Monitoring NetApp Cluster

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 2008, Windows 2012, Windows 2016, Windows 7, Widows 8, and Windows 10 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

Table of Contents

Table of Figures

1

Monitoring the NetApp Cluster

NetApp Clustered Data ONTAP is an enterprise-ready, unified scale-out storage which increases the scalability, protocol support, and data protection capabilities. Scale-out storage is the most powerful and flexible way to respond to the inevitable data growth and data management challenges in today's environments. With *scale-out*, as the storage environment grows, additional controllers are added seamlessly to the resource pool residing on a shared storage infrastructure. Scale-out, together with built-in storage virtualization, provides nondisruptive movement of host and client connections, as well as the datastores themselves, anywhere in the resource pool. With these capabilities, new workloads can be easily deployed and existing workloads can be easily and nondisruptively balanced over the available resources. Technology refreshes (replacing disk shelves, adding or completely replacing storage controllers) are accomplished while the environment remains online and serving data.

A clustered Data ONTAP system consists of NetApp storage controllers (including V-Series or FlexArray licensed systems) with attached disks. The basic building block is the high-availability (HA) pair which consists of two identical *nodes,* or instances of clustered Data ONTAP. Each node actively provides data services and has redundant cabled paths to the other node's disk storage. If either node is down for any reason, planned or unplanned, its HA partner can take over its storage and maintain access to the data. When the downed system rejoins the cluster, the partner node gives back the storage resources. The storage nodes are combined into a cluster to form a shared pool of physical resources that are available to applications, SAN hosts, and NAS clients (see Figure 1.1). The shared pool appears as a single system image for management purposes, providing a single common point of management, through GUI or CLI tools, for the entire cluster.

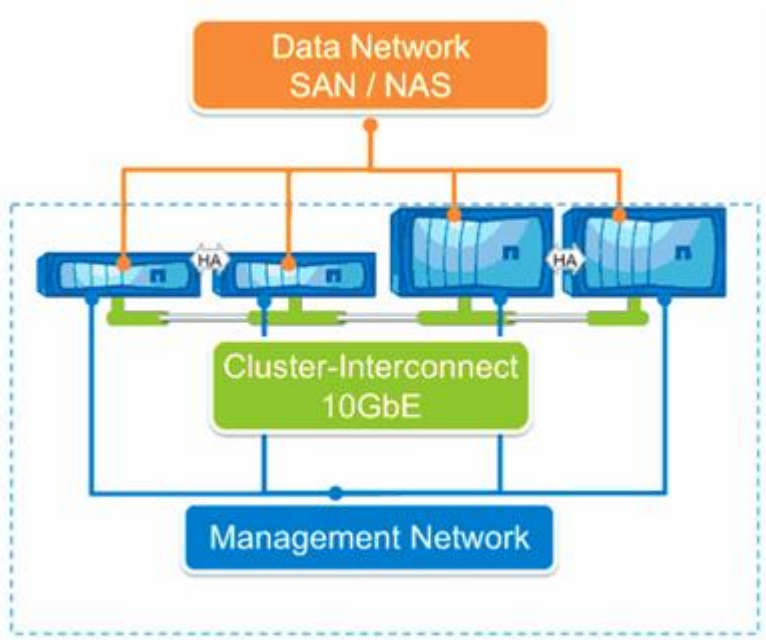

Figure 1.1: The NetApp Cluster architectural overview

A NetApp Cluster is composed of physical hardware such as storage controllers with attached disk shelves, network interface cards, and, optionally, Flash Cache cards. Together these components create a physical resource pool that is virtualized as logical cluster resources to provide data access. Abstracting and virtualizing physical assets into logical resources provide the flexibility and potential multi-tenancy in clustered Data ONTAP as well as the object mobility capabilities that are the heart of nondisruptive operations.

To understand the architecture of the NetApp Cluster in a better way, the components of the cluster are classified further into Physical Cluster Components and Logical Cluster Components. Let us now discuss each of them in detail.

Physical Cluster Components: Storage controllers, independent of the model, are considered equivalent in the cluster configuration in that they are all presented and managed as *cluster nodes*. Clustered Data ONTAP is a symmetrical architecture, with all nodes performing the same data-serving function.

Individual disks are managed by defining them into *aggregates:* groups of disks of a particular type that are protected by using NetApp RAID-DP® technology, similar to 7-Mode.

Network interface cards and HBAs provide physical *ports* (Ethernet and Fibre Channel) for connection to the management and data networks.

The physical components provide a pool of shared resources from which the logical cluster resources are constructed. Applications and hosts access data only through storage virtual machines (SVMs) that contain volumes and logical interfaces.

Logical Cluster Components: The primary logical cluster component is the storage virtual machine (SVM); all client and host data access is via an SVM. Clustered Data ONTAP supports a minimum of one and up to hundreds of SVMs in a single cluster. Each SVM is configured for the client and host access protocols it supports—any combination of SAN and NAS. Each SVM contains at least one volume and at least one logical interface. The accessing hosts and clients connect to the SVM via a *logical interface* (LIF).

Owing to their high availability and efficient load distribution features, the NetApp Cluster is very popular in large, mission-critical IT infrastructures, which require ready and reliable storage services. In such environments, the non-availability of the storage system or any of its core components, rapid erosion of storage space provided by the storage system, and inconsistencies in I/O load-balancing across disks/LUNs/Aggregate/Volumes can result in

short/prolonged delays in the delivery of storage services, which will ultimately slowdown the dependent end-user services. To avoid this, it is imperative to watch out for issues in the operations and usage of the cluster on a regular basis.

eG Enterprise provides out-of-the-box monitoring for the NetApp Cluster. The *NetApp Cluster* monitoring model (see Figure 1.2) offered by the eG Enterprise Suite monitors various aspects of the performance of the NetApp Cluster and promptly alerts storage administrators to potential I/O processing bottlenecks or space crunches.

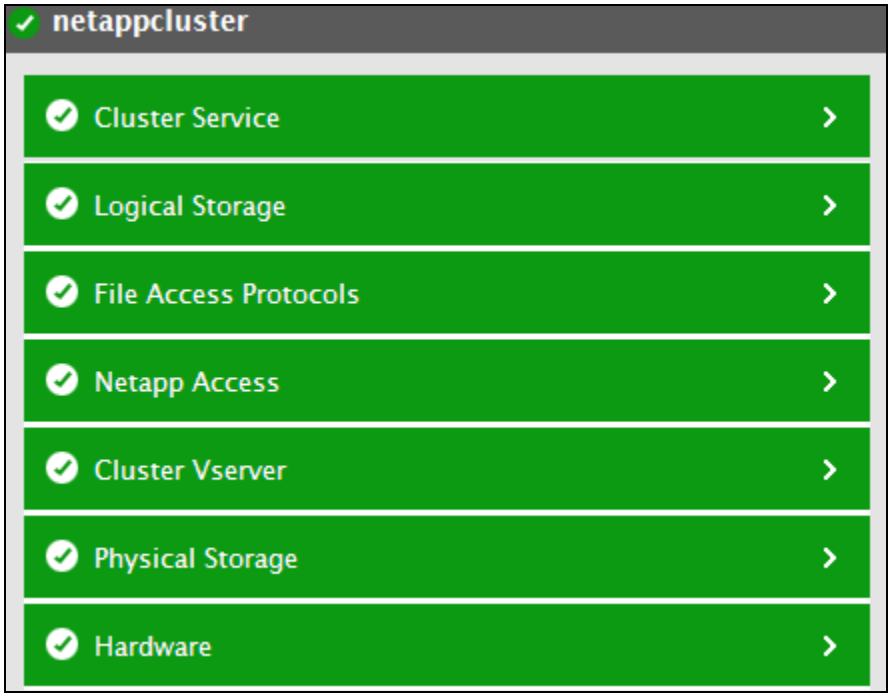

Figure 1.2: The layer model of a NetApp Cluster

1.1 How does eG Enterprise Monitor the NetApp USD?

In order to monitor a NetApp Cluster, eG uses best-of-both-worlds combination of SNMP and NetApp Manageability SDK. While a few tests directly poll the SNMP MIB of the device to pull out the metrics, most tests run the NetApp Manageability SDK commands for metrics collection.

