Monitoring Data Domain Storage System

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: HOW TO MONITOR DATA DOMAIN STORAGE SYSTEM USING EG ENTERPRISE? 2

2.1 Managing the Data Domain Storage System 2

CHAPTER 3: MONITORING DATA DOMAIN 5

3.1 The Hardware Layer 6

3.1.1 Fan Test 6

3.1.2 Disks Test 9

3.1.3 NVRAM Test 13

3.1.4 NVRAM Battery Test 15

3.2 The Operating System Layer 18

3.2.1 Power Module Test 19

3.2.2 Sensor Test 22

3.2.3 System Details Test 25

3.3 The Data Domain File System Layer 28

3.3.1 File System Status Test 28

3.3.2 File System Test 31

3.3.3 File System Compression Test 34

3.3.4 Event Log Test 36

ABOUT EG INNOVATIONS 40

Table of Figures

Figure 2.1: Adding a Data Domain 3

Figure 2.2: List of Unconfigured tests to be configured for the Data Domain server 3

Figure 2.3: Configuring the Data Domain Even Log test 4

Figure 3.1: The layer model of a Data Domain 5

Figure 3.2: The tests mapped to the Hardware layer 6

Figure 3.3: The tests mapped to the Operating System layer 19

Figure 3.4: The tests mapped to the Data Domain File System layer 28

Chapter 1: Introduction

The Data Domain storage system is a stand alone backup-to-disk appliance offering a network attached storage (NAS) front end (over IP) and an optional virtual tape library (VTL) front end (over FC). Both these configurations include data deduplication capability to efficiently store data that is written to the appliance. The Data Domain storage systems are inline deduplication appliances which means that all the data sent to the appliance is deduplicated immediately.

The Data Domain storage system with its data deduplication capability does the following:

- Eliminates redundant data from backups to reduce storage, elabling longer onsite retentionand reduce replication costs
- Performs sub file comparisons on variable length data blocks to capture small block inserts and overstrikes in unstructured and structured data.
- Provides high performing inline deduplication.

Includes built-in data compression that is additive to deduplication in the data reduction process. Since the storage system plays a crucial role in delivering resources to the environment, issues in its performance can cause serious fatalities, data loss etc. Therefore, it is essential to periodically monitor the storage system round the clock. This is exactly what the eG Enterprise does.

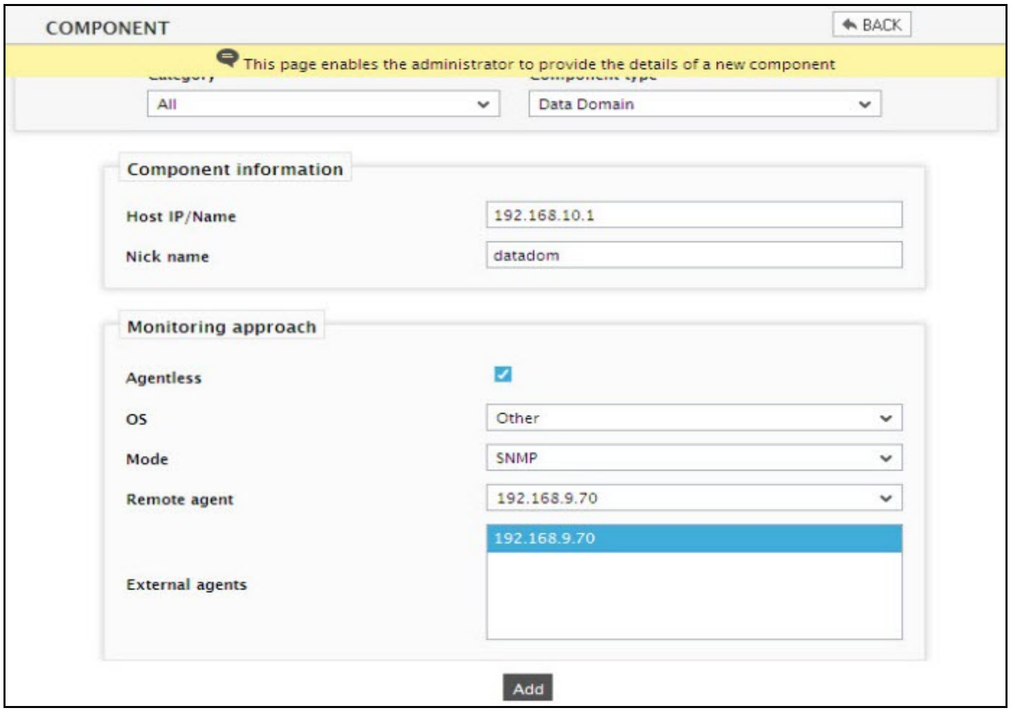
Chapter 2: How to Monitor Data Domain Storage System using eG Enterprise?

