Monitoring Dell Compellent

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 DELL COMPELLENT STORAGE CENTER 1

1.1 How does eG Enterprise Monitor a Dell Compellent Storage Center? 1

1.1.1 Configuring the Dell Compellent SMI-S Provider using a Local User Account (v5.5.4 and above) 2

1.1.2 Configuring the Dell Compellent SMI-S Provider using a Local Service Account (v5.5.4 and above) 9

1.2 The Dell Compellent Disk Layer 11

1.2.1 Dell Compellent Disks Test 11

1.3 The Dell Compellent System Layer 18

1.3.1 Dell Compellent Arrays Test 18

1.3.2 Dell Compellent Controllers Test 24

1.3.3 Dell Compellent Ports Test 30

1.4 The Dell Compellent Service Layer 35

1.4.1 Dell Compellent LUNs Test 35

CONCLUSION 43

1

Monitoring Dell Compellent Storage Center

The Dell Compellent Storage Center is an enterprise class storage area network (SAN) that significantly lowers capital expenditures, reduces storage management and administration time, provides continuous data availability and enables storage virtualization. Storage Center's industry-standard hardware and sophisticated software manage data at the block-level, maximizing utilization, automating tiered storage, simplifying replication and speeding data recovery.

eG Enterprise provides a specialized Dell Compellent Storage Center monitoring model (see Figure 1) to monitor the overall health and current stateof the disks, LUNs, arrays and controllers and analyze how well the Storage Center balances I/O load across the disks, LUNs etc.

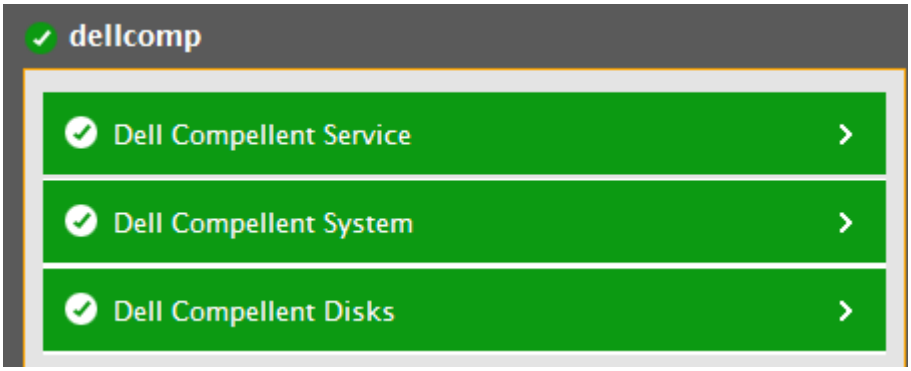

Figure 1: The layer model of a Dell Compellent Storage Center

Every layer of Figure 1 is mapped to a variety of tests which connect to the SMI-S Provider of the Dell Compellent Storage Center to collect critical statistics pertaining to its performance.

1.1 How does eG Enterprise Monitor a Dell Compellent Storage Center?

Storage Management Initiative Specification (SMI-S) is a standard interface specification developed by the Storage Networking Industry Association (SNIA). Based on the Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) standards, SMI-S defines common protocols and data models that enable interoperability between storage vendor software and hardware.

The Dell Compellent SMI-S Provider version 1.4 works with the open source OpenPegasus CIM Server, which is included with the Enterprise Manager Data Collector. SMI-S can be configured during initial Data Collector installation or post-installation by modifying the properties of the Enterprise Manager Data Collector. When SMI-S is enabled and configured, the Data Collector automatically installs and manages the Dell Compellent SMI-S Provider and the OpenPegasus CIM Server; no additional installation is required.

The Dell Compellent SMI-S Provider is set up via the **Properties** section of the **Compellent Enterprise Data Collector**

Manager. Once the Dell Compellent is configured, the eG agent will poll the **SMI-S Provider of the Dell Compellent** Storage Center at set intervals and collect the required performance metrics. Since the SMI-S Provider is embedded within the Dell Compellent Storage System, eG Enterprise Suite uses a **remote** agent to monitor the Dell Compellent Storage Center.

SMI-S can be set up during the Data Collector installation or at a latertime. Configuring the Dell Compellent SMI-S Provider consists of setting the following Data Collector Service properties:

- Selecting the **Service User Type** for the Data Collector Service. You can either choose the **Local User Account** or the **Local Service Account**.
- Manually/automatically creating the Pegasus Users according to the chosen **Service User Type**. If you choose the **Local User Account**, then the user type should possess *admin* privileges and should allow the Data Collector to automatically add a Pegasus CIM User. If you choose **Local Service Account** from this list, then you will be required to manually add atleast one Pegasus user to the Pegasus CIM Server.
- Enabling SMI-S properties including SLP/HTTP services, and selecting to manually/automatically manage the Pegasus users.

1.1.1 Configuring the Dell Compellent SMI-S Provider using a Local User Account (v5.5.4 and above)

To configure the Dell Compellent SMI-S Provider using a **Local User Account**, follow the steps as discussed below:

1. Login to the Windows server on which the the Dell Compellent Data Collector Manager is installed.
2. Create a local user on the server. The maximum length of the username and password should be 8 characters. **Note that the specified password should be Alpha-numeric. No special characters are allowed while specifying the user name.**
3. Add the local user to the **Administrators** group by following the steps mentioned below:
   - Select the **Groups** option from the **Local User and Groups** subnode of the **Server Manager** node. A context sensitive **Groups** section will appear in the right panel.
   - Clicking the **Administrators** group will invoke the **Administrators Properties** pop up window (see Figure 2)
   - The user that you have created will be listed in the **Members** section as shown in Figure 2.
   - Select the user and click the **Add** button to add the user to the **Administrators** group.

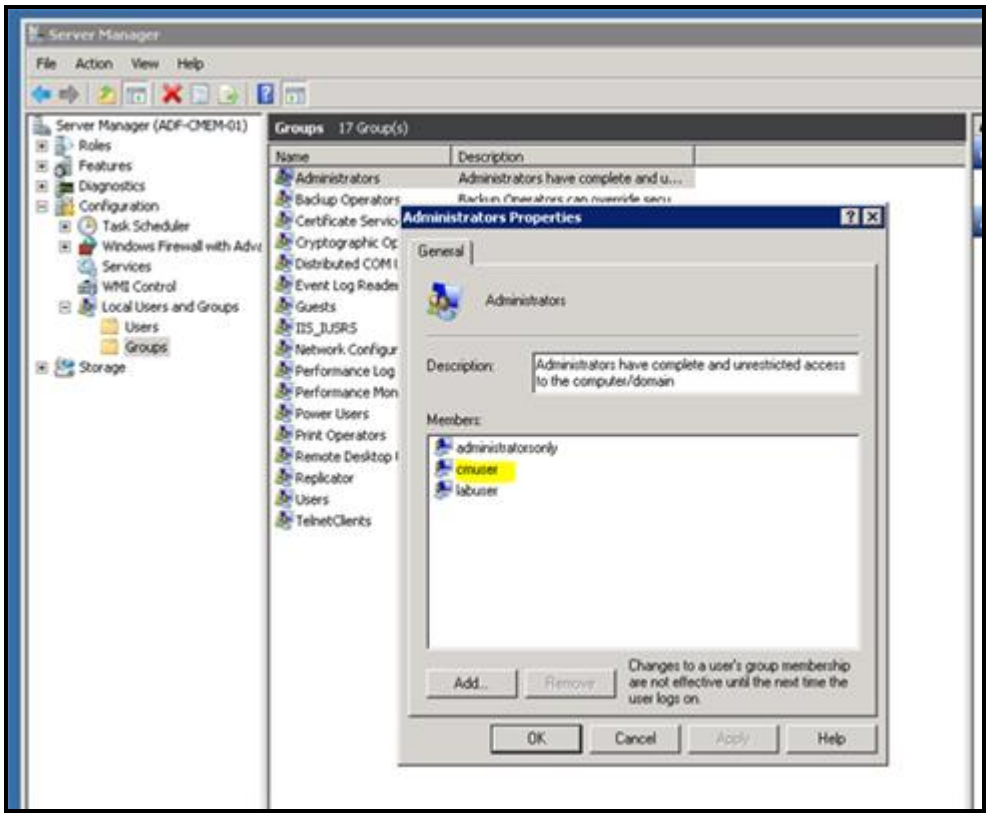

Figure 2: Adding the created local user to the Administrators group

4. Then, you will be required to associate this user to the **Logon as a Service** policy. To assoicate this user to the policy, do the following:

   - Follow the menu sequence in the Windows server: *Start -> All Programs -> Administrative Tools -> Local Policies -> User Rights Assignment*
   - A list of policies will then appear in the context sensitive right panel. Clicking the **Logon as a Service** policy will invoke the **Logon as a service Properties** window (See Figure 3).
   - Select the local user that you have created and click the **Add User or Group** button. Finally, clicking the **OK** button will register the necessary changes.