The metrics so collected report on the following:

- The performance of the hardware compoennts of the cluster;
- The health of the network components that interface with (and depend on) the hardware;
- The current status and space usage of physical storage entities (disks, aggregates etc);
- The efficiency of the access framework and protocols that are used to access the cluster – e.g., iSCSI;
- The NAS aspect of the NetApp Cluster; this includes the file access protocols such as CIFS;
- Abnormalities related to the usage of logical storage entities (such as volumes, LUNs, Qtrees etc.,) which are accessed using their framework by the end users;
- The overall status and performance of the NetApp Cluster which depends on all its underlying components;

- The failover state of the NetApp Cluster;

To know how to configure each of these monitoring mechanisms, refer to the sections below.

1.1.1 Configuring the eG Agent to Poll the SNMP MIB of the NetApp Cluster to Pull Out the Metrics

You can configure tests to periodically poll the SNMP MIB of the NetApp Cluster for collecting metrics of interest. For this, **you have to SNMP-enable the NetApp Cluster**.

1.1.2 Configuring the eG Agent to Use the NetApp Manageability SDK

The NetApp Manageability SDK (NMSDK) provides resources to develop applications that monitor and manage NetApp storage systems.

Many tests that execute on the NetApp Cluster run API commands provided by this SDK to extract the performance metrics.

To run these commands, the following pre-requisites need to be fulfilled:

- An **eG remote agent** should be installed on a remote Windows/Unix host in the environment. This remote agent should be assigned to the target storage device when managing that device using the eG administrative interface.
- The eG remote agent should be able to access the target storage device.
- The NMSDK should be available on the eG remote agent host. To achieve this, follow the steps discussed below:
  - Download the NMSDK from the following URL to any location on the remote agent host:

    http://support.netapp.com/NOW/cgi-bin/software

    To download the NMSDK, you will have to create a NOW login; to achieve this, go to the following URL:

    http://support.netapp.com

    Note:

    While you download the NMSDK, you should select the platform for which the download is applicable. For an eG agent to collect metrics, you should select **All platforms** option as shown in Figure 1.3.

Figure 1.3: Selecting the All Platforms option to download the NMSDK

  - The NMSDK will be downloaded as a zip file named **netapp-manageability-sdk-<SDK_version>.zip**. Extract the contents of the zip file to any location on the eG remote agent host.
  - Next, copy the **netapp-manageability-sdk-<SDK_version>\netapp-manageability-sdk-<SDK_version>\lib\java\classes\manageontap.jar** file from the extracted contents to the **<EG_AGENT_INSTALL_DIR>\lib** directory (on a Windows host; on Unix, this will be the **/opt/egurkha/lib** directory). Sometimes, the name of the jar file may be suffixed by the NMSDK version number. For instance, instead of **manageontap.jar**, you might find **manageontap-5.2.jar** in **\java\classes**. In such a

case, first, rename the jar file to **manageontap.jar**, and then copy the jar file to the **<EG_AGENT_INSTALL_DIR>\lib** directory.

- Then, start the eG agent.

- To invoke the API commands, the eG agent has to be configured with the *readonly* role of a NetApp Cluster user.

  For this purpose, you can either grant the aforesaid role to an existing user, or create a new user. The new user creation process has been detailed in Section 1.1.2.1 below. Once such a user is created, make sure that you configure the eG tests with the credentials of such a user.

- Manage the storage device as a *NetApp Cluster* in eG using its **Cluster Management IP address**. Before that, make sure that the target is indeed a *NetApp Cluster* device and not a stand-alone *NetApp Unified Storage* device. For that, check the full version string for the Data ONTAP version in the NetApp device. If the version string contains the word "c-mode" or the word "cDOT", then it means that the target NetApp device is part of a cluster.

1.1.2.1 Creating a New User with the Role Required for Monitoring the NetApp Cluster

As mentioned earlier, to run the API commands provided by the NMSDK and collect metrics, the eG agent requires the *readonly* role.

To create a new user with the *readonly* role, do the following:

1. Login to the system hosting the remote agent.
2. Connect to the NetApp Cluster's console via SSH (say, using **puTTy.exe**).
3. To create a new user with *readonly* role on a NetApp clustered Data ONTAP version 8.3 (and higher), run the following command at the console:

   Security login create –user-or-group-name <user1> –application ontapi –authmethod password –role readonly

   For instance, to create a new user named **eGMonuser** for monitoring a NetApp clustered Data ONTAP version 8.3 (or higher), the command will be as follows:

   Security login create –user-or-group-name eGMonuser –application ontapi –authmethod password –role readonly

   To create a new user with *readonly* role on a NetApp clustered Data ONTAP version 8.2 (and lower), run the following command at the console:

   Security login create –username <user1> –application ontapi –authmethod password –role readonly

   For instance, to create a new user named **eGMonuser** for monitoring a NetApp clustered Data ONTAP version 8.2 (or lower), the command will be as follows:

   Security login create –username eGMonuser –application ontapi –authmethod password –role readonly

4. This command, upon execution, will request for the password of the new user. The password is case-sensitive, and should be atleast 8 characters long. **It must contain atleast 2 alphabets and 1 digit**.

   ```
   Please enter a password for user 'eGMonuser':
   Please enter it again:
   ```

5. Then, confirm the new user's password by retyping it.

1.2 The Hardware Layer

Use the test mapped to this layer to determine current/potential issues (if any) in the health of the hardware components of the NetApp Cluster.

Figure 1.4: The tests mapped to the Hardware layer

1.2.1 System Performance Test

This test monitors the NetApp Cluster's support environment - which includes its hardware, the fans, the power supply units, and the battery - and promptly alerts you to current/potential issues in the health of this environment. These issues can range from abnormal hardware temperature to batteries fast-approaching their end-of-life and more!

Purpose	Monitors the NetApp Cluster's support environment - which includes its hardware, the fans, the power supply units and the battery - and promptly alerts you to current/potential issues in the health of this environment
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the NetApp Cluster 3. **SNMPPORT** – The SNMP Port number of the NetApp Cluster (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: ➢ **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: ➢ **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.

<table>
<tr><td></td><td colspan="3">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 NetApp Cluster over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.

16. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
o The eG manager license should allow the detailed diagnosis capability
o 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 the NetApp Cluster being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>CPU busy:
Indicates the percentage of time for which the CPU time was busy performing system-level processing during the last measurement period.</td><td>Percent</td><td>A high value indicates that the storage system is utilizing CPU resources excessively. A consistent increase in this value could indicate a potential CPU contention on the storage system.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Is over Temperature?:
Indicates whether/not the hardware is currently operating outside its recommended temperature range.</td>
<td></td>
<td>This measure reports a value Yes if the hardware temperature is operating outside the recommended temperature range and No if otherwise.
The numeric values corresponding to the above-mentioned measure values are as follows:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>1</td></tr>
<tr><td>Yes</td><td>2</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating whether the hardware is operating within the recommended temperature range or not. However, the graph of this measure will be represented using the corresponding numeric equivalents i.e., 1 or 2 only.</td>
</tr>
<tr>
<td></td>
<td>Failed fan count:
Indicates the number of fans that failed in the NetApp Cluster.</td>
<td>Number</td>
<td>The detailed diagnosis capability, if enabled for this test, will list the fans that failed and the reason for their failure.</td>
</tr>
<tr>
<td></td>
<td>Failed power supply count:
Indicates the number of power supply units that failed in the NetApp Cluster.</td>
<td>Number</td>
<td>The detailed diagnosis capability, if enabled for this test, will list the power supply units that have failed and the reason for their failure.</td>
</tr>
</table>

	Battery state: Indicates the current status of the NVRAM battery.		The values reported by this measure and their numeric equivalents are available in the table below: **Measure Value** / **Numeric Value** Ok / 1 Partially discharged / 2 Fully discharged / 3 Not present / 4 Near end of life / 5 At end of life / 6 Unknown / 7 Over charged / 8 Fully charged / 9 **Note:** This measure reports the **Measure Value**s listed in the table above to indicate the current battery status. However, in the graph of this measure, the same will be represented using only the **Numeric Value**s listed in the above table.

1.3 The Physical Storage Layer

The tests associated with this layer reveal abnormalities related to the core physical storage components such as Disks and Aggregates.