eG Enterprise monitors the Data Domain in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent is capable of polling the SNMP MIB Of the Data Domain at regular intervals and fetching statistics related its performance.

2.1 Managing the Data Domain Storage System

The eG Enterprise cannot automatically discover the Data Domain storage system so that you need to manually add the component for monitoring. The eG Enterprise is capable of automatically managing the components that are added manually. To add a Data Domain 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 Data Domain as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Data Domain

Component information

Host IP/Name: 192.168.10.1

Nick name: datadom

Monitoring approach

Agentless: ☑

OS: Other

Mode: SNMP

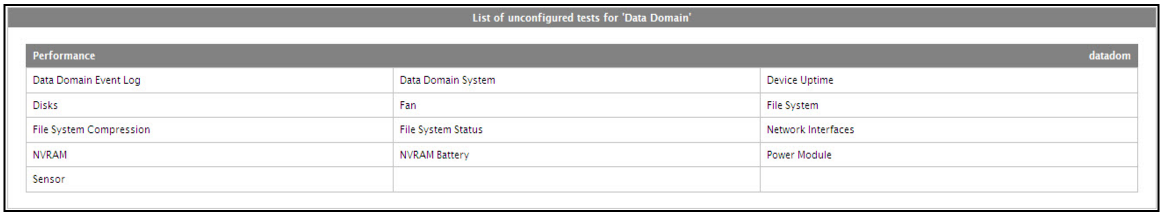
Remote agent: 192.168.9.70

External agents: 192.168.9.70

Figure 2.1: Adding a Data Domain

4. Specify the **Host IP/Name** and the **Nick name** of the Data Domain storage system in Figure 2.1. Also set the **Agentless** flag to **Yes**, select **Other** as the **OS** and **SNMP** as the **Mode**. Then click the **Add** button to register the changes.