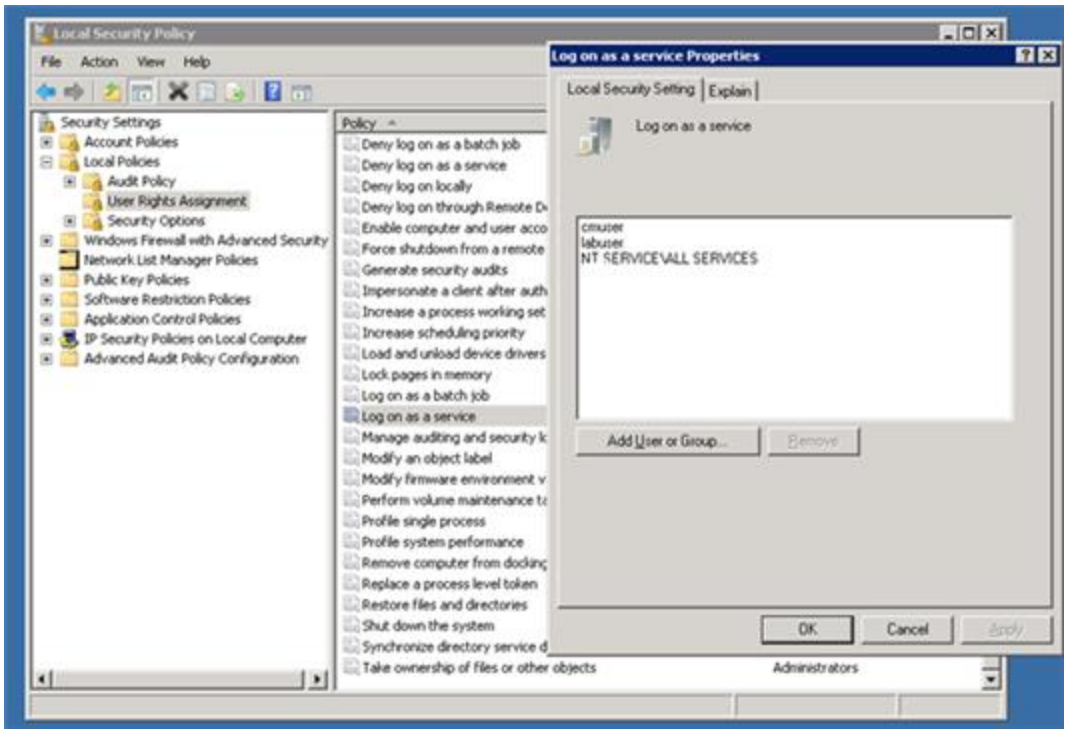

Figure 3: Associating the user to the Logon as a service policy

For the changes made in Step 3 and Step 4 to be effective, logoff and login to the Windows server with the credentials of the created local user.

5. Once you have provided the necessary privileges to the created local user, you will be required to add the same user to the Compellent Enterprise Manager.

6. If you have used the open security policy, then you can add the user through the Enterprise Manager Client Application. If you have used the Advanced security policy, then you can add the user from the Data Collector Manager Interface. Since we have used the open security policy, the user is added through the Enterprise Manager Client Application (see Figure 4).

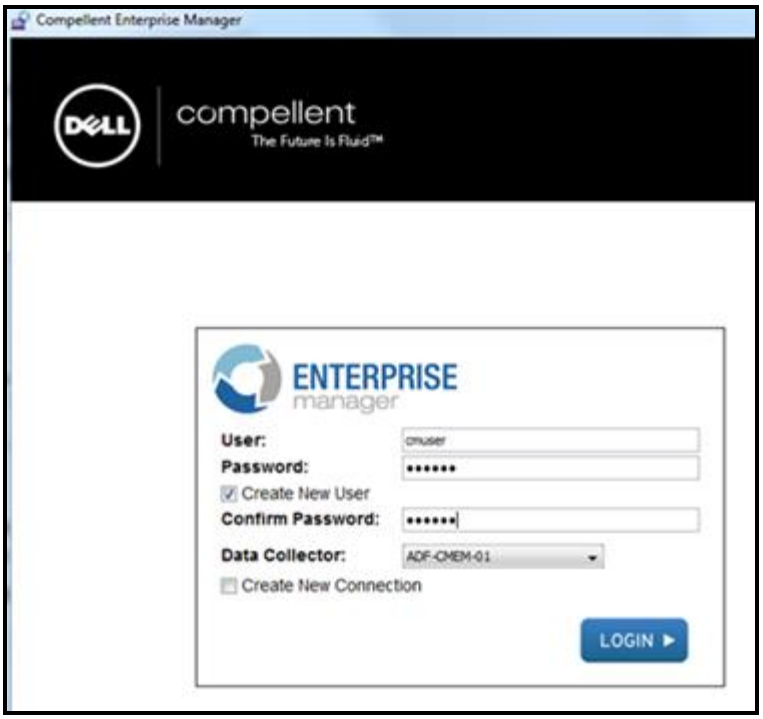

Figure 4: Adding a new user through the Compellent Enterprise Manager Client Application

7. Select the **Create New User** check box (see Figure 4) and then specify the **User** which is the same as the local user that you have created on the Windows server.

8. Specify the **Password** and then click the **LOGIN** button. **The password need not be the same as that of the password of the local user.**

9. Next, add the target Dell Compellent Storage Center that is to be monitored by clicking the **Add Storage Center** option that appears upon clicking the **Management** menu (see Figure 5):

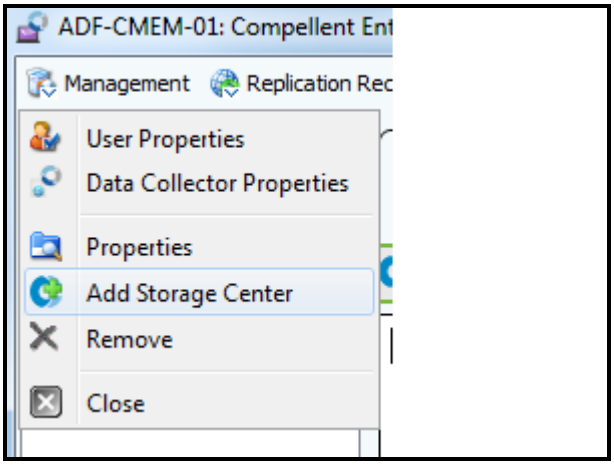

Figure 5: Navigating through the Management menu

10. In Figure 6 that appears, specify the following:

Figure 6: Specifying the credentials of the target Dell Compellent Storage Center

- Host Name – Specify the IP address of the target Dell Compellent Storage Center
- User Name – Specify the name of the user who is authorized to access the target Storage Center
- Password - Specify the password that corresponds to the specified User Name.

Note

If the user has been successfully added, then you can view the user when you click the **User Viewer** that appears upon clicking the **Properties** button of the **Compellent Enterprise Manager Data Collector**.

