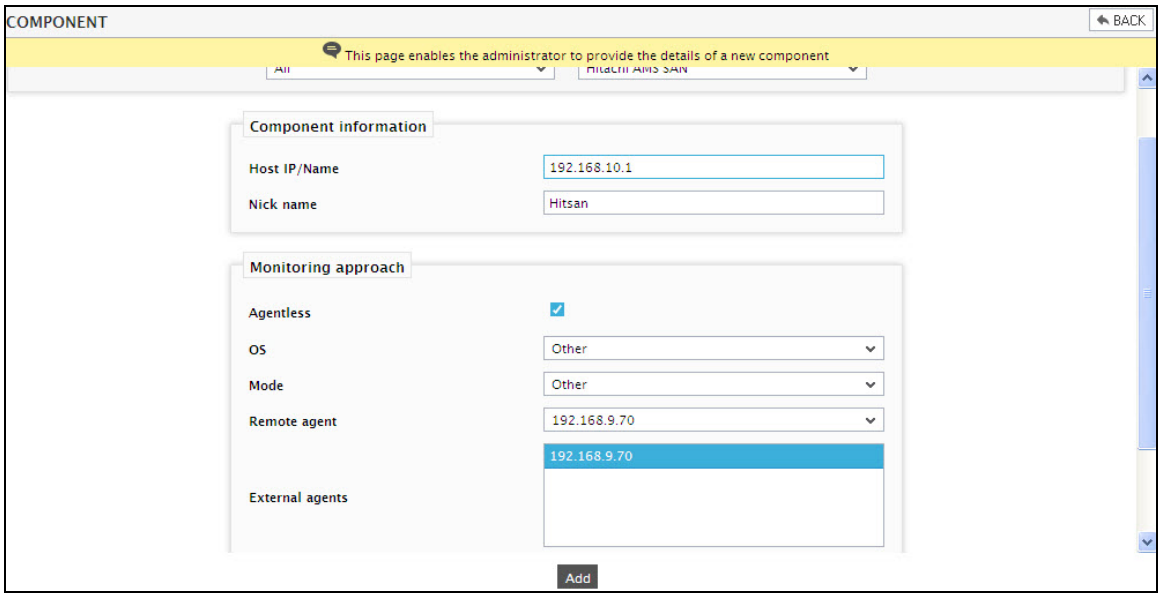


Figure 2.1: Adding a Hitachi AMS SAN server

4. Specify the **Host IP** and the **Nick name** of the Hitachi AMS SAN. Also select **Other** as the **OS** and **SNMP** as the **Mode**. Then, click the **Add** button to register the changes.

## 2.3 Configuring the tests

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

List of unconfigured tests for 'Hitachi AMS SAN'

| Performance | | Hitsan |
|---|---|---|
| Cache Memory Usage | Disk To Cache Load | Drive Load |
| Drive Operation | LUN Load | Port Load |
| Raid Group Load | Storage Processor Load | Cache Load |
| LUN Switch Details | Port Status | Trap Status |

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

2. Click on the test names to configure. To know how to configure the tests, refer to **Monitoring the Hitachi AMS Storage Device**.

3. Once all tests are configured, signout of the eG administrative interface.

# Chapter 3: Monitoring the Hitachi AMS Storage Device

The Hitachi AMS SAN 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.

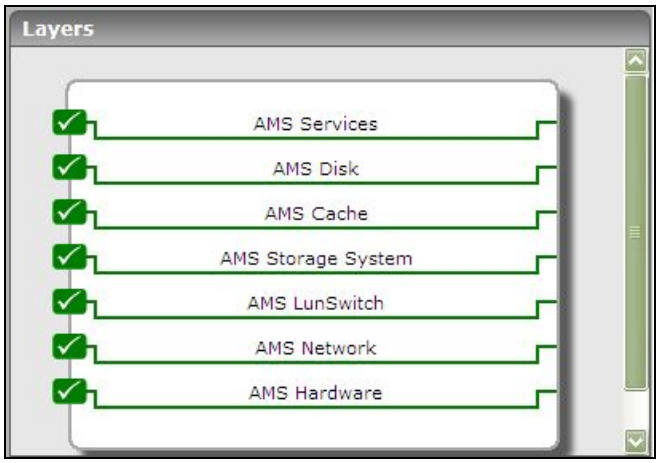


Figure 3.1: The layer model of an Hitachi AMS device

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 the layer model elaborately.