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

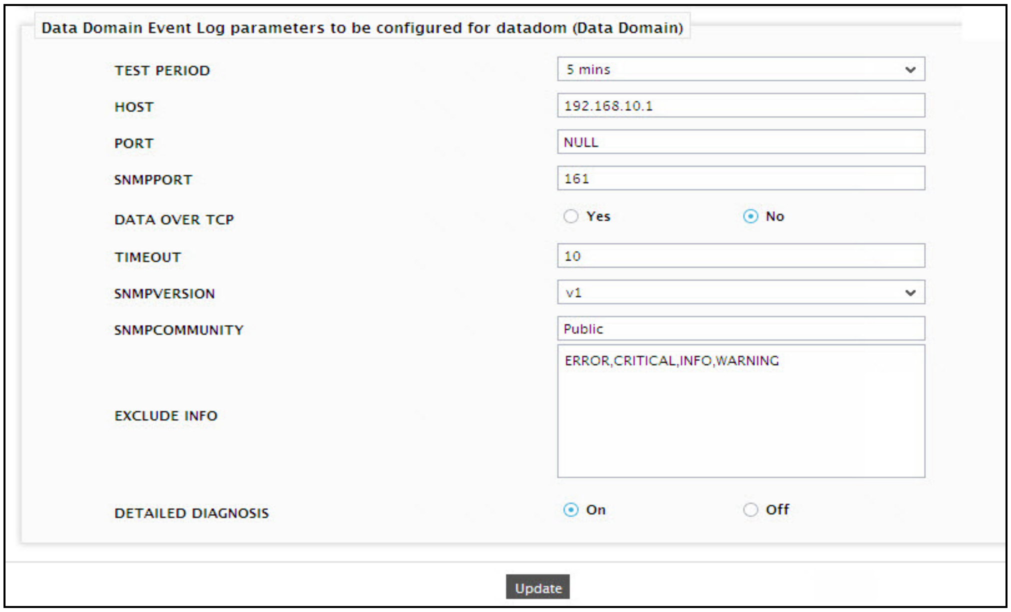


List of unconfigured tests for 'Data Domain'

Performance		datadom
Data Domain Event Log	Data Domain System	Device Uptime
Disks	Fan	File System
File System Compression	File System Status	Network Interfaces
NVRAM	NVRAM Battery	Power Module
Sensor		

Figure 2.2: List of Unconfigured tests to be configured for the Data Domain server

6. Click on any test in the list of unconfigured tests. For instance, click on the **Data Domain Even Log** test to configure it. In the page that appears, specify the parameters as shown in Chapter 2.



Data Domain Event Log parameters to be configured for datadom (Data Domain)

TEST PERIOD	5 mins
HOST	192.168.10.1
PORT	NULL
SNMPPORT	161
DATA OVER TCP	○ Yes ● No
TIMEOUT	10
SNMPVERSION	v1
SNMPCOMMUNITY	Public
EXCLUDE INFO	ERROR,CRITICAL,INFO,WARNING
DETAILED DIAGNOSIS	● On ○ Off

Figure 2.3: Configuring the Data Domain Even Log test

7. To know how to configure the tests, refer to **Monitoring Data Domain**.

8. Once all the tests are configured, sign out of the eG administrative interface.

Chapter 3: Monitoring Data Domain

eG Enterprise provides a specialized Data Domain monitoring model (see Figure 1) to monitor the hardware components of the Data Domain storage system, the I/O operations on the disks of the storage system, the status of the file system service, the space utilization of each file, the compression ration of each file system etc.

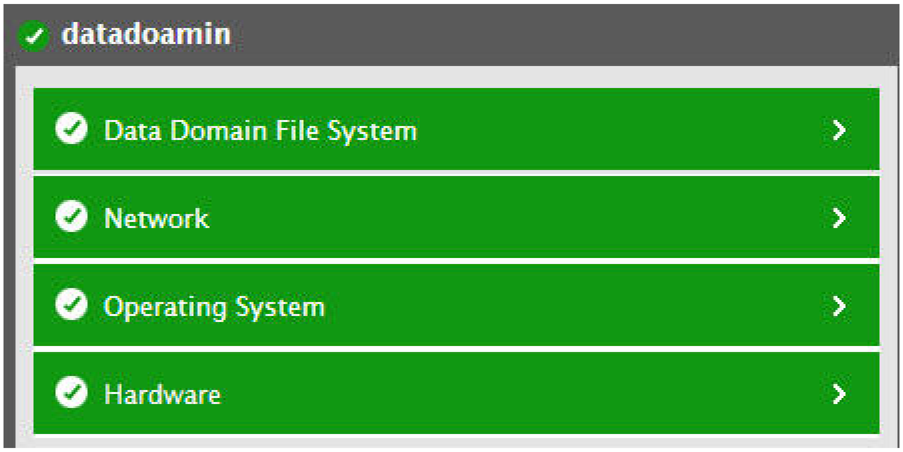


Figure 3.1: The layer model of a Data Domain

Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP MIB of the Data Domain storage system to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- What is the current status of each fan in the storage system?
- What is the current state, capacity and temperature of each disk?
- What is the size of the NVRAM in the storage system?
- Is the battery of NVRAM running out of charge?
- What is the current status of the power modules, sensors etc?
- What is the status of the file system service?
- How well the space of each file is utilized?
- How well each file system is compressed?