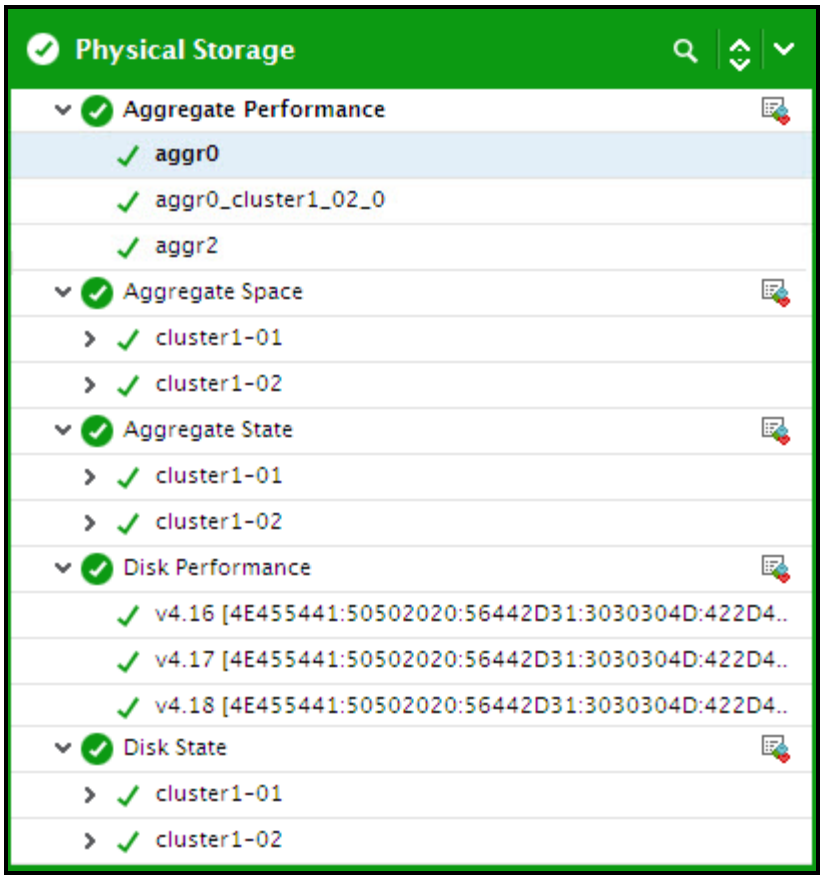

Figure 1.5: The test mapped to the Physical Storage layer

1.3.1 Aggregate Performance Test

To support the differing security, backup, performance, and data sharing needs of your users, you group the physical data storage resources on your storage system into one or more aggregates. These aggregates provide storage to the volume or volumes that they contain. Each aggregate has its own RAID configuration, plex structure, and set of assigned disks or array LUNs.

Periodically, you must monitor the I/O activity of each of the aggregates configured on your cluster, so that probable I/O overloads can be rapidly detected from time to time. The **NetApp Aggregates** test provides these performance insights. This test auto-discovers the aggregates configured on a NetApp Cluster, periodically reports the distribution of I/O load across all aggregates and helps you to identify the aggregate that is overloaded with read-write requests.

Purpose	Auto-discovers the aggregates configured on a NetApp Cluster, periodically reports the distribution of I/O load across all aggregates and helps you to identify the aggregate that is overloaded with read-write requests
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the **USE SSL** flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **EXCLUDE AGGREGATES –** If you wish to exclude certain aggregates from the scope of monitoring, specify a list of comma-separated aggregates in this text box. By default, *none* will be displayed here. 11. **RECORDS PER CALL –** The eG agent by default, executes the API commands in order to query the aggregates in the target environment. In critical infrastructures spanning large number of aggregates, a single execution by the eG agent may query(or download) a sizeable amount of monitoring data, thereby adding to the cluster load. To avoid this, you can tweak the **RECORDS PER CALL** parameter to enable the eG agent to obtain monitoring data iteratively in chunks instead of retrieving the entire amount of monitoring data in a single go. Say for example, the eG agent is required to query 1000 aggregates, then specifying the value 100 in this text box will enable the eG agent to query 100 aggregates at a time for 10 times to obtain monitoring data from all the aggregates. By default, the value of this parameter is 10. 12. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •
Outputs of the test	One set of results for each aggregate on the NetApp Cluster being monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Consistency point reads: Indicates the rate at which the read requests from the user is serviced during a Consistency Point (CP) operation in this aggregate.	Reads/Sec	A consistent decrease in the value of this measure could indicate that CP operations are slowing down the processing of read requests.
	Total transfers: Indicates the rate at which the transfers are serviced by this aggregate.	Transfers/Sec	Compare the value of this measure across aggregates to identify the busy aggregates.
	User read blocks: Indicates the rate at which the blocks are read from this aggregate upon a user request.	Blocks/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing read requests. Compare the value of this measure across aggregates to know which aggregates service block read requests slowly.
	User reads: Indicates the rate at which the read request from the user is serviced by this aggregate.	Reads/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing read requests. Compare the value of this measure across aggregates to know which aggregates service read requests slowly.
	User write blocks: Indicates the rate at which the blocks are written to this aggregate upon a user request.	Blocks/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing write requests. Compare the value of this measure across aggregates to know which aggregates are servicing block write requests slowly.
	User writes: Indicates the rate at which the write request from the user is serviced in this aggregate.	Writes/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing write requests. Compare the value of this measure across aggregates to know which aggregates are servicing write requests slowly.

1.3.2 Aggregate Space Test

For an aggregate to perform effectively, there must be adequate free space in the aggregate. Periodical monitoring of the aggregates for the space usage of each of the aggregates is mandatory to identify probable space contentions which may indirectly slowdown the performance of the aggregates. This is why you need the **Aggregate Space** test! This test auto-discovers the aggregates in the NetApp Cluster and reports the space utilization of each aggregate.

Purpose	Reports the current state of each aggregate in the NetApp Cluster
Target of the	A NetApp Cluster

<table>
<tr><td>test</td><td colspan="3"></td></tr>
<tr><td>Agent deploying the test</td><td colspan="3">An external/remote agent</td></tr>
<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 controller cluster.
3. PORT – The port number at which the specified HOST listens to. By default, this is NULL.
4. USER – Here, specify the name of the user who possesses the readonly role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document.
5. PASSWORD - Specify the password that corresponds to the above-mentioned USER.
6. CONFIRM PASSWORD – Confirm the PASSWORD by retping it here.
7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. EXCLUDE AGGREGATES – If you wish to exclude certain aggregates from the scope of monitoring, specify a list of comma-separated aggregates in this text box. By default, none will be displayed here.
11. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each aggregate on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

test	**Total space:** Indicates the total size of this aggregate.	GB	The size of this aggregate excludes the WAFL reserve and the aggregate snapshot reserve. This measure will report a value of *0* if the state of the aggregate is *Restricted* or *Offline*.
	Available space: Indicates the amount of space that is currently available for use in this aggregate.	GB	A very low value for this measure indicates that the aggeragate is currently running out of space.
	Max used space: Indicates the maximum amount of space that is used in this aggregate since the start of the NetApp Cluster.	GB	If the value of this measure is close to that of the *Total space* measure, it indicates potential space crunch in the aggregate. Administrators may increase the size of the aggregate so that the space utilization of the aggregate is optimal.
	Percentage max used space: Indicates the maximum percentage of space that is used in this aggregate since the start of the NetApp Cluster.	Percent	A value close to 100 for this measure is a cause for concern.

1.3.3 Aggregate State Test

This test reports the current state of each aggregate in the NetApp Cluster. Using this test, you can easily figure out the aggreagtes that are currently online, the ones that have failed and the ones that are currently offline.

Purpose	Reports the current state of each aggregate in the NetApp Cluster
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**.