## 3.1 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.

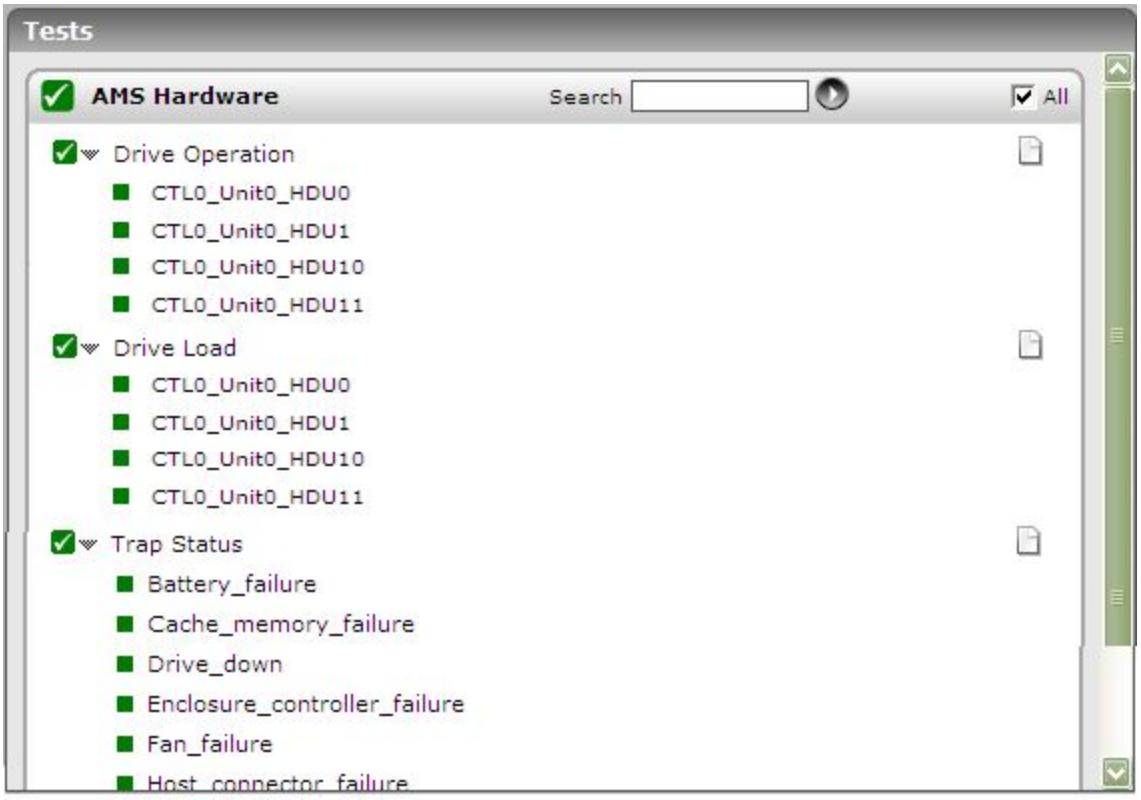


Figure 3.2: The tests mapped to the AMS Hardware layer

### 3.1.1 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

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

### Configurable parameters for the test

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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:<br>*startnsmen*<br>*auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

### Measurements made by the test

| Measurement | Description | 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 | |

## 3.1.2 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 this test.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each drive on the storage device monitored.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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:<br>*startnsmen*<br>*auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

**Measurements made by the test**

| Measurement | Description | 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 |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | | | 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 | |

### 3.1.3 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for each of the traps configured for the storage device monitored.

