



Monitoring Data Domain

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

©2015 eG Innovations Inc. All rights reserved.

Table of Contents

- MONITORING DATA DOMAIN..... 1
 - 1.1 The Hardware Layer 2
 - 1.1.1 Fan Test..... 2
 - 1.1.2 Disks Test..... 6
 - 1.1.3 NVRAM Test..... 9
 - 1.1.4 NVRAM Battery Test 11
 - 1.2 The Operating System Layer 13
 - 1.2.1 Power Module Test 14
 - 1.2.2 Sensor Test..... 16
 - 1.2.3 System Details Test 19
 - 1.3 The Data Domain File System Layer 23
 - 1.3.1 File System Status Test 23
 - 1.3.2 File System Test 25
 - 1.3.3 File System Compression Test 28
 - 1.3.4 Event Log Test..... 31
- CONCLUSION 34

Monitoring Data Domain

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, enabling longer onsite retention and 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.

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 ratio of each file system etc.

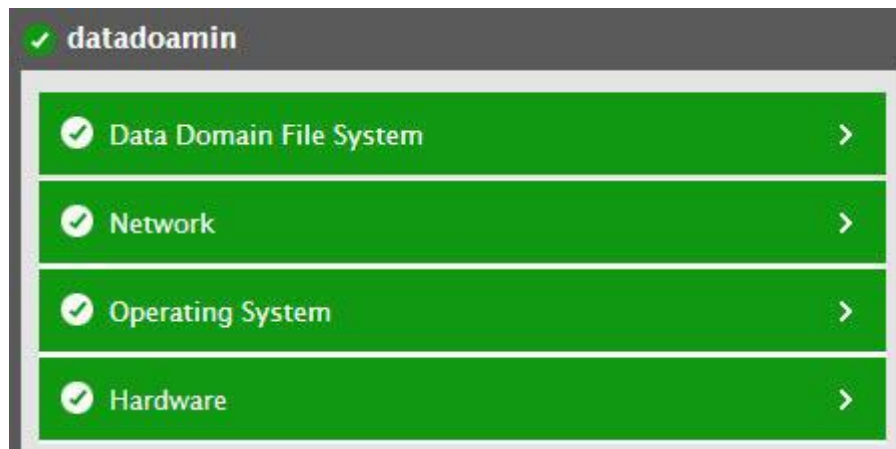


Figure 1: The layer model of a Data Domain

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?

Monitoring Data Domain

- 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 Web Servers document, the sections to come will discuss the remaining layers of Figure 1.

1.1 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 2: The tests mapped to the Hardware layer

1.1.1 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.

Purpose	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
Target of the test	A Data Domain storage system
Agent deploying the test	An external agent

Monitoring Data Domain

Configurable parameters for the test	<ol style="list-style-type: none">1. TEST PERIOD - How often should the test be executed2. HOST – The IP address of the Data Domain3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically)4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.
---	--

	<ol style="list-style-type: none"> 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds. 15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
Outputs of the test	One set of results for each fan in the Data Domain storage system to be monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation										
	Fan status: Indicates the current status of this fan.		<p>The values reported by this measure and their numeric equivalents are available in the table below:</p> <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> <p>Note:</p> <p>This measure reports the Measure Values listed in the table above to indicate the current status of the fan. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.</p>	Measure Value	Numeric Value	Not found	0	OK	1	Fail	2		
Measure Value	Numeric Value												
Not found	0												
OK	1												
Fail	2												
	Fan running level: Indicates the current status of this fan’s speed.		<p>The values reported by this measure and their numeric equivalents are available in the table below:</p> <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> <p>Note:</p> <p>This measure reports the Measure Values 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.</p>	Measure Value	Numeric Value	Unknown	0	Low	1	Normal	100	High	2
Measure Value	Numeric Value												
Unknown	0												
Low	1												
Normal	100												
High	2												

1.1.2 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.