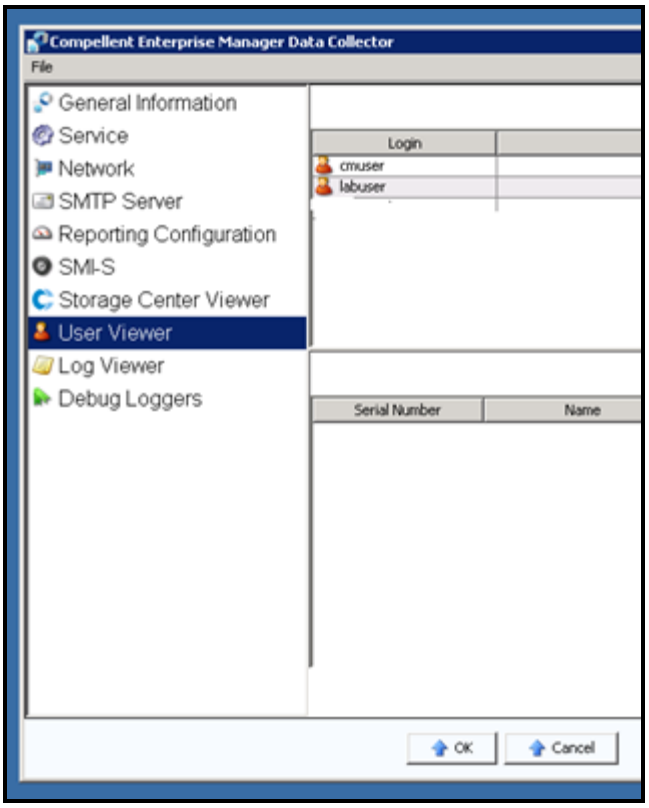

Figure 7: Viewing the created user by clicking the User Viewer node

11. Once you have created the Compellent Enterprise Manager User, you will be required to provide the necessary **Data Collector Service Properties** by following the menu sequence: *Start -> All Programs -> Compellent Technologies -> Compellent Enterprise Manager -> Compellent Enterprise Data Collection Manager -> Service.* Figure 8 will then appear.

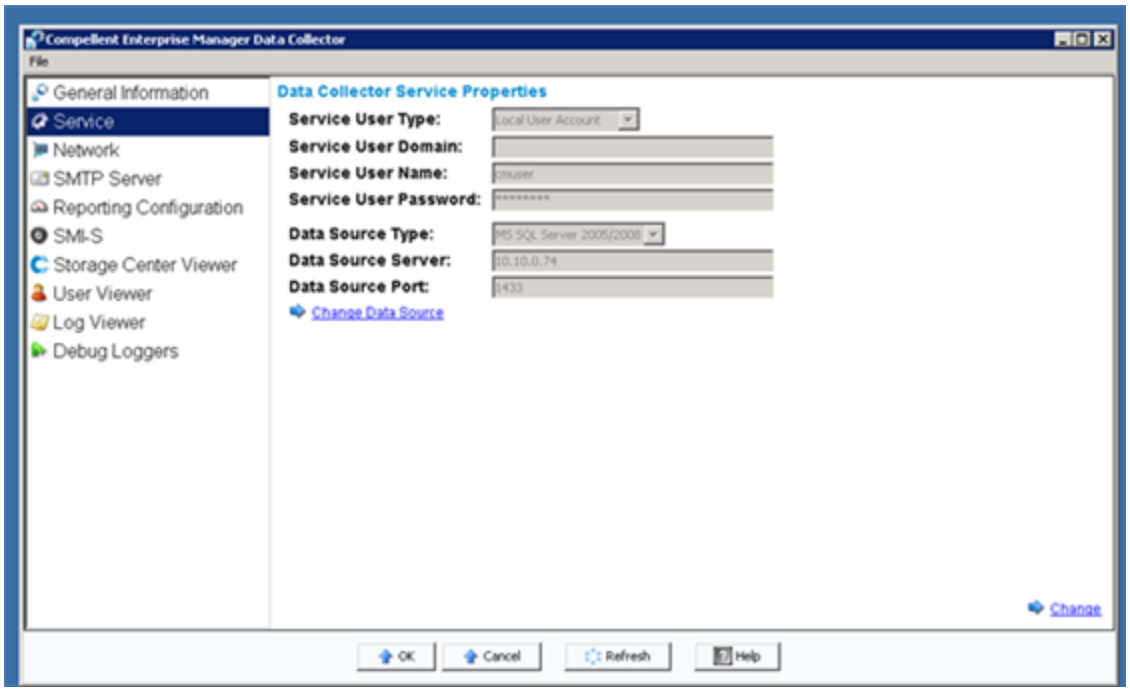

Figure 8: Specifying the Data Collector Service Properties

12. Clicking the **Change** link in Figure 8 will enable you to edit the properties of the **Data Collector Service**. Now, choose **Local User Account** from the **Service User Type** drop down list.

13. Then, in the **Service User Name** and **Service User Password** text boxes, specify the credentials of the local user that you have created in Step 2.

14. Finally, you will be required to enable the SMI-S Server properties as shown in Figure 9 . Clicking the **Change** link in Figure 9 will enable you to make the following changes to the **SMI-S Server Configuration**:

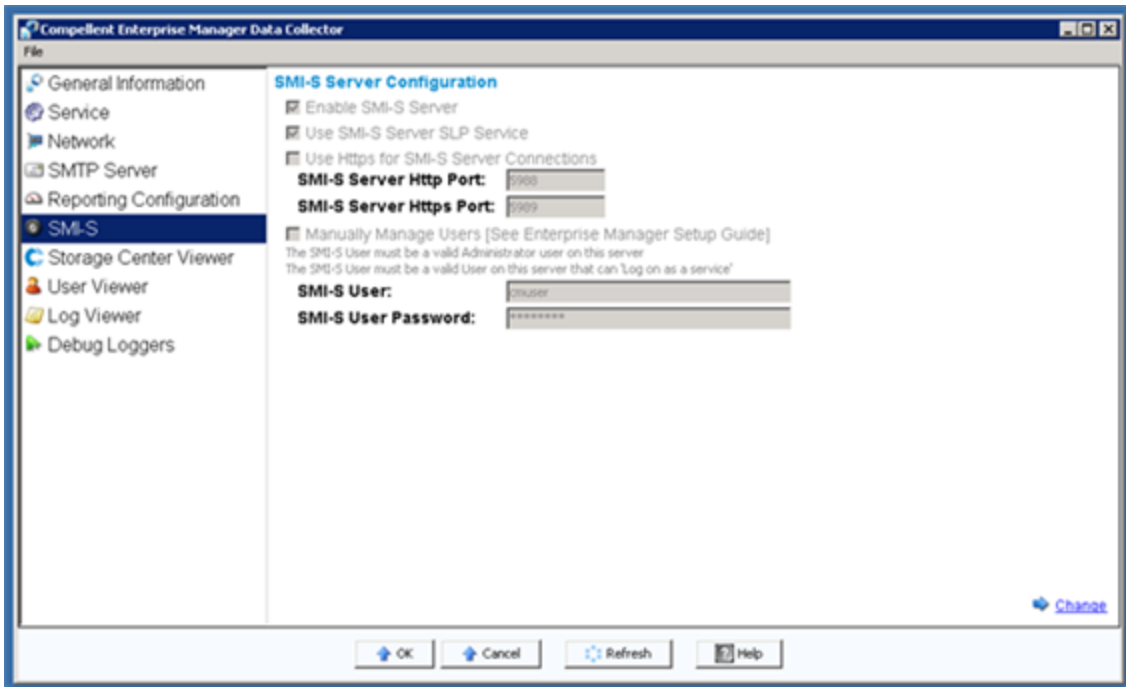

Figure 9: Enabling the SMI-S Server properties

- Select the checkbox that appears before the **Enable SMI-S Server** option.
- Uncheck the **Use Https for SMI-S Server Connections** option.
- Uncheck the **Manually Manage Users** option and then provide the credentials of the Enterprise Manager user that you have created in the **SMI-S User** and **SMI-S User Password** text boxes.
- Finally, clicking the **Apply Changes** link will apply the changes that you have made in the **SMI-S Server Configuration** section.