**Configurable parameters for the test**

| Parameters | Description |
|---|---|
| Test Period | How often should the test be executed |
| Host | The host for which the test is to be configured. |
| Source Address | 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. |
| OID Value | 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: |

| 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 |

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 hostT 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

| Parameters | Description |
|---|---|
| | 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:<br><br>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.<br><br>In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:<br><br>Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.<br><br>Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID. |
| 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. |
| TrapOIDs | By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified sourceaddresses. 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. |
| 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. |
| 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.<br><br>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:<br><br>• The eG manager license should allow the detailed diagnosis capability |

| Parameters | Description |
|---|---|
| | • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0. |

**Measurements made by the test**

| Measurement | Description | 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. |

## 3.2 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.

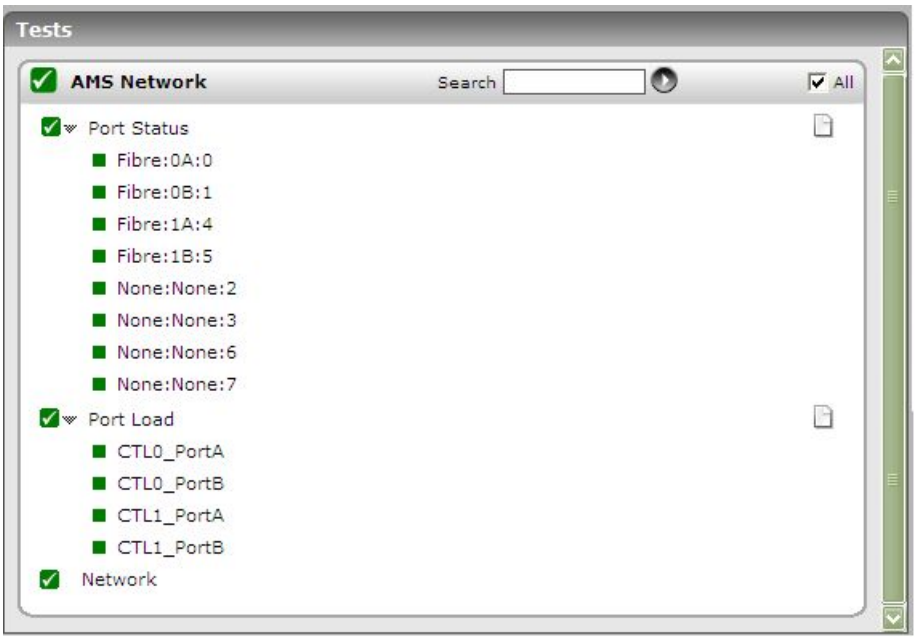


Figure 3.3: The tests mapped to the AMS Network layer

## 3.2.1 Port Status Test

This test 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

**Outputs of the test :** One set of results for each port type on the storage device being monitored.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device 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. |

| Parameter | Description |
|---|---|
| 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 transactions. You can choose between the following options:<br>• **MD5** – Message Digest Algorithm<br>• **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 |

| Parameter | Description |
|---|---|
| | selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:<br>• **DES** – Data Encryption Standard<br>• **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 |
|---|---|---|---|
| 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. |

## 3.2.2 Port Load Test

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

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for every port on the storage device monitored.

### Configurable parameters for the test

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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:<br>*startnsmen*<br>*auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

### Measurements made by the test

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| 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 | |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| 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 | |

## 3.3 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.

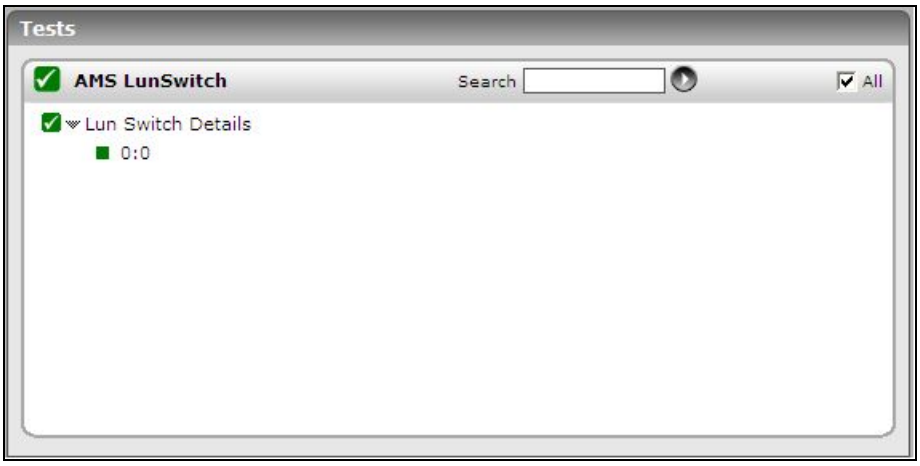


Figure 3.4: The tests mapped to the AMS LunSwitch layer

## 3.3.1 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** An external agent

**Outputs of the test :** One set of results for every LUN switch on the storage device.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device 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. |