	8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **EXCLUDE AGGREGATES –** If you wish to exclude certain aggregates from the scope of monitoring, specify a list of comma-separated aggregates in this text box. By default, *none* will be displayed here. 11. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each aggregate on the NetApp Cluster being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>test</td>
<td>State:
Indicates the current state of this aggregate.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Creating</td><td>1</td></tr>
<tr><td>Online</td><td>2</td></tr>
<tr><td>Relocating</td><td>3</td></tr>
<tr><td>Frozen</td><td>4</td></tr>
<tr><td>Iron restricted</td><td>5</td></tr>
<tr><td>Mounting</td><td>6</td></tr>
<tr><td>Partial</td><td>7</td></tr>
<tr><td>Quiesced</td><td>8</td></tr>
<tr><td>Quiescing</td><td>9</td></tr>
<tr><td>Reverted</td><td>10</td></tr>
<tr><td>Unmounted</td><td>11</td></tr>
<tr><td>Unmounting</td><td>12</td></tr>
<tr><td>Restricted</td><td>13</td></tr>
<tr><td>Inconsistent</td><td>14</td></tr>
<tr><td>Destroying</td><td>15</td></tr>
<tr><td>Unknown</td><td>16</td></tr>
<tr><td>Offline</td><td>17</td></tr>
<tr><td>Failed</td><td>18</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current status of an aggregate. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 1 to 18.
If the Measure Values corresponding to the Numeric Values of 13 and above are reported, then it indicates that the aggregate in consideration is problematic.</td>
</tr>
</table>

1.3.4 Disk Performance Test

Disks form the basic storage device in the NetApp storage systems. ATA disks, Fibre Channel disks, SCSI disks, SAS disks or SATA disks are used, depending on the storage system model.

Data ONTAP assigns and makes use of four different disk categories to support data storage, parity protection, and disk replacement. The disk category can be one of the following types:

- **Data disk** - Holds data stored on behalf of clients within RAID groups (and any system management data)
- **Global hot spare disk** - Does not hold usable data, but is available to be added to a RAID group in an aggregate. Any functioning disk that is not assigned to an aggregate functions acts as a hot spare disk.
- **Parity disk** - Stores information required for data reconstruction within RAID groups.
- **Double-parity disk** - Stores double-parity information within RAID groups, if RAID-DP is used.

Administrators should closely monitor the level of I/O activity of each of these disks, so that they can proactively detect an I/O latency and receive early warnings of inconsistencies in load-balancing across disks. The **Disk Performance** test aids administrators in this endeavor. This test auto-discovers the disks used by the NetApp Cluster and reports how well every disk processes the I/O requests. This way, potential I/O latencies can be isolated, and slow disks can be identified. In the process, the test turns the spotlight on irregularities in load-balancing.

Purpose	Auto-discovers the disks used by the NetApp Cluster and reports how well every disk processes the I/O requests
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not.

<table>
<tr><td></td><td colspan="3">
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.

In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.

10. EXCLUDE DISKS – If you wish to exclude certain disks from the scope of monitoring, specify a list of comma-separated aggregates in this text box. By default, none will be displayed here.

11. RECORDS PER CALL - The eG agent by default, executes the API commands in order to query the disks in the target environment. In critical infrastructures spanning large number of disks, a single execution by the eG agent may query (or download) a sizeable amount of monitoring data, thereby adding to the cluster load. To avoid this, you can tweak the RECORDS PER CALL parameter to enable the eG agent to obtain monitoring data iteratively in chunks instead of retrieving the entire amount of monitoring data in a single go. Say for example, the eG agent is required to query 1000 disks, then specifying the value 100 in this text box will enable the eG agent to query 100 disks at a time for 10 times to obtain monitoring data from all the disks. By default, the value of this parameter is 10.

12. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.

•
</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each aggregate on the NetApp Cluster being monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Consistency point reads:
Indicates the rate at which the read requests from the user are serviced during a Consistency Point (CP) operation in this disk.</td><td>Reads/Sec</td><td>A consistent decrease in the value of this measure could indicate that CP operations are slowing down the processing of read requests.</td></tr>
<tr><td>Consistency point read latency:
Indicates the time taken for retrieving data or metadata associated with user requests during a Consistency Point operation in this disk.</td><td>Secs</td><td></td></tr>
</table>

	Disk busy: Indicates the percentage of time there was atleast one outstanding request (i.e., read or write) to this disk.	Percent	A value greater than 70% is a cause of concern which indicates performance degradation of the disk. Comparing the percentage of time that the different disks are busy, an administrator can determine whether the application load is properly balanced across the different disks.
	Average IO request pending: Indicates the average number of I/O requests to this disk that were pending processing.	Number	A low value is desired for this measure. A gradual/sudden increase in the value of this measure may be due to the performance degradation of the disk, network congestion or a request on the disk that is taking too long to complete.
	Average IO request queued: Indicates the average number of I/O requests that are queued but are yet to be issued to this disk.	Number	
	Total transfers: Indicates the rate at which data transfer is being initiated from this disk.	Transfers/Sec	
	User read blocks: Indicates the rate at which the blocks are read from this disk upon a user request.	Blocks/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing read requests. Compare the value of this measure across disks to know which disks service block read requests slowly.
	User reads: Indicates the rate at which the read requests from the user are serviced by this disk.	Reads/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing read requests. Compare the value of this measure across the disks to know which disks service read requests slowly.
	User read latency: Indicates the average time taken to read a block from this disk upon a user request.	Secs	
	User write blocks: Indicates the rate at which the blocks are written to this disk upon a user request.	Blocks/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing write requests. Compare the value of this measure across disks to know which disks are servicing block write requests slowly.

	User writes: Indicates the rate at which the write requests from the user are serviced in this disk.	Writes/Sec	A consistent decrease in the value of this measure could indicate a bottleneck when processing write requests. Compare the value of this measure across disks to know which disks are servicing write requests slowly.
	User write latency: Indicates the average time taken to write a block to this disk upon a user request.	Secs	

1.3.5 Disk State Test

This test reports the current state of each disk in the NetApp Cluster. Using this test, you can easily figure out the the disks that currently offline, the disks that are currently in the *Replacing/Reconstructing/Failed* states.

Purpose	Reports the current state of each disk in the NetApp Cluster. Using this test, you can easily figure out the the disks that currently offline, the disks that are currently in the *Replacing/Reconstructing/Failed* states
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not.

<table>
<tr><td></td><td colspan="3">9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.

In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.

10. EXCLUDE DISKS – If you wish to exclude certain disks from the scope of monitoring, specify a list of comma-separated aggregates in this text box. By default, none will be displayed here.

11. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.

•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each disk on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Is failed?:

Indicates whether/not the status of this disk is Failed.</td><td></td><td>This measure reports a value Yes if the status of the disk is Failed and No if otherwise.

The values that this measure can report and their corresponding numeric values have been listed in the table below.

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
Note:

By default, this measure reports the above-mentioned Measure Values while indicating whether the status of this disk is Failed or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Is offline?:
Indicates whether/not the status of this disk is Offline.</td>
<td></td>
<td>This measure reports a value Yes if the disk is Offline and No if otherwise.

The values that this measure can report and their corresponding numeric values have been listed in the table below.

<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Yes</td><td>1</td></tr>
<tr><td>No</td><td>0</td></tr>
</table>
Note:

By default, this measure reports the above-mentioned Measure Values while indicating whether the status of this disk is Offline or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
<tr>
<td></td>
<td>Is prefailed?:
Indicates whether/not the status of this disk is Prefailed.</td>
<td></td>
<td>The disks that are manually failed due to excessive error logging are termed as Prefailed disks. The contents of these disks are copied into suitable replacement disks i.e., the spare disks available in the storage system.

This measure reports a value Yes if the status of the disk is Prefailed and No if otherwise.

The values that this measure can report and their corresponding numeric values have been listed in the table below.

<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Yes</td><td>1</td></tr>
<tr><td>No</td><td>0</td></tr>
</table>
Note:

By default, this measure reports the above-mentioned Measure Values while indicating whether the status of the disk is Prefailed or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Is reconstructing?:
Indicates whether/not the status of this disk is Reconstructing.</td>
<td></td>
<td>This measure reports a value Yes if the status of the disk is Reconstructing and No if otherwise.