Since the **Network** layer has been dealt with *Monitoring Windows and Unix Servers* document, the sections to come will discuss the remaining layers of Figure 3.1.

3.1 The Hardware Layer

Using the tests mapped to the Hardware layer, administrators can proactively detect the failure of the hardware components such as fans, disks and batteries of the Data Domain storage system.

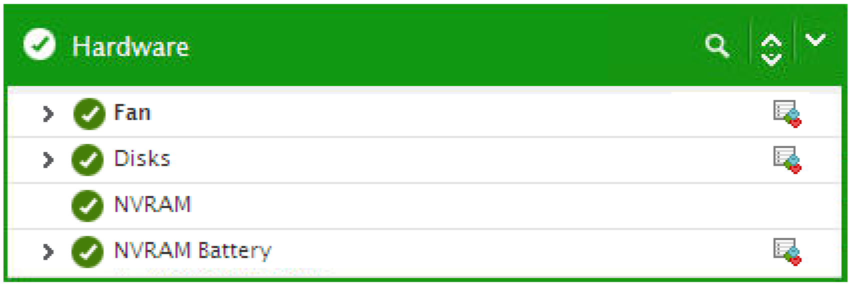


Figure 3.2: The tests mapped to the Hardware layer

3.1.1 Fan Test

This test auto discovers the fans in the Data Domain storage system and reports the current status of each fan as well as the current status of each fan’s speed. Using this test administrators can keep a check on the fan’s that are running at abnormal speed.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan in the Data Domain storage system to be 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

Parameter	Description
	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 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.

Parameter	Description
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Fan status</td><td>Indicates the current status of this fan.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Not found</td><td>0</td></tr>
<tr><td>OK</td><td>1</td></tr>
<tr><td>Fail</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of the fan.</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>However, in the graph, this measure is indicated using the Numeric Values listed in the above table.</td></tr>
<tr><td>Fan running level</td><td>Indicates the current status of this fan’s speed.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0</td></tr>
<tr><td>Low</td><td>1</td></tr>
<tr><td>Normal</td><td>100</td></tr>
<tr><td>High</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of the fan’s speed. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.</td></tr>
</table>

3.1.2 Disks Test

This test monitors the current state, capacity, temperature of each disk as well as I/O operations performed on each disk in the Data Domain storage system. Using this test, administrators can identify the error-prone disks that may fail any time using which they can avert potential disk failures. In addition, this test points administrators to the temperature of the disks using which abnormalities in the disk temperature can be easily identified and rectified before any irreversible damage is caused to the disk.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk of the Data Domain storage system to be 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
Disk status	Indicates the current status of this disk.		The values reported by this measure and their numeric equivalents are available in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Ok</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Absent</td><td>3</td></tr><tr><td>Failed</td><td>4</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of the disk. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.</td></tr>
<tr><td>Disk capacity</td><td>Indicates the capacity of this disk.</td><td>GB</td><td></td></tr>
<tr><td>Disk busy</td><td>Indicates the percentage of disk that is currently in use.</td><td>Percent</td><td>A consistently high value for this measure is a cause of concern as it indicates that the disk is running out of space. Administrators may need to add more space to the disk to maintain optimal utilization of the disk.</td></tr>
<tr><td>Disk read rate</td><td>Indicates the rate at which disk sectors are read from this disk.</td><td>Sectors/sec</td><td rowspan="2">Comparing the value of these measures across the disks helps you in identifying the disk that is busy in terms of disk reads and disk writes.</td></tr>
<tr><td>Disk write rate</td><td>Indicates the rate at which disk sectorers are written to this disk.</td><td>Sectors/sec</td></tr>
<tr><td>Disk read write rate</td><td>Indicates the average rate at which data is read from/written to this disk.</td><td>Kb/sec</td><td></td></tr>
<tr><td>Disk temperature</td><td>Indicates the current temperature of this disk.</td><td>Celsius</td><td>The value of this measure should be within the specified optimal range. A gradual/sudden increase in the value of this measure indicates abnormal condition which when left unattended</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			will drastically affect the performance of the storage system.