15. Now, you can proceed to configure the tests that pertain to the Dell Compellent Storage Center.

1.1.2 Configuring the Dell Compellent SMI-S Provider using a Local Service Account (v5.5.4 and above)

To configure the Dell Compellent SMI-S Provider using a **Local Service Account**, follow the Step 1 through Step 12 mentioned in Section 1.1.1 and proceed with the following steps:

1. Clicking the **Change** link in Figure 8 will enable you to edit the properties of the **Data Collector Service**. Now, set the **Service User Type** to **Local Service Account**.
2. If the **Service User Name** and **Service User Password** text boxes are populated, you will be required to clear those text boxes. Then, clicking the **Apply Changes** link will help you update the changes as per your selection.
3. Finally, you will be required to enable the SMI-S server properties as shown in Figure 10 . Clicking the **Change** link in Figure 10 will enable you to make the following changes to the SMI-S Server Configuration:

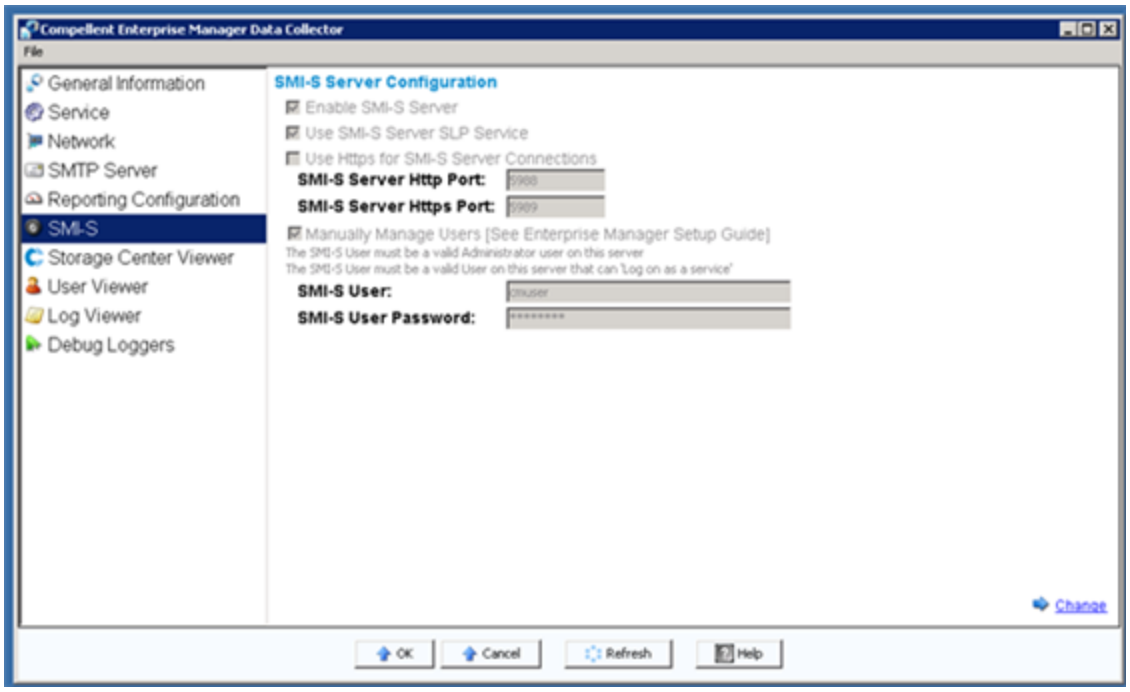

Figure 10: Enabling the SMI-S Server properties for a Local Service Account Service User Type

- Select the check box that appears before the **Enable SMI-S Server** option.
- Uncheck the **Use Https for SMI-S Server Connections** option.
- Select the check box that appears before the **Manually Manage Users** option.
- Finally, clicking the **Apply Changes** link will apply the changes that you have made in the **SMI-S Server Configuration** section.

4. Now, you will be required to add the SMI-S user through the Command Line Interface of the Dell Compellent Storage Center as discussed in Section 1.1.2.1.

1.1.2.1 Adding the SMI-S User from CLI

To add the SMI-S User from the Command Line Interface, do the following:

1. Open a Command prompt in the Dell Compellent Storage Center.
2. Change the directory of the Storage Center to <Dell_Compellent_install_Dir>\Compellent Enterprise Manager\msaservice\Pegasus\bin.
3. Then you will be required to execute the following command:

   ```
   cimuser.exe –a <Username> -w <password>
   ```

   where,

   username is the name of the Enterprise Manager user

   password is the password that corresponds to the Enterprise Manager user
4. If you have chosen to check the Use Https for SMI-S Server Connections check box, then you have to run the following command too:

   ```
   cimtrust.exe
   ```

   By running the command, you can add the Pegasus user to the list of trusted users.

5. Restarting the Data Collector Manager Service will add the SMI-S user to the SMI-S Provider.
6. Now, you can proceed to configure the tests that pertain to the Dell Compellent Storage Center.

The sections discussed below helps you to analyze each and every layer of the Dell Compellent Storage Center.

1.2 The Dell Compellent Disk Layer

This layer monitors the disks of the Dell Compellent Storage Center and reports how healthy each disk is and how well the Storage Center balances I/O load across disks.

Figure 11: The tests mapped to the Dell Compellent Disk layer

1.2.1 Dell Compellent Disks Test

This test monitors the current state, overall health, and the load-balancing capability of each disk in the Storage Center. With the help of this test, administrators can not only identify failed disks, but can also predict the potential failure of a disk, so that efforts can be undertaken to avert the same. In addition, the test also points administrators to disks that are handling more I/O requests than the rest, thus shedding light on irregularities in the distribution of I/O load across disks and prompting administrators to fine-tune the load-balancing algorithm. In addition, the test also proactively alerts administrators to probable slowdowns in I/O processing by specific disks, thereby enabling administrators to initiate pre-emptive actions.

Purpose	Monitors the current state, overall health, and the load-balancing capability of each disk in the Dell Compellent Storage Center
Target of the test	A Dell Compellent Storage Center
Agent deploying the test	A remote agent

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The IP address of the storage device
3. PORT - The port number at which the storage device listens. The default is NULL.
4. USER and PASSWORD – Specify the credentials of a user who has the right to execute API commands on the Dell Compellent Storage Center and pull out metrics. The specified user should possess Administator privileges and should be associated with the Logon as a Service policy.
5. CONFIRM PASSWORD – Confirm the PASSWORD by retyping it here.
6. SSL – Set this flag to Yes, if the storage device being monitored is SSL-enabled.
7. CIM SERVER PORT - The SMI–S provider of the Dell Compellent Storage Center provides access for monitoring and management via the HTTP and HTTPS protocols for CIM API request/response semantics. To enable the eG agent to access the SMI-S Provider, invoke the CIM API commands, and collect the required metrics, you need to specify the service port on the SMI- S provider in the CIM SERVER PORT text box that listens for HTTP/HTTPS requests for CIM API semantics. By default, this is port 5988. If the service port on the SMI-S Provider listens only to HTTPS requests, then specify the port as 5989.
8. ISEMBEDDED – If this flag is set to True, it indicates that the SMI-S Provider is embedded on the Storage Center. On the other hand, if this flag is set to False, it indicates that the SMI-S Provider has been implemented as a proxy.
9. SERIALNUMBER – If the SMI-S Provider has been implemented as a proxy, then such a provider can be configured to manage multiple Storage Centers. This is why, if the ISEMBEDDED flag is set to False, you will have to explicitly specify which Storage Center you want the eG agent to monitor. Since each Storage Center is uniquely identified by a serial number, specify the same in the SERIALNUMBER text box.
10. DETAILED DIAGNOSIS – To make diagnosis more efficient and accurate, the eG Enterprise system 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 against DETAILED DIAGNOSIS. 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:
➢ 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each disk on the Dell Compellent Storage Center</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td>test</td>
<td>Health state:
Indicates how healthy this disk currently is.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>Unknown</td></tr>
<tr><td>2</td><td>Degraded/Warning</td></tr>
<tr><td>3</td><td>Minor failure</td></tr>
<tr><td>4</td><td>Major failure</td></tr>
<tr><td>5</td><td>Critical failure</td></tr>
<tr><td>6</td><td>Non-recoverable error</td></tr>
</table>

By default, this measure reports the Measure Values discussed above to indicate the state of a disk. In the graph of this measure however, states are represented using the numeric equivalents only.