The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Yes</td><td>1</td></tr>
<tr><td>No</td><td>0</td></tr>
</table>
Note:

By default, this measure reports the above-mentioned Measure Values while indicating whether the status of this disk is Reconstructing or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
</table>

	Is replacing?: Indicates whether/not the status of the disk is *Replacing*.		Mismatched disks that are part of an aggregate can be replaced with a more suitable spare disk without disrupting the data service. This process uses the Rapid RAID Recovery process to copy the data from the disk being replaced to a specified spare disk. Frequently replacing the disks will lead to the system degradation. Therefore, the frequent replacement of the disks needs to be avoided by proper initial configuration. This measure reports a value *Yes* if the status of the disk is *Replacing* and *No* if otherwise. The values that this measure can report and their corresponding numeric values have been listed in the table below. **Measure Value** / **Numeric Value**: Yes / 1; No / 0 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating whether this disk is a replacing disk or not. However, in the graph of this measure, **Measure Value**s will be represented using the corresponding numeric equivalents i.e., *0* or *1*.

1.4 The Cluster Vserver Layer

The tests associated with this layer (see Figure 1.6) monitor the nodes and Vservers of the NetApp Cluster and reports the following:

- How well the jobs of each job type have been processed? How many jobs have failed, succeeded, quit etc?
- What is the current state of the node and how well each node processes I/O requests?
- What is the current state of the Vserver peer relationship?
- What is the current state of the flash cache and is the cluster peer currently available?

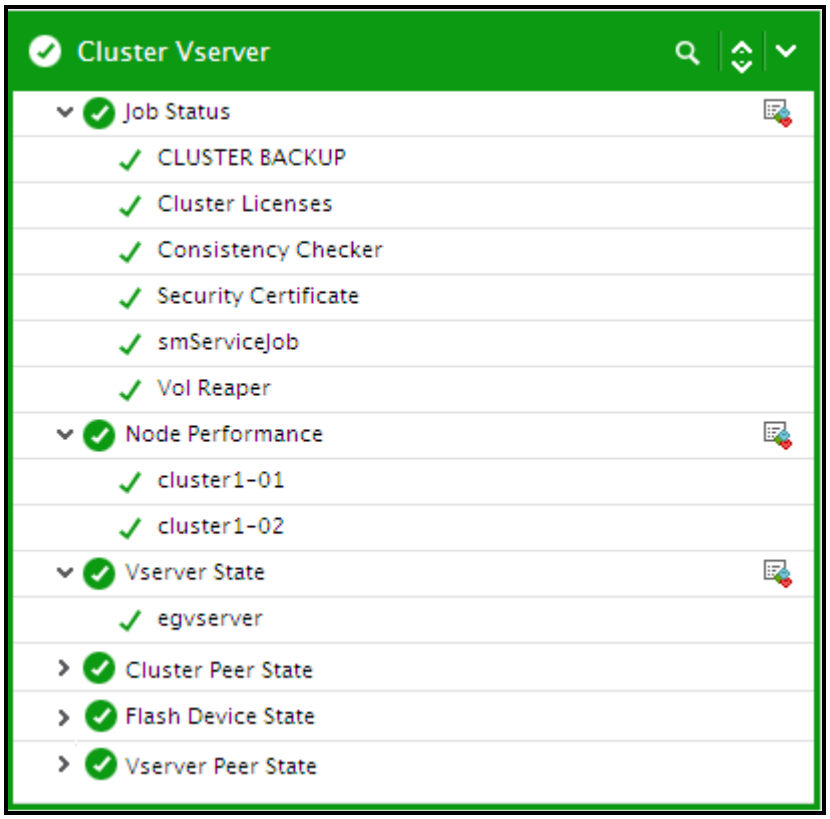

Figure 1.6: The tests mapped to the Cluster Vserver layer

1.4.1 Job Status Test

A job is any asynchronous task performed on the NetApp Cluster. Jobs are typically long-running volume operations such as copy, move, and mirror. You can monitor, pause, stop, and restart jobs, and configure them to run on specified schedules.

There are three categories of jobs that you can manage: server-affiliated, cluster-affiliated, and private.

A job can be in any of the following categories:

- **Server-Affiliated jobs:** These jobs are queued by the management framework to a specific node to be run.
- **Cluster-Affiliated jobs:** These jobs are queued by the management framework to any node in the cluster to be run.
- **Private jobs:** These jobs are specific to a node and do not use the replicated database (RDB) or any other cluster mechanism.

Jobs are placed into a job queue and run when resources are available. If the jobs in the job queue are not processed quickly, it would result in an overload condition characterized by long-winding job queues thus leading to the slowdown of the NetApp Cluster. In the event of such abnormalities, administrators will have to instantly figure out which type of jobs are contributing to the overload and why – is it because jobs of this type are failing frequently owing to errors? Or is it because the Cluster is not adequately configured to handle these jobs? The **Job Status** test helps administrators answer these questions!

This test auto-discovers the type of jobs in queue, and for each job type, reports the count of jobs that were successful, running, rescheduled, failed etc. This way, the test sheds light on job types that fail often, those that are taking too long to complete, and the probable reasons for the same.

Purpose	Auto-discovers the type of jobs in queue, and for each job type, reports the count of jobs that were successful, running, rescheduled, failed etc
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. 10. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.

<table>
<tr><td></td><td colspan="3">11. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
12. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
o The eG manager license should allow the detailed diagnosis capability
o 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 job type on the NetApp Cluster that is being monitored</td></tr>
<tr><td rowspan="6">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Success jobs:
Indicates the number of jobs of this job type that were completed successfully.</td><td>Number</td><td>A high value is desired for this measure.</td></tr>
<tr><td>Initial jobs:
Indicates the number of jobs of this job type that had been created but yet to be queued.</td><td>Number</td><td></td></tr>
<tr><td>Running jobs:
Indicates the number of jobs of this job type that ran upon picked by an instance of the Job Manager.</td><td>Number</td><td></td></tr>
<tr><td>Waiting jobs:
Indicates the number of jobs of this job type that were waiting for another job to complete.</td><td>Number</td><td>A high value for this measure is an indication of an endlessly running job which needs to be terminated failing which there may be a performance bottleneck.</td></tr>
<tr><td>Queued jobs:
Indicates the number of jobs of this job type that were queued for execution.</td><td>Number</td><td>Queued jobs could be run immediately or may be scheduled to run at a later time.</td></tr>
<tr><td>Pausing jobs:
Indicates the number of jobs of this job type that were in the process of pausing after being requested to pause.</td><td>Number</td><td></td></tr>
</table>

	Paused jobs: Indicates the number of jobs of this job type that were paused indefinetely.	Number	
	Quitting jobs: Indicates the number of jobs of this job type that had been requested to terminate and were shutting down.	Number	
	Quit jobs: Indicates the number of jobs of this job type that had been requested to terminate.	Number	
	Reschedule jobs: Indicates the number of jobs of this job type that were rescheduled.	Number	
	Error jobs: Indicates the number of times internal error occurred while processing the jobs of this job type.	Number	Ideally, the value of this measure should be zero. The detailed diagnosis of this measure if enabled, lists the name of the vServer, the name of the Job, the priority of the job, description of the job and the progress of the job.
	Failure jobs: Indicates the number of jobs of this job type that failed to execute.	Number	A low value is desired for this measure. The detailed diagnosis of this measure if enabled, lists the name of the vServer, the name of the Job, the priority of the job, description of the job and the progress of the job.
	Dead jobs: Indicates the number of jobs of this job type that exceeded the *drop dead time* and are being removed from the queue.	Number	The detailed diagnosis of this measure if enabled, lists the name of the vServer, the name of the Job, the priority of the job, description of the job and the progress of the job.
	Unknown jobs: Indicates the number of jobs of this job type that were in the *Unknown* state.	Number	The detailed diagnosis of this measure if enabled, lists the name of the vServer, the name of the Job, the priority of the job, description of the job and the progress of the job.
	Restart jobs: Indicates the number of jobs of this job type that were restarted.	Number	

	Dormant jobs: Indicates the number of jobs of this job type that were inactive while waiting on some external event.	Number	

1.4.2 Node Performance Test

A node is a controller in a cluster. You can group pairs of nodes together to form a scalable cluster. Creating a cluster enables the nodes to pool their resources and distribute work across the cluster, while presenting administrators with a single entity to manage. Clustering also enables continuous service to end users if individual nodes go offline.