Purpose	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
Target of the test	A Data Domain storage system
Agent deploying the test	An external agent
Configurable parameters for the test	<ol style="list-style-type: none">1. TEST PERIOD - How often should the test be executed2. HOST – The IP address of the Data Domain3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically)4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.

	<p>6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter.</p> <p>7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3.</p> <p>8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here.</p> <p>9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:</p> <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm <p>10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option.</p> <p>11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:</p> <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard <p>12. ENCRYPTPASSWORD – Specify the encryption password here.</p> <p>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.</p> <p>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.</p> <p>15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</p>
Outputs of the test	One set of results for each disk of the Data Domain storage system to be monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation										
	Disk status: Indicates the current status of this disk.		<p>The values reported by this measure and their numeric equivalents are available in the table below:</p> <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> <p>Note: This measure reports the Measure Values 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.</p>	Measure Value	Numeric Value	Ok	1	Unknown	2	Absent	3	Failed	4
Measure Value	Numeric Value												
Ok	1												
Unknown	2												
Absent	3												
Failed	4												
	Disk capacity: Indicates the capacity of this disk.	GB											
	Disk busy: Indicates the percentage of disk that is currently in use.	Percent	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.										
	Disk read rate: Indicates the rate at which disk sectors are read from this disk.	Sectors/sec	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.										
	Disk write rate: Indicates the rate at which disk sectorers are written to this disk.	Sectors/sec											

Monitoring Data Domain

	Disk read write rate: Indicates the average rate at which data is read from/written to this disk.	Kb/sec	
	Disk temperature: Indicates the current temperature of this disk.	Celcius	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 will drastically affect the performance of the storage system.

1.1.3 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.

Purpose	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
Configurable parameters for the test	<ol style="list-style-type: none">1. TEST PERIOD - How often should the test be executed2. HOST – The IP address of the Data Domain3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically)4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.

	<ol style="list-style-type: none"> 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds. 15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
Outputs of the test	One set of results for the Data Domain storage system to be monitored

Measurements made by the test	Measurement	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 memory 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.

1.1.4 NVRAM Battery Test

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

Purpose	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
Configurable parameters for the test	<ol style="list-style-type: none"> 1. TEST PERIOD - How often should the test be executed 2. HOST – The IP address of the Data Domain 3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically) 4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list. 5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.

	<p>6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter.</p> <p>7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3.</p> <p>8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here.</p> <p>9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:</p> <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm <p>10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option.</p> <p>11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types:</p> <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard <p>12. ENCRYPTPASSWORD – Specify the encryption password here.</p> <p>13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.</p> <p>14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.</p> <p>15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</p>
Outputs of the test	One set of results for each NVRAM battery of the Data Domain storage system to be monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation										
	Battery status: Indicates the current status of this NVRAM battery.	MB	<p>The values reported by this measure and their numeric equivalents are available in the table below:</p> <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> <p>Note:</p> <p>This measure reports the Measure Values listed in the table above to indicate the current status of the NVRAM battery. However, in the graph, this measure is indicated using the Numeric Values listed in the above table.</p>	Measure Value	Numeric Value	Ok	0	Disabled	1	Discharged	2	Softdisabled	3
Measure Value	Numeric Value												
Ok	0												
Disabled	1												
Discharged	2												
Softdisabled	3												
	Charge remaining: Indicates the percentage of charge that is currently available in this battery.	Percent	A low value for this measure indicates that the battery is currently running out of charge.										

1.2 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.



Figure 3: The tests mapped to the Operating System layer

1.2.1 Power Module Test

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

Purpose	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
Configurable parameters for the test	<ol style="list-style-type: none"> 1. TEST PERIOD - How often should the test be executed 2. HOST – The IP address of the Data Domain 3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically) 4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list. 5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.