The detailed diagnosis of this measure if enabled, lists the capacity of the disk.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Operational status:
Indicates the current operational state of this disk.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>In Service</td></tr>
<tr><td>2</td><td>Power Mode</td></tr>
<tr><td>3</td><td>Completed</td></tr>
<tr><td>4</td><td>Starting</td></tr>
<tr><td>5</td><td>Dormant</td></tr>
<tr><td>6</td><td>Other</td></tr>
<tr><td>7</td><td>Unknown</td></tr>
<tr><td>8</td><td>Stopping</td></tr>
<tr><td>9</td><td>Stressed</td></tr>
<tr><td>10</td><td>Stopped</td></tr>
<tr><td>11</td><td>Supporting Entity in Error</td></tr>
<tr><td>12</td><td>Degraded or Predicted Failure</td></tr>
<tr><td>13</td><td>Predictive Failure</td></tr>
<tr><td>14</td><td>Lost Communication</td></tr>
<tr><td>15</td><td>No Contact</td></tr>
<tr><td>16</td><td>Aborted</td></tr>
<tr><td>17</td><td>Error</td></tr>
<tr><td>18</td><td>Non-Recoverable Error</td></tr>
</table>
</td>
</tr>
</table>

			Note By default, this measure reports the **Measure Values** discussed above to indicate the operational state of a disk. In the graph of this measure however, operational states are represented using the numeric equivalents only.

<table>
<tr>
<td></td>
<td>Detailed operational status:
Describes the current operational state of this disk.</td>
<td></td>
<td>Typically, the detailed state will describe why the disk is in a particular operational state. For instance, if the Operational status measure reports the value Stopping for a disk, then this measure will explain why that disk is being stopped.

The values that this measure can report and their corresponding numeric values are discussed in the table below:

<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>Online</td></tr>
<tr><td>1</td><td>Success</td></tr>
<tr><td>2</td><td>Power Saving Mode</td></tr>
<tr><td>3</td><td>Write Protected</td></tr>
<tr><td>4</td><td>Write Disabled</td></tr>
<tr><td>5</td><td>Not Ready</td></tr>
<tr><td>6</td><td>Removed</td></tr>
<tr><td>7</td><td>Rebooting</td></tr>
<tr><td>8</td><td>Offline</td></tr>
<tr><td>9</td><td>Failure</td></tr>
</table>

Note

By default, this measure reports the Measure Values discussed above to indicate the detailed operational state of a disk. In the graph of this measure however, detailed operational states are represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Data transmitted:
Indicates the rate at which data was transmitted by this disk.</td>
<td>MB/Sec</td>
<td></td>
</tr>
</table>

	IOPS: Indicates the rate at which I/O operations were performed on this disk.	IOPS	Compare the value of this measure across disks to know which disk handled the maximum number of I/O requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across disks. You may then want to take a look at the *Reads* and *Writes* measure to understand what to fine-tune – the load-balancing algorithm for read requests or that of the write requests.
	Reads: Indicates the rate at which read operations were performed on this disk.	Reads/Sec	Compare the value of this measure across disks to know which disk handled the maximum number of read requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across disks.
	Writes: Indicates the rate at which write operations were performed on this disk.	Writes/Sec	Compare the value of this measure across disks to know which disk handled the maximum number of write requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across disks.
	Data reads: Indicates the rate at which data is read from this disk.	MB/Sec	Compare the value of these measures across disks to identify the slowest disk in terms of servicing read and write requests (respectively).
	Data writes: Indicates the rate at which data is written to this disk.	MB/Sec	
	Disk busy: Indicates the percentage of time this disk was busy processing requests.	Percent	Compare the value of this measure across disks to know which disk was the busiest and which disk was not. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across disks.
	Average read size: Indicates the amount of data read from this disk per I/O operation	MB/Op	Compare the value of these measures across disks to identify the slowest disk in terms of servicing read and write requests (respectively).
	Average write size: Indicates the amount of data written to this disk per I/O operation.	MB/Op	

	Read hits: Indicates the percentage of read requests that were serviced by the cache of this disk.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct disk accesses, which are expensive operations, are high.
	Write hits: Indicates the percentage of write requests that were serviced by the cache of this disk.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct disk accesses, which are expensive operations, are high.
	Average response time: Indicates the time taken by this disk to respond to I/O requests.	Microsecs	Ideally, this value should be low. If not, it implies that the disk is slow.
	Queue depth: Indicates the number of requests that are in queue for this disk.	Number	A consistent increase in this value indicates a potential processing bottleneck with the disk.

1.3 The Dell Compellent System Layer

Using the test mapped to this layer, administrators can monitor the overall health, operational state, and I/O activity on the arrays, controllers and the I/O load on the ports.

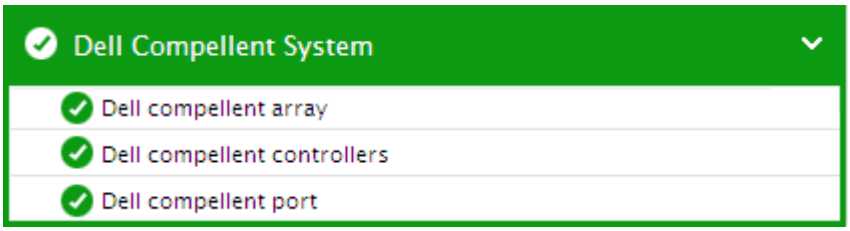

Figure 12: The tests mapped to the Dell Compellent System layer

1.3.1 Dell Compellent Arrays Test

This test monitors the current state, overall health, and the load-balancing capability of each storage array in the Dell Compellent Storage Center. With the help of this test, administrators can be proactively alerted to potential array failures / slowdowns / overload conditions. This way, irregularities in the distribution of I/O load across arrays comes to light, prompting administrators to fine-tune the load-balancing algorithm.

Purpose	Monitors the current state, overall health, and the load-balancing capability of each storage array in the Dell Compellent Storage Center
Target of the test	A Dell Compellent Storage Center
Agent deploying the	A remote agent

test	
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The IP address of the storage device 3. **PORT** - The port number at which the storage device listens. The default is NULL. 4. **USER** and **PASSWORD** – Specify the credentials of a user who has the right to execute API commands on the Dell Compellent Storage Center and pull out metrics. The specified user is the Pegasus CIM User who should possess *Administator* privileges and should be associated with the *Logon as a Service* policy. 5. **CONFIRM PASSWORD** – Confirm the **PASSWORD** by retyping it here. 6. **SSL** – Set this flag to **Yes**, if the storage device being monitored is SSL-enabled. 7. **CIM SERVER PORT** - The SMI–S provider of the Dell Compellent Storage Center provides access for monitoring and management via the HTTP and HTTPS protocols for CIM API request/response semantics. To enable the eG agent to access the SMI-S Provider, invoke the CIM API commands, and collect the required metrics, you need to specify the service port on the SMI- S provider in the **CIM SERVER PORT** text box that listens for HTTP/HTTPS requests for CIM API semantics. By default, this is port 5988. If the service port on the SMI-S Provider listens only to HTTPS requests, then specify the port as 5989. 8. **ISEMBEDDED** – If this flag is set to **True**, it indicates that the SMI-S Provider is embedded on the Storage Center. On the other hand, if this flag is set to **False**, it indicates that the SMI-S Provider has been implemented as a proxy. 9. **SERIALNUMBER** – If the SMI-S Provider has been implemented as a proxy, then such a provider can be configured to manage multiple Storage Centers. This is why, if the **ISEMBEDDED** flag is set to **False**, you will have to explicitly specify which Storage Center you want the eG agent to monitor. Since each Storage Center is uniquely identified by a serial number, specify the same in the **SERIALNUMBER** text box.
Outputs of the test	One set of results for each storage array on the Dell Compellent Storage Center

<table>
<tr>
<td></td>
<td>Operational status:
Indicates the current operational state of this storage array.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>In Service</td></tr>
<tr><td>2</td><td>Power Mode</td></tr>
<tr><td>3</td><td>Completed</td></tr>
<tr><td>4</td><td>Starting</td></tr>
<tr><td>5</td><td>Dormant</td></tr>
<tr><td>6</td><td>Other</td></tr>
<tr><td>7</td><td>Unknown</td></tr>
<tr><td>8</td><td>Stopping</td></tr>
<tr><td>9</td><td>Stressed</td></tr>
<tr><td>10</td><td>Stopped</td></tr>
<tr><td>11</td><td>Supporting Entity in Error</td></tr>
<tr><td>12</td><td>Degraded or Predicted Failure</td></tr>
<tr><td>13</td><td>Predictive Failure</td></tr>
<tr><td>14</td><td>Lost Communication</td></tr>
<tr><td>15</td><td>No Contact</td></tr>
<tr><td>16</td><td>Aborted</td></tr>
<tr><td>17</td><td>Error</td></tr>
<tr><td>18</td><td>Non-Recoverable Error</td></tr>
</table>
</td>
</tr>
</table>

			By default, this measure reports the **Measure Values** discussed above to indicate the operational state of a storage array. In the graph of this measure however, operational states are represented using the numeric equivalents only.