| Parameter | Description |
|---|---|
| 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 transactions. You can choose between the following options:<br>• **MD5** – Message Digest Algorithm<br>• **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 |

| Parameter | Description |
|---|---|
| | selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:<br>• **DES** – Data Encryption Standard<br>• **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 |
|---|---|---|---|
| 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.<br>• 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.<br>• If the value of this measure is 0, it indicates that the control status of the LUN switch is Off. |

## 3.4 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.

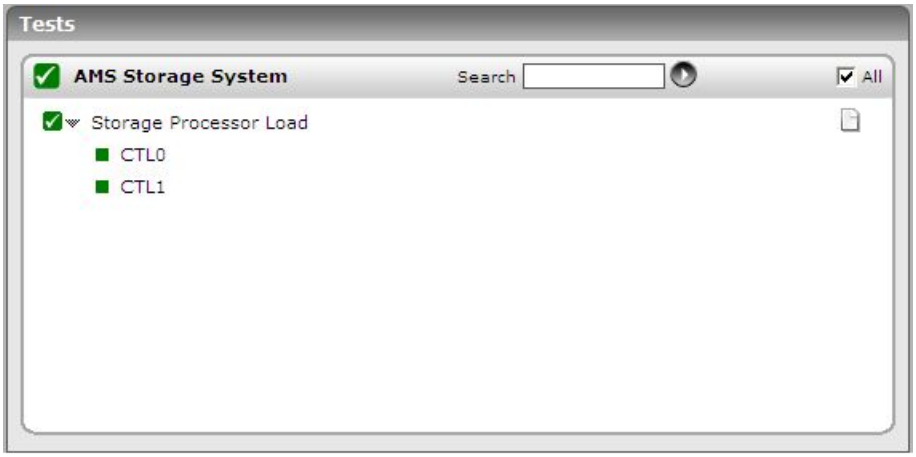


Figure 3.5: The test mapped to the AMS Storage System layer

### 3.4.1 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each processor supported by the storage device monitored.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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 |

| Parameter | Description |
|---|---|
| | CLI directory on the Storage Navigator Client:<br>*startnsmen*<br>*auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

**Measurements made by the test**

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| Usage | Indicates the percentage of CPU resources of this processor currently utilized. | Percent | 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. |

## 3.5 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.

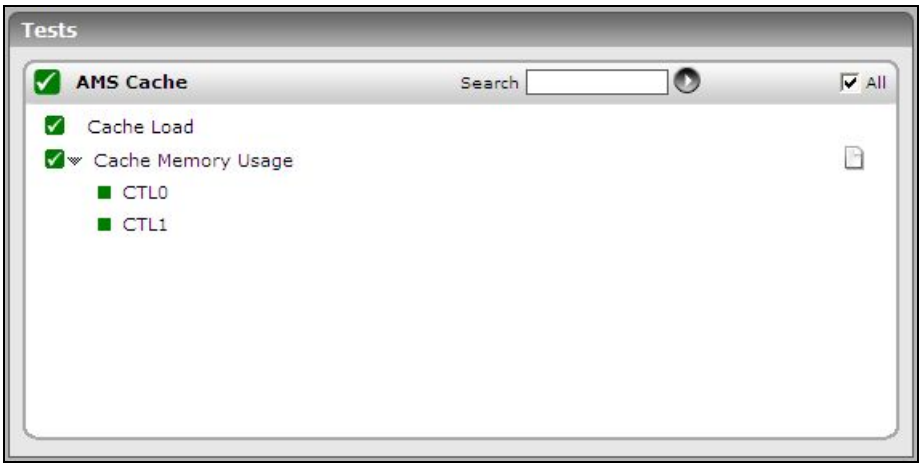


Figure 3.6: The tests mapped to the AMS Cache layer

## 3.5.1 Cache Load Test

This test 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

**Outputs of the test :** One set of results for each cache supported by the storage device monitored.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device 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 |