A cluster can contain up to 24 nodes (unless the iSCSI or FC protocols are enabled, in which case the cluster can contain up to eight nodes). Each node in the cluster can view and manage the same volumes as any other node in the cluster. The total file-system namespace, which comprises all of the volumes and their resultant paths, spans the cluster.

When new nodes are added to a cluster, there is no need to update clients to point to the new nodes. The existence of the new nodes is transparent to the clients.

Periodically monitoring the state and I/O activity of each of the node in the NetApp Cluster enables you to rapidly detect I/O overloads and figure out the nodes that are inconsistent/offline. This is exactly where the **Node Performance** test helps!

This test auto-discovers the nodes on the NetApp Cluster, and periodically reports the following:

- What is the current state of the node?
- Which are the nodes that are busy processing I/O requests
- Is the I/O load activity uniform across all the nodes? Are any nodes overloaded with I/O read-write requests?

Purpose	Auto-discovers the nodes on the NetApp Cluster, and periodically reports the following: ➢ What is the current state of the node? ➢ Which are the nodes that are busy processing I/O requests ➢ Is the I/O load activity uniform across all the nodes? Are any nodes overloaded with I/O read-write requests?
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*.

	4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each node configured on the NetApp Cluster being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr><td rowspan="6">test</td><td>State:
Indicates the current state of this node.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unhealthy</td><td>0</td></tr><tr><td>Healthy</td><td>1</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current state of this node. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td></tr>
<tr><td>Total operations:
Indicates the rate at which all operations were performed on this node.</td><td>Ops/Sec</td><td></td></tr>
<tr><td>Write operations:
Indicates the rate at which the write operations were performed on this node.</td><td>Ops/Sec</td><td>A consistent decrease in the value of this measure could indicate a bottleneck when processing write requests. Compare the value of this measure across nodes to know which nodes are servicing write requests slowly.</td></tr>
<tr><td>Read operations:
Indicates the rate at which the read operations were performed on this node.</td><td>Ops/Sec</td><td>A consistent decrease in the value of this measure could indicate a bottleneck when processing read requests. Compare the value of this measure across nodes to know which nodes service read requests slowly.</td></tr>
<tr><td>HTTP operations:
Indicates the rate at which HTTP operations were performed on this node.</td><td>Ops/Sec</td><td>A consistent decrease in the value of this measure could indicate a bottleneck when processing HTTP requests. Compare the value of this measure across nodes to know which nodes service HTTP requests slowly.</td></tr>
<tr><td>Disk data read:
Indicates the rate at which data was read from the disk of this node.</td><td>MB/Sec</td><td>Comparing the value of this measure across nodes will help you identify the node that is the slowest in terms of reading the data from the disk.</td></tr>
</table>

	Net data received: Indicates the rate at which network data is received on this node.	MB/Sec	
	Net data sent: Indicates the rate at which network data is sent through this node.	MB/Sec	
	Average system latency: Indicates the average time taken by the system to perform operations through this node.	Secs	A high value for this measure is a cause of concern.

1.4.3 Vserver State Test

A virtual storage server (Vserver) contains data volumes and one or more Logical interfaces (LIFs) through which it serves data to the clients. Starting with clustered Data ONTAP 8.1.1, a Vserver can either contain one or more FlexVol volumes, or a single Infinite Volume.

A Vserver securely isolates the shared virtualized data storage and network, and appears as a single dedicated server to its clients. Each Vserver has a separate administrator authentication domain and can be managed independently by a Vserver administrator.

In a cluster, Vserver facilitates data access. A cluster must have at least one Vserver to serve data.

Vservers use the storage and network resources of the cluster. However, the volumes and LIFs are exclusive to the Vserver. Multiple Vservers can coexist in a single cluster without being bound to any node in a cluster. However, they are bound to the physical cluster on which they exist.

A cluster can have one or more Vservers with FlexVol volumes and Vservers with Infinite Volumes.

A NetApp Cluster contains the following types of Vservers:

- Admin Vserver
- Node Vserver
- Data Vserver

Vservers provide data access to clients without regard to physical storage or controller, similar to any storage system. When you use Vservers, they provide benefits such as nondisruptive operation, scalability, security and support unified storage. Therefore, continuous availability of the Vserver is essential so that there does not exist any disrutipon in the data transfer and hence, it becomes imperative to monitor the state of the Vservers. This is exactly how the **Vserver State** test helps!

This test auto-discovers the Vservers configured on the NetApp Cluster and reports the current state of each Vserver.

Purpose	Auto-discovers the Vservers configured on the NetApp Cluster and reports the current state of each Vserver
Target of the test	A NetApp Cluster

Agent deploying the test	An external/remote agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each Vserver on the NetApp Cluster being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>test</td>
<td>State:
Indicates the current state of this Vserver.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Running</td><td>0</td></tr>
<tr><td>Starting</td><td>1</td></tr>
<tr><td>Initializing</td><td>2</td></tr>
<tr><td>Stopping</td><td>3</td></tr>
<tr><td>Stopped</td><td>4</td></tr>
<tr><td>Deleting</td><td>5</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current state of this Vserver. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 to 5.</td>
</tr>
</table>

1.4.4 Cluster Peer State Test

The cluster peer feature in the clustered DATA ONTAP allows two clusters to coordinate and share resources between them. You can create data protection mirroring relationships from one cluster to another and you can manage the jobs on a remote cluster from another cluster if you have cluster peer relationships. You connect clusters together in a cluster peer relationship to share information and to provide access to operations on the peer cluster. Therefore it becomes important to monitor the availability of the cluster peer on the NetApp Cluster. This can be achieved using the **Cluster Peer State** test!

For each Cluster peer on the NetApp Cluster, this test reports whether/not the cluster peer is available.

Purpose	For each Cluster peer on the NetApp Cluster, this test reports whether/not the cluster peer is available
Target of the test	A NetApp Cluster
Agent deploying the test	An external/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 controller cluster.
3. PORT – The port number at which the specified HOST listens to. By default, this is NULL.
4. USER – Here, specify the name of the user who possesses the readonly role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document.
5. PASSWORD - Specify the password that corresponds to the above-mentioned USER.
6. CONFIRM PASSWORD – Confirm the PASSWORD by retping it here.
7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each Cluster peer on the NetApp Cluster being monitored</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>Availability?:
Indicates whether/not this Cluster peer is available.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Available</td><td>0</td></tr><tr><td>Unavailable</td><td>1</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values while indicating whether this Cluster peer is available or not. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
</table>

1.4.5 Flash Device State Test

A Flash Cache 2, Flash Cache, or Performance Acceleration Module (PAM) PCIe-based, memory module optimizes the performance of random read-intensive workloads by functioning as an intelligent external read cache. This hardware works in tandem with the WAFL External Cache software component of Data ONTAP. Flash Cache speeds data access through intelligent caching of recently read user data or NetApp metadata. Flash Cache works with all NetApp storage protocols and software, enabling you to:

- Increase I/O throughput by up to 75% thus eliminating performance bottlenecks
- Use up to 75% fewer disk drives without compromising performance
- Increase e-mail users by up to 67% without adding disk drives
- Lower costs—use SATA drives with Flash Cache for important workloads.
- Save power, cooling & rack space by using fewer, larger hard disk drives.

This test monitors the current state of each Flash Cache installed on the NetApp Cluster and reports the percentage of Flash Cache that is currently online.

Purpose	Monitors the current state of each Flash Cache installed on the NetApp Cluster and reports the percentage of Flash Cache that is currently online
Target of the test	A NetApp Cluster
Agent deploying the test	An external/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 controller cluster.
3. PORT – The port number at which the specified HOST listens to. By default, this is NULL.
4. USER – Here, specify the name of the user who possesses the readonly role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document.
5. PASSWORD - Specify the password that corresponds to the above-mentioned USER.
6. CONFIRM PASSWORD – Confirm the PASSWORD by retping it here.
7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each aggregate on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr><td rowspan="2">test</td><td>State:
Indicates the current state of this Flash Cache.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Online</td><td>0</td></tr><tr><td>Offline_failed</td><td>1</td></tr><tr><td>Offline_threshold</td><td>2</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current status of a Flash Cache. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 to 2.</td></tr>
<tr><td>Online:
Indicates the percentage of Flash Cache capacity that is currently online.</td><td>Percent</td><td>A high value is desired for this measure.</td></tr>
</table>

1.4.6 Vserver Peer State Test

Vserver peer relationship is an authorization infrastructure that enables a cluster administrator to set up peering applications such as SnapMirror relationships between Vservers either existing within a cluster (intracluster) or in the peered clusters (intercluster). Only a cluster administrator can set up Vserver peer relationships.