<table>
<tr>
<td></td>
<td>Detailed operational status:
Describes the current operational state of this storage array.</td>
<td></td>
<td>Typically, the detailed state will describe why the storage array is in a particular operational state. For instance, if the Operational status measure reports the value Stopping for a storage array, then this measure will explain why that storage array is being stopped.

The values that this measure can report and their corresponding numeric values are discussed in the table below:

<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>Online</td></tr>
<tr><td>1</td><td>Success</td></tr>
<tr><td>2</td><td>Power Saving Mode</td></tr>
<tr><td>3</td><td>Write Protected</td></tr>
<tr><td>4</td><td>Write Disabled</td></tr>
<tr><td>5</td><td>Not Ready</td></tr>
<tr><td>6</td><td>Removed</td></tr>
<tr><td>7</td><td>Rebooting</td></tr>
<tr><td>8</td><td>Offline</td></tr>
<tr><td>9</td><td>Failure</td></tr>
</table>

Note

By default, this measure reports the Measure Values discussed above to indicate the detailed operational state of an array. In the graph of this measure however, detailed operational states are represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Data transmitted:
Indicates the rate at which data was transmitted by this storage array.</td>
<td>MB/Sec</td>
<td></td>
</tr>
</table>

	IOPS: Indicates the rate at which I/O operations were performed on this storage array.	IOPS	Compare the value of this measure across storage arrays to know which storage array handled the maximum number of I/O requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across storage arrays. You may then want to take a look at the *Reads* and *Writes* measures to understand what to fine-tune – the load-balancing algorithm for read requests or that of the write requests.
	Reads: Indicates the rate at which read operations were performed on this storage array.	Reads/Sec	Compare the value of this measure across storage arrays to know which storage array handled the maximum number of read requests and which handled the least.
	Writes: Indicates the rate at which write operations were performed on this storage array.	Writes/Sec	Compare the value of this measure across storage arrays to know which storage array handled the maximum number of write requests and which handled the least.
	Data reads: Indicates the rate at which data is read from this storage array.	MB/Sec	Compare the value of these measures across storage arrays to identify the slowest storage array in terms of servicing read and write requests (respectively).
	Data writes: Indicates the rate at which data is written to this storage array.	MB/Sec	
	Read hits: Indicates the percentage of read requests that were serviced by the cache of this storage array.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct storage array accesses, which are expensive operations, are high.
	Write hits: Indicates the percentage of write requests that were serviced by the cache of this storage array.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct storage array accesses, which are resource-intensive operations, are high.

	Average read size: Indicates the amount of data read from this storage array per I/O operation.	MB/Op	Compare the value of these measures across storage arrays to identify the slowest storage array in terms of servicing read and write requests (respectively).
	Average write size: Indicates the amount of data written to this storage array per I/O operation.	MB/Op	

1.3.2 Dell Compellent Controllers Test

The controller of the Dell Compellent Storage Center enables the administrator in serving the purpose of the following:

- binding LUNs
- execute CLI commands
- perform read/write operations from external server to SAN

Excessive usage of or heavy I/O load on a single controller can cause deterioration in the overall performance of the storage center, as it is indicative of severe deficiencies in the load-balancing algorithm that drives the controllers. Using the **Dell Compellent Controllers** test, administrators can easily monitor the current state, usage, and load on each of the controller on the Storage Center, quickly detect an overload condition, precisely point to the controller that is overloaded, and promptly initiate measures to resolve the issue, so as to ensure the optimal performance of the Storage Center.

Purpose	Using the **Dell Compellent Controllers** test, administrators can easily monitor the current state, usage, and load on each of the controller on the Storage Center, quickly detect an overload condition, precisely point to the controller that is overloaded, and promptly initiate measures to resolve the issue, so as to ensure the optimal performance of the Storage Center
Target of the test	A Dell Compellent Storage Center
Agent deploying the test	A remote agent

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The IP address of the storage device
3. PORT - The port number at which the storage device listens. The default is NULL.
4. USER and PASSWORD – Specify the credentials of a user who has the right to execute API commands on the Dell Compellent Storage Center and pull out metrics. The specified user should possess Administator privileges and should be associated with the Logon as a Service policy.
5. CONFIRM PASSWORD – Confirm the PASSWORD by retyping it here.
6. SSL – Set this flag to Yes, if the storage device being monitored is SSL-enabled.
7. CIM SERVER PORT - The SMI–S provider of the Dell Compellent Storage Center provides access for monitoring and management via the HTTP and HTTPS protocols for CIM API request/response semantics. To enable the eG agent to access the SMI-S Provider, invoke the CIM API commands, and collect the required metrics, you need to specify the service port on the SMI- S provider in the CIM SERVER PORT text box that listens for HTTP/HTTPS requests for CIM API semantics. By default, this is port 5988. If the service port on the SMI-S Provider listens only to HTTPS requests, then specify the port as 5989.
8. ISEMBEDDED – If this flag is set to True, it indicates that the SMI-S Provider is embedded on the Storage Center. On the other hand, if this flag is set to False, it indicates that the SMI-S Provider has been implemented as a proxy.
9. SERIALNUMBER – If the SMI-S Provider has been implemented as a proxy, then such a provider can be configured to manage multiple Storage Centers. This is why, if the ISEMBEDDED flag is set to False, you will have to explicitly specify which Storage Center you want the eG agent to monitor. Since each Storage Center is uniquely identified by a serial number, specify the same in the SERIALNUMBER text box.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each controller on the Dell Compellent Storage Center</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Operational status:
Indicates the current operational state of this controller.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>In Service</td></tr>
<tr><td>2</td><td>Power Mode</td></tr>
<tr><td>3</td><td>Completed</td></tr>
<tr><td>4</td><td>Starting</td></tr>
<tr><td>5</td><td>Dormant</td></tr>
<tr><td>6</td><td>Other</td></tr>
<tr><td>7</td><td>Unknown</td></tr>
<tr><td>8</td><td>Stopping</td></tr>
<tr><td>9</td><td>Stressed</td></tr>
<tr><td>10</td><td>Stopped</td></tr>
<tr><td>11</td><td>Supporting Entity in Error</td></tr>
<tr><td>12</td><td>Degraded or Predicted Failure</td></tr>
<tr><td>13</td><td>Predictive Failure</td></tr>
<tr><td>14</td><td>Lost Communication</td></tr>
<tr><td>15</td><td>No Contact</td></tr>
<tr><td>16</td><td>Aborted</td></tr>
<tr><td>17</td><td>Error</td></tr>
<tr><td>18</td><td>Non-Recoverable Error</td></tr>
</table>
</td>
</tr>
</table>

			Note By default, this measure reports the **Measure Values** discussed above to indicate the operational state of a controller. In the graph of this measure however, operational states are represented using the numeric equivalents only.

<table>
<tr>
<td></td>
<td>Detailed operational status:
Describes the current operational state of this controller.</td>
<td></td>
<td>Typically, the detailed state will describe why the controller is in a particular operational state. For instance, if the Operational status measure reports the value Stopping for a controller, then this measure will explain why that controller is being stopped.