	<ol style="list-style-type: none"> 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds. 15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
Outputs of the test	One set of results for each power module of the Data Domain storage system being monitored

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

1.2.2 Sensor Test

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

Purpose	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

Monitoring Data Domain

Configurable parameters for the test	<ol style="list-style-type: none">1. TEST PERIOD - How often should the test be executed2. HOST – The IP address of the Data Domain3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically)4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.
---	--

	<ol style="list-style-type: none"> 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds. 15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
Outputs of the test	One set of results for each sensor of the Data Domain storage system being monitored

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

1.2.3 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 this test, administrators can easily detect potential resource contentions.

Purpose	Reports critical statistics indicating the level of performance and overall health of the UPS battery along with the current status of the battery
Target of the test	A Data Domain storage system
Agent deploying the test	An external agent

Monitoring Data Domain

Configurable parameters for the test	<ol style="list-style-type: none">1. TEST PERIOD - How often should the test be executed2. HOST – The IP address of the Data Domain3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically)4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list.5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear.
---	--

	<ol style="list-style-type: none"> 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the SNMPVERSION. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the ENCRYPTFLAG is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds. 15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
Outputs of the test	One set of results for the Data Domain storage system being monitored

Measurements made by the test	Measurement	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 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	

1.3 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 sytem etc.

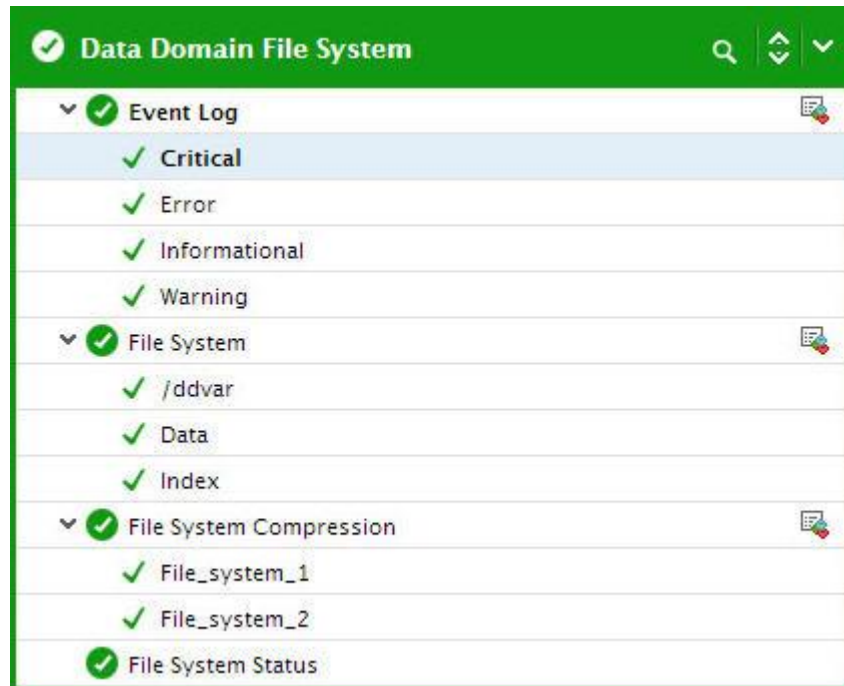


Figure 4: The tests mapped to the Data Domain File System layer

1.3.1 File System Status Test

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

Purpose	Monitors the current status of the file system service in the Data Domain storage sytem
Target of the test	A Data Domain storage system
Agent deploying the test	An external agent

Configurable parameters for the test	<ol style="list-style-type: none"> 1. TEST PERIOD - How often should the test be executed 2. HOST – The IP address of the Data Domain 3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically) 4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list. 5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear. 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the encryptflag is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
--------------------------------------	---

	15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes . By default, this flag is set to No .											
Outputs of the test	One set of results for the Data Domain storage system that is to be monitored											
Measurements made by the test	Measurement	Measurement Unit	Interpretation									
	File system status: Indicates the current status of the file system service in this storage system.		<p>The values reported by this measure and their numeric equivalents are available in the table below:</p> <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> <p>Note:</p> <p>This measure reports the Measure Values 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 Numeric Values listed in the above table.</p>	Measure Value	Numeric Value	Disabled	0	Enabled	1	Running	3	Unknown
Measure Value	Numeric Value											
Disabled	0											
Enabled	1											
Running	3											
Unknown	4											

1.3.2 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.