| Parameter | Description |
|---|---|
| | 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 transactions. You can choose between the following options:<br>• **MD5** – Message Digest Algorithm<br>• **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:<br>• **DES** – Data Encryption Standard<br>• **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 |
|---|---|---|---|
| WriteDataRate | Indicates the rate at which data is written to the cache memory of the storage device. | Bytes/sec | |

## 3.5.2 Cache Memory Usage Test

This test 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

**Outputs of the test :** One set of results for every cache on the storage device.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| UnitName | Specify the name of the storage unit to be monitored. To determine the unit name |

| Parameter | Description |
|---|---|
| | 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:<br>*startnsmen*<br>*auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

### Measurements made by the test

| Measurement | Description | 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.<br>On the other hand, if the values of these measures are low, it is a sign of good cache health. |
| 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 | |
| Total queue usage rate | Indicates the percentage of the cache queue currently utilized. | Percent | |

## 3.6 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 3.7: The tests mapped to the AMS Disk layer

### 3.6.1 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each LUN on the storage device monitored.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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:<br>*startnsmen* |

| Parameter | Description |
|---|---|
| | *auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

### Measurements made by the test

| Measurement | Description | 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. |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| 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 | |

## 3.6.2 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each RAID group on the storage device monitored.

### Configurable parameters for the test

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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:<br>*startnsmen*<br>*auunitref*<br>The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

### Measurements made by the test

| Measurement | Description | 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 | IOPS | |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | on this RAID group per second. | | |
| 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 | |

## 3.7 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.

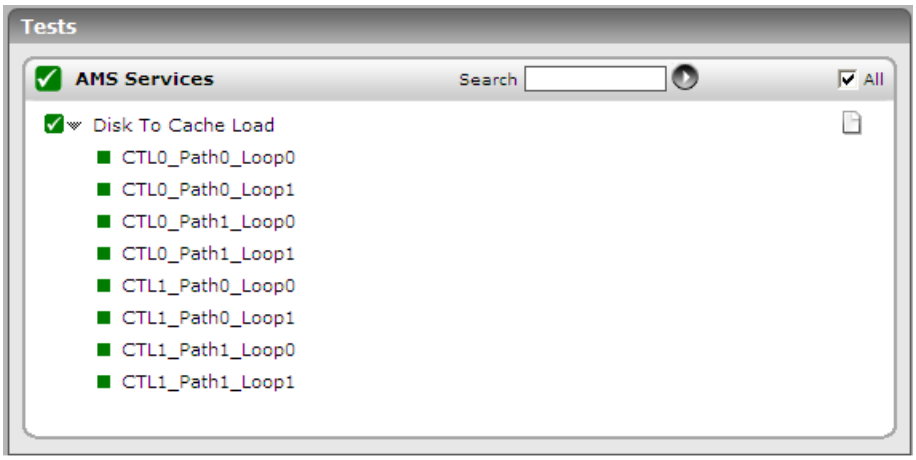


Figure 3.8: The test mapped to the AMS Services Layer

## 3.7.1 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.

**Target of the test :** A Hitachi AMS storage device

**Agent deploying the test :** A remote agent

**Outputs of the test :** One set of results for each backend loop.

**Configurable parameters for the test**

| Parameter | Description |
|---|---|
| Test Period | How often should the test be executed. |
| Host | The IP address of the storage device. |
| 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:<br>*startnsmen*<br>*auunitref* |

| Parameter | Description |
|---|---|
| | The output of the command includes the Name of the storage unit. DF700M_75011118 is a sample unit name. |
| MCType | Indicate the machine type. The value can be **AMS** or **WMS**. By default, this parameter is set to **AMS**. |
| SNClientLocation | Specify the full path to the install directory of the storage navigator. |
| 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. |

### Measurements made by the test

| Measurement | Description | 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 | KB/sec | |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| | second. | | |
| 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 | |

# 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.