The values that this measure can report and their corresponding numeric values are discussed in the table below:

<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>Online</td></tr>
<tr><td>1</td><td>Success</td></tr>
<tr><td>2</td><td>Power Saving Mode</td></tr>
<tr><td>3</td><td>Write Protected</td></tr>
<tr><td>4</td><td>Write Disabled</td></tr>
<tr><td>5</td><td>Not Ready</td></tr>
<tr><td>6</td><td>Removed</td></tr>
<tr><td>7</td><td>Rebooting</td></tr>
<tr><td>8</td><td>Offline</td></tr>
<tr><td>9</td><td>Failure</td></tr>
</table>

Note
By default, this measure reports the Measure Values discussed above to indicate the detailed operational state of a controller. In the graph of this measure however, detailed operational states are represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Data transmitted:
Indicates the rate at which data was transmitted by this controller.</td>
<td>MB/Sec</td>
<td></td>
</tr>
</table>

	IOPS: Indicates the rate at which I/O operations were performed on this controller.	IOPS	Compare the value of this measure across controllers to know which controller handled the maximum number of I/O requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across controllers. You may then want to take a look at the *Reads* and *Writes* measures to understand what to fine-tune – the load-balancing algorithm for read requests or that of the write requests.
	Reads: Indicates the rate at which read operations were performed on this controller.	Reads/Sec	Compare the value of this measure across controllers to know which controller handled the maximum number of read requests and which handled the least.
	Writes: Indicates the rate at which write operations were performed on this controller.	Writes/Sec	Compare the value of this measure across controllers to know which controller handled the maximum number of write requests and which handled the least.
	Data reads: Indicates the rate at which data is read from this controller.	MB/Sec	Compare the value of these measures across controllers to identify the slowest controller in terms of servicing read and write requests (respectively).
	Data writes: Indicates the rate at which data is written to this controller.	MB/Sec	
	Average read size: Indicates the amount of data read from this controller per I/O operation	MB/Op	Compare the value of these measures across controllers to identify the slowest controller in terms of servicing read and write requests (respectively).
	Average write size: Indicates the amount of data written to this controller per I/O operation.	MB/Op	
	Read hits: Indicates the percentage of read requests that were serviced by the cache of this controller.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct controller accesses, which are expensive operations, are high.

	Write hits: Indicates the percentage of write requests that were serviced by the cache of this controller.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct controller accesses, which are expensive operations, are high.

1.3.3 Dell Compellent Ports Test

Storage ports help the controllers receive and process I/O requests. By periodically checking port status and measuring the I/O load on the ports, you can identify overloaded ports and thus proactively detect potential/existing load-balancing irregularities and/or processing bottlenecks with the ports. The **Dell Compellent Ports** test facilitates this port check. For every port configured for the controllers supported by the Storage Center, this test reports the port state, the I/O load on the ports, and the processing ability of the ports. In the process, the test not only points administrators to overloaded ports, but also puts a finger on ports that are slow when processing I/O requests.

Purpose	For every port configured for the controllers supported by the Storage Center, this test reports the port state, the I/O load on the ports, and the processing ability of the ports. In the process, the test not only points administrators to overloaded ports, but also puts a finger on ports that are slow when processing I/O requests
Target of the test	A Dell Compellent Storage Center
Agent deploying the test	A remote agent

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The IP address of the storage device
3. PORT - The port number at which the storage device listens. The default is NULL.
4. USER and PASSWORD – Specify the credentials of a user who has the right to execute API commands on the Dell Compellent Storage Center and pull out metrics. The specified user should possess Administator privileges and should be associated with the Logon as a Service policy.
5. CONFIRM PASSWORD – Confirm the PASSWORD by retyping it here.
6. SSL – Set this flag to Yes, if the storage device being monitored is SSL-enabled.
7. CIM SERVER PORT - The SMI–S provider of the Dell Compellent Storage Center provides access for monitoring and management via the HTTP and HTTPS protocols for CIM API request/response semantics. To enable the eG agent to access the SMI-S Provider, invoke the CIM API commands, and collect the required metrics, you need to specify the service port on the SMI- S provider in the CIM SERVER PORT text box that listens for HTTP/HTTPS requests for CIM API semantics. By default, this is port 5988. If the service port on the SMI-S Provider listens only to HTTPS requests, then specify the port as 5989.
8. ISEMBEDDED – If this flag is set to True, it indicates that the SMI-S Provider is embedded on the Storage Center. On the other hand, if this flag is set to False, it indicates that the SMI-S Provider has been implemented as a proxy.
9. SERIALNUMBER – If the SMI-S Provider has been implemented as a proxy, then such a provider can be configured to manage multiple Storage Centers. This is why, if the ISEMBEDDED flag is set to False, you will have to explicitly specify which Storage Center you want the eG agent to monitor. Since each Storage Center is uniquely identified by a serial number, specify the same in the SERIALNUMBER text box.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each storage port on the Dell Compellent Storage Center</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td>test</td>
<td>Health state:
Indicates how healthy this port currently is.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>Unknown</td></tr>
<tr><td>2</td><td>Degraded/Warning</td></tr>
<tr><td>3</td><td>Minor failure</td></tr>
<tr><td>4</td><td>Major failure</td></tr>
<tr><td>5</td><td>Critical failure</td></tr>
<tr><td>6</td><td>Non-recoverable error</td></tr>
</table>

By default, this measure reports the Measure Values discussed above to indicate the state of a port. In the graph of this measure however, states are represented using the numeric equivalents only.</td>
</tr>
</table>

	Operational status: Indicates the current operational state of this port.		The values that this measure can report and their corresponding numeric values are discussed in the table below:

Numeric Value	Measure Value
0	OK
1	In Service
2	Power Mode
3	Completed
4	Starting
5	Dormant
6	Other
7	Unknown
8	Stopping
9	Stressed
10	Stopped
11	Supporting Entity in Error
12	Degraded or Predicted Failure
13	Predictive Failure
14	Lost Communication
15	No Contact
16	Aborted
17	Error
18	Non-Recoverable Error

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>

By default, this measure reports the Measure Values discussed above to indicate the operational state of a port. In the graph of this measure however, operational states are represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Detailed operational status:
Describes the current operational state of this port.</td>
<td></td>
<td>Typically, the detailed state will describe why the port is in a particular operational state. For instance, if the Operational status measure reports the value Stopping for a port, then this measure will explain why that port is being stopped.

The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>Online</td></tr>
<tr><td>1</td><td>Success</td></tr>
<tr><td>2</td><td>Power Saving Mode</td></tr>
<tr><td>3</td><td>Write Protected</td></tr>
<tr><td>4</td><td>Write Disabled</td></tr>
<tr><td>5</td><td>Not Ready</td></tr>
<tr><td>6</td><td>Removed</td></tr>
<tr><td>7</td><td>Rebooting</td></tr>
<tr><td>8</td><td>Offline</td></tr>
<tr><td>9</td><td>Failure</td></tr>
</table>

By default, this measure reports the Measure Values discussed above to indicate the detailed operational state of a port. In the graph of this measure however, detailed operational states are represented using the numeric equivalents only.</td>
</tr>
</table>

	Data transmitted: Indicates the rate at which data was transmitted by this port.	MB/Sec	
	IOPS: Indicates the rate at which I/O operations were performed on this port.	IOPS	Compare the value of this measure across ports to know which port handled the maximum number of I/O requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across ports.

1.4 The Dell Compellent Service Layer

This layer monitors the LUNs and reports how healthy each LUN is and how well the storage system balances I/O load across LUNs.

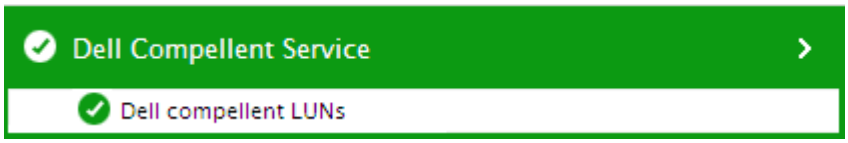

Figure 13: The tests mapped to the Dell Compellent Service layer

1.4.1 Dell Compellent LUNs Test

A logical unit number (LUN) is a unique identifier used to designate individual or collections of hard disk devices for address by a protocol associated with a SCSI, iSCSI, Fibre Channel (FC) or similar interface. LUNs are central to the management of storage arrays shared over a storage area network (SAN). LUN errors, poor LUN cache usage, and abnormal I/O activity on the LUNs, if not promptly detected and resolved, can hence significantly degrade the performance of the storage array. This is why, it is important that LUN performance is continuously monitored. This can be achieved using the **Dell Compellent LUNs** test. This test auto-discovers the LUNs in the Storage Center and reports the current state of each LUN, captures LUN errors, and measures the level of I/O activity on every LUN, so that administrators are notified of LUN-related problems well before they impact Storage Center performance.