Purpose	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

Monitoring Data Domain

Agent deploying the test	An external agent
--------------------------------	-------------------

Configurable parameters for the test	<ol style="list-style-type: none"> 1. TEST PERIOD - How often should the test be executed 2. HOST – The IP address of the Data Domain 3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically) 4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list. 5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear. 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the encryptflag is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
--------------------------------------	---

	15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes . By default, this flag is set to No .		
Outputs of the test	One set of results for each file of the Data Domain storage system that is to be monitored		
Measurements made by the test	Measurement	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 <i>File system size</i> 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.

1.3.3 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.

Purpose	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 that is compressed for each file system
Target of the test	A Data Domain

Monitoring Data Domain

Agent deploying the test	An external agent
--------------------------------	-------------------

Configurable parameters for the test	<ol style="list-style-type: none"> 1. TEST PERIOD - How often should the test be executed 2. HOST – The IP address of the Data Domain 3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically) 4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list. 5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear. 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the encryptflag is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
--------------------------------------	---

Monitoring Data Domain

	15. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes . By default, this flag is set to No .		
Outputs of the test	One set of results for the Data Domain that is to be monitored		
Measurements made by the test	Measurement	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.

1.3.4 Event Log Test

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

Purpose	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

Configurable parameters for the test	<ol style="list-style-type: none"> 1. TEST PERIOD - How often should the test be executed 2. HOST – The IP address of the Data Domain 3. SNMPPORT – The SNMP Port number of the Data Domain (161 typically) 4. SNMPVERSION – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVERSION list is v1. However, if a different SNMP framework is in use in your environment, say SNMP v2 or v3, then select the corresponding option from this list. 5. SNMPCOMMUNITY – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP v1 and v2 only. Therefore, if the SNMPVERSION chosen is v3, then this parameter will not appear. 6. USERNAME – This parameter appears only when v3 is selected as the SNMPVERSION. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the USERNAME parameter. 7. AUTHPASS – Specify the password that corresponds to the above-mentioned USERNAME. This parameter once again appears only if the snmpversion selected is v3. 8. CONFIRM PASSWORD – Confirm the AUTHPASS by retyping it here. 9. AUTHTYPE – This parameter too appears only if v3 is selected as the SNMPVERSION. From the AUTHTYPE list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: <ul style="list-style-type: none"> ➤ MD5 – Message Digest Algorithm ➤ SHA – Secure Hash Algorithm 10. ENCRYPTFLAG – This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option. 11. ENCRYPTTYPE – If the encryptflag is set to YES, then you will have to mention the encryption type by selecting an option from the ENCRYPTTYPE list. SNMP v3 supports the following encryption types: <ul style="list-style-type: none"> ➤ DES – Data Encryption Standard ➤ AES – Advanced Encryption Standard 12. ENCRYPTPASSWORD – Specify the encryption password here. 13. CONFIRM PASSWORD – Confirm the encryption password by retyping it here. 14. INCLUDE INFO – Specify a comma separated list of events for which this test should report metrics. Each event specified in this list box will be listed as a descriptor of this test. 15. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
--------------------------------------	---

Monitoring Data Domain

	<p>16. 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 Data Domain over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</p>		
Outputs of the test	One set of results for the event of each type that occurred in the Data Domain storage system		
Measurements made by the test	Measurement	Measurement Unit	Interpretation
	<p>Number of events:</p> <p>Indicates the number of events of this type that occurred in this storage system during the last measurement period.</p>	Number	<p>A very low value (zero) indicates that the system is in a healthy state.</p> <p>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.</p>

Conclusion

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

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