Vserver peer infrastructure enables you to set up a backup and recovery mechanism between Vservers. You can set up mirroring relationship at volume level between peered Vservers. If a Vserver's volume becomes unavailable, the cluster administrator or a Vserver administrator can configure the respective mirrored volume of the peered Vserver to serve data.

One Vserver can be peered with multiple Vservers within a cluster or across clusters. In clustered Data ONTAP 8.2, only SnapMirror data protection (DP), vault (XDP) and load-sharing relationship (LS) relationships can be set up by using the Vserver peer infrastructure.

For a hassle free data transfer through the NetApp Cluster, administrators need to constantly monitor the state of the Vserver peer relationship failing which administrators may not be able to figure out the Vserver through which data transfer stopped abruptly. The **Vserver Peer State** test exactly helps the administrators achieve this!

This test auto-discovers the Vservers on the NetApp Cluster and reports the current state of the Vserver peer relationship for each Vserver.

Purpose	Auto-discovers the Vservers on the NetApp Cluster and reports the current state of the Vserver peer relationship for each Vserver
Target of the test	A NetApp Cluster

Agent deploying the test	An external/remote agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each local *Vserver:peered Vserver* on the NetApp Cluster being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr>
<td>test</td>
<td>State:
Indicates the current state of this Vserver peer relationship.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th><th>Description</th></tr>
<tr><td>Peered</td><td>1</td><td>Indicates either one of the following:
➢ An intercluster Vserver peer relationship is accepted from the peered cluster.
➢ An intracluster Vserver peer relationship is established.
➢ An intercluster or intracluster Vserver peer relationship is resumed.</td></tr>
<tr><td>Pending</td><td>2</td><td>An intercluster Vserver peer relationship is requested from the local cluster.</td></tr>
<tr><td>Initializing</td><td>3</td><td>The local cluster is communicating with the peer cluster for initializing the Vserver peer relationship.</td></tr>
<tr><td>Initiated</td><td>4</td><td>An intercluster Vserver peer relationship is requested from the local cluster.</td></tr>
<tr><td>Deleted</td><td>5</td><td>An intercluster Vserver peer relationship isdeleted from any of the peered clusters.</td></tr>
<tr><td>Suspended</td><td>6</td><td>An intercluster or intracluster Vserver peer relationship is suspended from the local or peered cluster.</td></tr>
<tr><td>Rejected</td><td>7</td><td>An intercluster Vserver peer relationship is rejected from the peered cluster.</td></tr>
</table>
</td>
</tr>
</table>

			Note: By default, this measure reports the above-mentioned **Measure Value**s while indicating the current state of this Vserver peer. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., *1 to 7*.

1.5 The Netapp Access Layer

To monitor the load imposed by iSCSI connections, the load through the FC ports and the logical interfaces to the NetApp Cluster and to understand how well/poorly the NetApp Cluster handles this load, use the tests mapped to this layer.

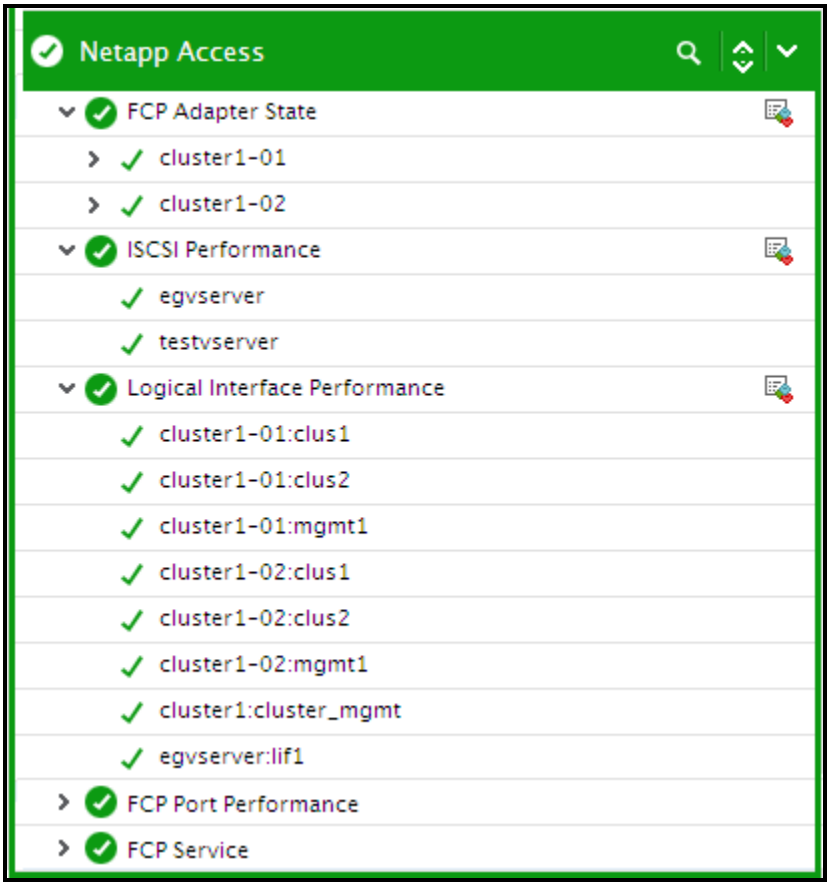

Figure 1.7: The tests mapped to the NetApp Access layer

1.5.1 FCP Adapter State Test

This test instantly detects changes in the overall health, state/mode of the Fiber Channel Adapter and immediately notifies administrators of the errors/problem conditions experienced by the Fiber Channel Adapter.

Purpose	Instantly detects changes in the overall health, state/mode of the Fiber Channel Adapter and immediately notifies administrators of the errors/problem conditions experienced by the Fiber Channel Adapter
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •
Outputs of the test	One set of results for each Host Bus Adapter on the NetApp Cluster being monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>State:
Indicates the current state of this Fiber Channel Adapter.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Startup</td><td>0</td></tr><tr><td>Online</td><td>1</td></tr><tr><td>Initializing firmware</td><td>2</td></tr><tr><td>Waiting for link up</td><td>3</td></tr><tr><td>Uninitialized</td><td>4</td></tr><tr><td>Resetting</td><td>5</td></tr><tr><td>Link not connected</td><td>6</td></tr><tr><td>Link disconnected</td><td>7</td></tr><tr><td>Offlined by user/system</td><td>8</td></tr><tr><td>Offline</td><td>9</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current state of this Fiber Channel Adapter. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 to 9.</td></tr>
</table>

1.5.2 ISCSI Performance Test

The iSCSI protocol is a licensed service on the storage system that enables you to transfer block data to hosts using the SCSI protocol over TCP/IP. The iSCSI protocol standard is defined by RFC 3720. In an iSCSI network, storage systems are targets that have storage target devices, which are referred to as LUNs (logical units). A host with an iSCSI host bus adapter (HBA), or running iSCSI initiator software, uses the iSCSI protocol to access LUNs on a storage system. The iSCSI protocol is implemented over the storage system's standard gigabit Ethernet interfaces using a software driver. The connection between the initiator and target uses a standard TCP/IP network. No special network configuration is needed to support iSCSI traffic. The network can be a dedicated TCP/IP network, or it can be your regular public network. The storage system listens for iSCSI connections on TCP port 3260.

This test monitors the active and attempted iSCSI sessions on each VServer hosting the iSCSI service on the NetApp Cluster, and promptly captures the processing ability, login failures, failed tasks, and errors encountered by these sessions.

Purpose	Monitors the active and attempted iSCSI sessions on each VServer hosting the iSCSI service on the NetApp Cluster, and promptly captures the processing ability, login failures, failed tasks, and errors encountered by these sessions
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default.