Purpose	Auto-discovers the LUNs in the Storage Center and reports the current state of each LUN, captures LUN errors, and measures the level of I/O activity on every LUN, so that administrators are notified of LUN-related problems well before they impact Storage Center performance
Target of the test	A Dell Compellent Storage Center
Agent deploying the test	A remote agent

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The IP address of the storage device
3. PORT - The port number at which the storage device listens. The default is NULL.
4. USER and PASSWORD – Specify the credentials of a user who has the right to execute API commands on the Dell Compellent Storage Center and pull out metrics. The specified user should possess Administator privileges and should be associated with the Logon as a Service policy.
5. CONFIRM PASSWORD – Confirm the PASSWORD by retyping it here.
6. SSL – Set this flag to Yes, if the storage device being monitored is SSL-enabled.
7. CIM SERVER PORT - The SMI–S provider of the Dell Compellent Storage Center provides access for monitoring and management via the HTTP and HTTPS protocols for CIM API request/response semantics. To enable the eG agent to access the SMI-S Provider, invoke the CIM API commands, and collect the required metrics, you need to specify the service port on the SMI- S provider in the CIM SERVER PORT text box that listens for HTTP/HTTPS requests for CIM API semantics. By default, this is port 5988. If the service port on the SMI-S Provider listens only to HTTPS requests, then specify the port as 5989.
8. ISEMBEDDED – If this flag is set to True, it indicates that the SMI-S Provider is embedded on the Storage Center. On the other hand, if this flag is set to False, it indicates that the SMI-S Provider has been implemented as a proxy.
9. SERIALNUMBER – If the SMI-S Provider has been implemented as a proxy, then such a provider can be configured to manage multiple Storage Centers. This is why, if the ISEMBEDDED flag is set to False, you will have to explicitly specify which Storage Center you want the eG agent to monitor. Since each Storage Center is uniquely identified by a serial number, specify the same in the SERIALNUMBER text box.
10. DETAILED DIAGNOSIS – To make diagnosis more efficient and accurate, the eG Enterprise system 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 against DETAILED DIAGNOSIS. 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:
➢ 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each LUN on the Dell Compellent Storage Center</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td>test</td>
<td>Health state:
Indicates how healthy this LUN currently is.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>Unknown</td></tr>
<tr><td>2</td><td>Degraded/Warning</td></tr>
<tr><td>3</td><td>Minor failure</td></tr>
<tr><td>4</td><td>Major failure</td></tr>
<tr><td>5</td><td>Critical failure</td></tr>
<tr><td>6</td><td>Non-recoverable error</td></tr>
</table>

By default, this measure reports the Measure Values discussed above to indicate the state of a LUN In the graph of this measure however, states are represented using the numeric equivalents only.

The detailed diagnosis of this measure if enabled, lists the capacity of the LUN.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Operational status:
Indicates the current operational state of this LUN.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>OK</td></tr>
<tr><td>1</td><td>In Service</td></tr>
<tr><td>2</td><td>Power Mode</td></tr>
<tr><td>3</td><td>Completed</td></tr>
<tr><td>4</td><td>Starting</td></tr>
<tr><td>5</td><td>Dormant</td></tr>
<tr><td>6</td><td>Other</td></tr>
<tr><td>7</td><td>Unknown</td></tr>
<tr><td>8</td><td>Stopping</td></tr>
<tr><td>9</td><td>Stressed</td></tr>
<tr><td>10</td><td>Stopped</td></tr>
<tr><td>11</td><td>Supporting Entity in Error</td></tr>
<tr><td>12</td><td>Degraded or Predicted Failure</td></tr>
<tr><td>13</td><td>Predictive Failure</td></tr>
<tr><td>14</td><td>Lost Communication</td></tr>
<tr><td>15</td><td>No Contact</td></tr>
<tr><td>16</td><td>Aborted</td></tr>
<tr><td>17</td><td>Error</td></tr>
<tr><td>18</td><td>Non-Recoverable Error</td></tr>
</table>
</td>
</tr>
</table>

			Note By default, this measure reports the **Measure Values** discussed above to indicate the operational state of a LUN. In the graph of this measure however, operational states are represented using the numeric equivalents only.

<table>
<tr>
<td></td>
<td>Detailed operational state:
Describes the current operational state of this LUN.</td>
<td></td>
<td>Typically, the detailed state will describe why the LUN is in a particular operational state. For instance, if the Operational status measure reports the value Stopping for a LUN, then this measure will explain why that LUN is being stopped.

The values that this measure can report and their corresponding numeric values are discussed in the table below:

<table>
<tr><th>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>0</td><td>Online</td></tr>
<tr><td>1</td><td>Success</td></tr>
<tr><td>2</td><td>Power Saving Mode</td></tr>
<tr><td>3</td><td>Write Protected</td></tr>
<tr><td>4</td><td>Write Disabled</td></tr>
<tr><td>5</td><td>Not Ready</td></tr>
<tr><td>6</td><td>Removed</td></tr>
<tr><td>7</td><td>Rebooting</td></tr>
<tr><td>8</td><td>Offline</td></tr>
<tr><td>9</td><td>Failure</td></tr>
</table>

Note

By default, this measure reports the Measure Values discussed above to indicate the detailed operational state of a LUN. In the graph of this measure however, detailed operational states are represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Data transmitted:
Indicates the rate at which data was transmitted by this LUN.</td>
<td>MB/Sec</td>
<td></td>
</tr>
</table>

	IOPS: Indicates the rate at which I/O operations were performed on this LUN.	IOPS	Compare the value of this measure across LUNs to know which LUN handled the maximum number of I/O requests and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across LUNs. You may then want to take a look at the *Reads* and *Writes* measures to understand what to fine-tune – the load-balancing algorithm for read requests or that of the write requests.
	Reads: Indicates the rate at which read operations were performed on this LUN.	Reads/Sec	Compare the value of this measure across LUNs to know which LUN handled the maximum number of read requests and which handled the least.
	Writes: Indicates the rate at which write operations were performed on this LUN.	Writes/Sec	Compare the value of this measure across LUNs to know which LUN handled the maximum number of write requests and which handled the least.
	Data reads: Indicates the rate at which data is read from this LUN.	MB/Sec	Compare the value of these measures across LUNs to identify the slowest LUN in terms of servicing read and write requests (respectively).
	Data writes: Indicates the rate at which data is written to this LUN.	MB/Sec	
	LUNs busy: Indicates the percentage of time this LUN was busy processing requests.	Percent	Compare the value of this measure across LUNs to know which LUN was the busiest and which LUN was not. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across LUNs.
	Average read size: Indicates the amount of data read from this LUN per I/O operation.	MB/Op	Compare the value of these measures across LUNs to identify the slowest LUN in terms of servicing read and write requests (respectively).
	Average write size: Indicates the amount of data written to this LUN per I/O operation.	MB/Op	

	Read hits: Indicates the percentage of read requests that were serviced by the cache of this LUN.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct LUN accesses, which are expensive operations, are high.
	Write hits: Indicates the percentage of write requests that were serviced by the cache of this LUN.	Percent	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies that direct LUN accesses, which are expensive operations, are high.
	Average response time: Indicates the time taken by this LUN to respond to I/O requests.	Microsecs	Ideally, this value should be low. If not, it implies that the LUN is slow.
	Queue depth: Indicates the number of requests that are in queue for this LUN.	Number	A consistent increase in this value indicates a potential processing bottleneck with the LUN.

2

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 **Dell Compellent** Storage Center. 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.