3.1.3 NVRAM Test

This test reports the current size of the NVRAM on the Data Domain storage system. In addition, this test reports the number of memory and PCI errors that occurred on the NVRAM.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Data Domain storage system to be 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.

Parameter	Description
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.
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.

Parameter	Description
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
Non volatile RAM size	Indicates the size of the non-volatile RAM in this system.	MB	
Memory errors on NVRAM	Indicates the number of memoru errors that occurred on the NVRAM.	Number	Ideally, the value of this measure should be zero.
PCI errors on NVRAM	Indicates the number of PCI errors that occurred on the NVRAM.	Number	Ideally, the value of this measure should be zero. Any value higher than 0 may lead to the performance degradation of the storage system eventually leading to the crash of the system.

3.1.4 NVRAM Battery Test

This test reports the current status of each battery and the percentage of charge remaining in the battery.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each NVRAM battery of the Data Domain storage system to be 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**.

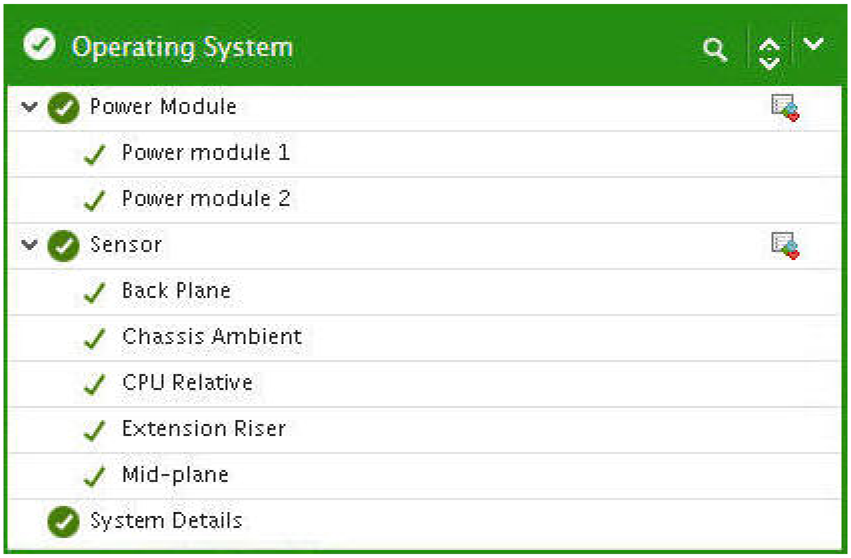
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Battery status	Indicates the current status of this NVRAM battery.	MB	The values reported by this measure and their numeric equivalents are available in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Ok</td><td>0</td></tr><tr><td>Disabled</td><td>1</td></tr><tr><td>Discharged</td><td>2</td></tr><tr><td>Softdisabled</td><td>3</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of the NVRAM battery. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td>Charge remaining</td><td>Indicates the percentage of charge that is currently available in this battery.</td><td>Percent</td><td>A low value for this measure indicates that the battery is currently running out of charge.</td></tr>
</table>

3.2 The Operating System Layer

Using the tests mapped to this layer, administrators can easily determine the current status of the sensors and the power modules in the Data Domain storage system, the CPU utilization of the storage system, the I/O operations performed on the storage system, the data transmitted/received for replication etc.



Operating System

- Power Module
  - Power module 1
  - Power module 2
- Sensor
  - Back Plane
  - Chassis Ambient
  - CPU Relative
  - Extension Riser
  - Mid-plane
- System Details

Figure 3.3: The tests mapped to the Operating System layer

3.2.1 Power Module Test

This test reports the current status of each power module in the Data Domain storage system.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each power module of the Data Domain storage system being 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

Parameter	Description
	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: • **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:

Parameter	Description
	• **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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Power status</td><td>Indicates the current status of this Power module.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Ok</td><td>1</td></tr>
<tr><td>Failed</td><td>2</td></tr>
<tr><td>Fault</td><td>3</td></tr>
<tr><td>Unknown</td><td>99</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of this power module. However, in the graph, this measure is indicated using the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Numeric Values listed in the above table.

3.2.2 Sensor Test

This test reports the current status of the sensors of the Data Domain storage system.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each sensor of the Data Domain storage system being 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.

Parameter	Description
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.
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.

Parameter	Description
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this sensor.</td><td></td><td>The values reported by this measure and their numeric equivalents are available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Absent</td><td>0</td></tr>
<tr><td>Ok</td><td>100</td></tr>
<tr><td>Not found</td><td>2</td></tr>
<tr><td>Overheat warning</td><td>3</td></tr>
<tr><td>Overheat critical</td><td>4</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Value</b>s listed in the table above to indicate the current status of this sensor. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td>Temperature</td><td>Indicates the current temperature of this sensor.</td><td>Celsius</td><td></td></tr>
</table>

3.2.3 System Details Test

This test monitors the CPU, I/O operations on the disks of the storage system and the data transmitted/received for replication in this storage system. Using ths test, administrators can easily detect potential resource contentions.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Data Domain storage system being 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

Parameter	Description
	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.
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

Parameter	Description
	to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

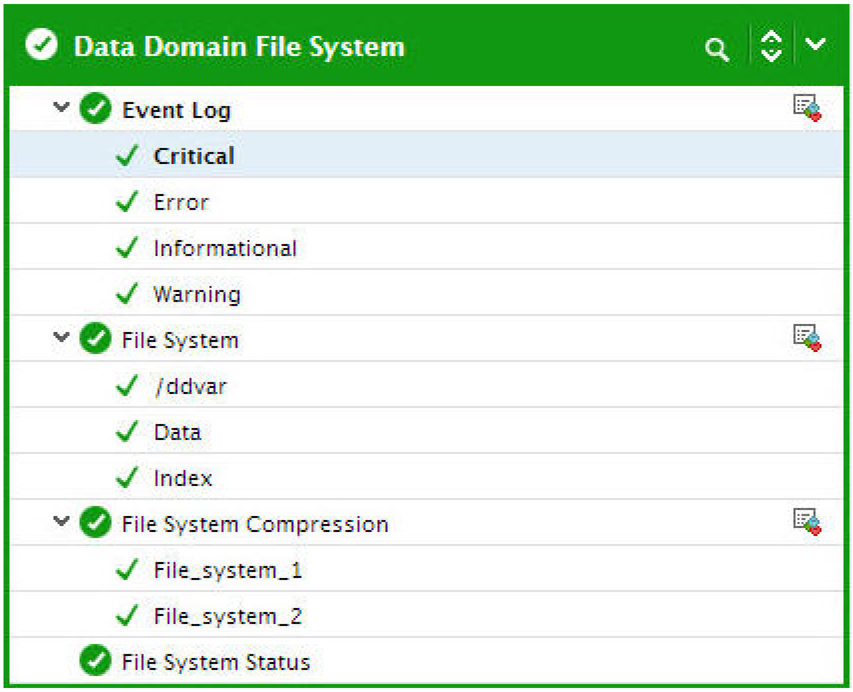
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the percentage of CPU utilized by the Data Domain storage system.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the CPU usage of the system. A consistent increase however could indicate a gradual, yet steady erosion of CPU resources, and is hence a cause for concern.
Disk read rate	Indicates the rate at which data is read from the disks of this storage system.	KB/Sec	
Disk write rate	Indicates the rate at which data is written to the disks of this storage system.	KB/Sec	
Disk busy	Indicates the percentage of time the disks were busy processing requests in this storage system.	Percent	
Non volatile RAM read rate	Indicates the rate at which data is read from the NVRAM of this storage system.	KB/Sec	
Non volatile RAM write rate	Indicates the rate at which data is written to the NVRAM of this storage system.	KB/Sec	
Data transmitted for replication	Indicates the rate at which data is transmitted for replication in this storage system.	KB/Sec	The Data Domain replication option leverages its deduplication capability, thus substantially reducing the amount of backup data that needs to be

Measurement	Description	Measurement Unit	Interpretation
			migrated to a remote site. Replication provides rapid local and remote restores from the storage system. A high value is desired for these measures.
Data received for replication	Indicates the rate at which data is received for replication by this storage system.	KB/Sec	

3.3 The Data Domain File System Layer

This layer helps administrators determine the status of the file systems, the availability, size and utilization of the file systems, the size of each file system prior to and after compression, the event trap messages generated by the storage system etc.



Data Domain File System

- Event Log
  - Critical
  - Error
  - Informational
  - Warning
- File System
  - /ddvar
  - Data
  - Index
- File System Compression
  - File_system_1
  - File_system_2
- File System Status

Figure 3.4: The tests mapped to the Data Domain File System layer

3.3.1 File System Status Test

This test reports the current status of the file system service in the Data Domain storage system.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Data Domain storage system that is to be 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.

Parameter	Description
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.
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
File system status	Indicates the current status of the file system		The values reported by this measure and their numeric equivalents are

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>service in this storage system.</td><td></td><td>available in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Disabled</td><td>0</td></tr>
<tr><td>Enabled</td><td>1</td></tr>
<tr><td>Running</td><td>3</td></tr>
<tr><td>Unknown</td><td>4</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of the file system service. However, in the graph, this measure is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
</table>

3.3.2 File System Test

This test monitors the space utilization of each file available in the Data Domain storage system and reports the administrators of potential space crunch on the files.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each file of the Data Domian storage system that is to be 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.

Parameter	Description
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 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

Parameter	Description
	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
File system size	Indicates the total size allocated to this file.	GB	
Used size	Indicates the space currently utilized by this file.	GB	A value close to the File system size measure indicates that the file is running out of space.
Available size	Indicates the space that is currently available for use in this file.	GB	A high value is desired for this measure.
Size utilization	Indicates the percentage of space that is currently utilized by this file.	Percent	A value close to 100 is a cause of concern.

3.3.3 File System Compression Test

The deduplication process divides the data into variable length blocks and calculates a signature for each block. For each signature, the deduplication process determines if any other identical signature exists, and if not, hardware compresses the unique block and writes it to the data pool. If it finds any matches to these signatures, it replaces that redundant block with a pointer to the unique block so that only one copy of that data block exists on disk.

This test monitors the file systems of the Data domain storage system and reports the size of each file system prior to and after compression. In addition, this test reports the percentage of size reduced due to compression for each file system. Using this test, administrators can easily figure out how well a file system has been deduplicated and to what extent the deduplication was successful by merely analyzing the compression ratio of the file systems prior to and after compression.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Data Domain that is to be 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
Pre compression size	Indicates the size of this file system prior to compression.	GB	
Post compression size	Indicates the size of this file system after compression.	GB	
Reduction percentage	Indicates the percentage of size that was reduced during compression.	Percent	A high value is desired for this measure.

3.3.4 Event Log Test

This test reports the number of events of each type that were generated by the target Data Domain storage system.

Target of the test : A Data Domain storage system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the event of each type that occurred in the Data Domain storage system.

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**.
Exclude Info	Specify a comma separated list of events for which this test should not report metrics. Each event specified in this list box will be listed as a descriptor of this test.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

Parameter	Description
	- The eG manager license should allow the detailed diagnosis capability - 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 events	Indicates the number of events of this type that occurred in this storage system during the last measurement period.	Number	A very low value (zero) indicates that the system is in a healthy state. The detailed diagnosis of this measure if enabled, lists the time of the event, the status of the event and the message generated for the event.

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.