	In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each Vserver hosting the iSCSI service on the NetApp Cluster being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Command descriptor blocks processed:** Indicates the rate at which the Command Descriptor Blocks were processed by the inititator.	Blocks/Sec	The SCSI Command Descriptor Block (CDB) is a block of information that describes the command. Commands are sent from SCSI Initiators, which are contained in host computers, to SCSI Targets, which are controllers of some type of storage device (hard disk, tape drive, etc.). Almost every CDB contains 3 parts: ➢ a "What" field, ➢ a "Where" field, and ➢ a "How Much" field. For some commands, these fields are implied or not required. The "What" field is called the Operation Code (or OpCode) and tells the target what the command is supposed to do. A couple of examples would be READ or WRITE. The READ command moves data from the storage device to the host system, while the WRITE command moves data to the storage device for later access. The "Where" field tells the target where to begin the operation and is expressed as a Logical Block Address, or LBA. This address ranges from zero (0) to the maximum address of the device. Some commands, such as INQUIRY, do not require this field. The "How Much" field tells the target how many blocks (or bytes) or data to move. The block size of most storage devices is 512 bytes, but in certain storage devices, the block size can be different. This field is expressed as either Transfer Length (in blocks), Allocation Length (bytes moving to the host), or Parameter List Length (bytes moving to the device). Which name is used depends on the command itself. CDBs come in various sizes, typically 6, 10, 12, or 16 bytes total. Below is a figure of a 10-byte READ command to be sent to a hard drive. This command, if successful, will move one block (512 bytes) of data to the host computer system, from logical block address 100h (hex). All other bits or fields that are not labeled are set to zero. This measure is a good indicator for analyzing the traffic/load in this cluster.

	Successfully processed command descriptor blocks: Indicates the rate at which the Command Descriptor Blocks were successfully executed by the initiator.	Blocks/Sec	A high value is desired for this measure. A low value indicates that there were too many unsuccessful CDB executions, which may have caused a processing bottleneck.
	Command descriptor blocks with errors: Indicates the rate at which the Command Descriptor Blocks were processed by the initiators with errors.	Errors/Sec	Ideally, the value of this measure should be 0. A high value indicates that there were too many errors that occurred while processing the CDBs which may affect the performance of the storage system. Some of the common errors that occur while the CDBs are processed include the medium/hardware errors, providing illegal parameters for the CDB, accessing unauthorized data, volume overflow etc.
	Total errors: Indicates the rate at which the iSCSI errors occurred.	Errors/Sec	Ideally, the value of this measure should be 0. Some of the common iSCSI errors that occur are digest errors, login/logout errors, PDU errors etc.
	Failed logins: Indicates the rate at which failed login attempts were made by the initiator while creating new iSCSI sessions.	Logins/Sec	Ideally, the value of this measure should be 0.
	Failed logouts: Indicates the rate at which logouts failed while attempting to gracefully end the iSCSI sessions.	Logouts/Sec	Ideally, the value of this measure should be 0.
	Failed tasks: Indicates the rate at which iSCSI tasks failed.	Tasks/Sec	
	Protocol errors: Indicates the rate at which protocol errors occurred.	Errors/Sec	Ideally, the value of this measure should be 0. Protocol errors mainly occur due to the violation of protocol rules. The protocol errors occur in scenarios like violation of iSCSI PDU exchange sequences, duplication of protocol steps, invalid format/entries in protocol messages etc.

	Login requests: Indicates the rate at which login requests were made.	Requests/Sec	This measure is an actual indicator of the users who are attempting to login to the storage system. Compare this value with the *Failed logins* measure to find out how well the user requests are processed in this storage system.
	Logout requests: Indicates the rate at which the logout requests were made.	Requests/Sec	This measure is an actual indicator of the users who are attempting to logout of the storage system. Compare this value with the *Failed logouts* measure to find out how well the user requests are processed in this storage system.
	Protocol Data Units rejected: Indicates the rate at which Protocol Data Units were rejected by the initiator.	Units/Sec	In a layered system such as iSCSI, a unit of data which is specified in a protocol of a given layer and which consists of protocol-control information and possibly user data of that layer is termed as a Protocol Data Unit. Ideally, the value of this measure should be 0. The Protocol Data Units are rejected due to iSCSI error conditions such as protocol errors, unsupported option etc., which may lead to connection/data loss, performance/processing bottleneck on the storage system etc.

1.5.3 Logical Interface Performance Test

A logical interface is an IP address associated with a physical network port on the NetApp Cluster. For logical interfaces using NAS data protocols, the interface can fail over or be migrated to a different physical port in the event of component failures, thereby continuing to provide network access despite the component failure.

This test auto-discovers the logical interfaces and for each logical interface, this test, promptly captures the processing ability, errors encountered during data transmission/reception and the uptime of the interface.

Purpose	Auto-discovers the logical interfaces and for each logical interface, this test, promptly captures the processing ability, errors encountered during data transmission/reception and the uptime of the interface
Target of the test	A NetApp Cluster
Agent deploying the test	An external/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 controller cluster.
3. PORT – The port number at which the specified HOST listens to. By default, this is NULL.
4. USER – Here, specify the name of the user who possesses the readonly role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document.
5. PASSWORD - Specify the password that corresponds to the above-mentioned USER.
6. CONFIRM PASSWORD – Confirm the PASSWORD by retping it here.
7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each logical interface on the NetApp Cluster being monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Data received:
Indicates the rate at which data was received by this logical interface.</td><td>MB/Sec</td><td></td></tr>
<tr><td>Received errors:
Indicates the rate at which erorrs occurred while receiving data through this logical interface.</td><td>Errors/Sec</td><td>Ideally, the value of this measure should be zero.</td></tr>
</table>

	Packets received: Indicates the rate at which the data packets were received by this logical interface.	Packets/Sec	
	Data sent: Indicates the rate at which data was sent through this logical interface.	MB/Sec	
	Sent errors: Indicates the rate at which errors occurred while sending data through this logical interface.	Errors/Sec	Ideally, the value of this measure should be 0.
	Packets sent: Indicates the rate at which data packets were sent through this logical interface.	Packets/Sec	
	Uptime: Indicates the total time duration for which this logical interface has been up.	Mins	
	Uptime since last measure: Indicates the time duration for which this logical interface has been up since the last measurement period.	Secs	

1.5.4 FCP Port Performance Test

A Fibre Channel (FC) port is a hardware pathway into and out of a node that performs data communication over an FC link i.e., an FC Channel. The FC ports therefore are the primary handlers of I/O requests from the NetApp Cluster. I/O load on the ports directly translate into load on the volumes of the cluster. This is why, administrators need to continuously monitor the data and read/write latency on each port, so that overloaded ports can be quickly identified and the load-balancing algorithim fine-tuned accordingly. Moreover, since port-related errors can deny hosts access to the data stored in the NetApp Cluster, port monitoring is imperative to enable administrators to quickly detect such errors and fix them to ensure the normal functioning of the cluster. This can be achieved using the **FCP Port Performance** test! For each FC port on the NetApp Cluster, this test reports the rate at which data and I/O requests are handled and the number and nature of errors/failures encountered by each FC port. This way, administrators can be proactively alerted to potential port overloads and error conditions (with FC ports), and thus enabled to rapidly initiate remedial measures to avoid an impending system slowdown.

Purpose	For each FC port on the NetApp Cluster, this test reports the rate at which data and I/O requests are handled and the number and nature of errors/failures encountered by each FC port
Target of the	A NetApp Cluster

<table>
<tr><td>test</td><td colspan="3"></td></tr>
<tr><td>Agent deploying the test</td><td colspan="3">An external/remote agent</td></tr>
<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 controller cluster.
3. PORT – The port number at which the specified HOST listens to. By default, this is NULL.
4. USER – Here, specify the name of the user who possesses the readonly role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document.
5. PASSWORD - Specify the password that corresponds to the above-mentioned USER.
6. CONFIRM PASSWORD – Confirm the PASSWORD by retping it here.
7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each FC port on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Other latency:
Indicates the average time taken to perform operations other than read and write through this port.</td><td>Secs</td><td></td></tr>
</table>

	Other operations: Indicates the rate at which operations other than read and write are performed through this port.	Ops/Sec	
	Read operations: Indicates the rate at which data/block is read through this port.	Ops/Sec	Very high values for these measures are indicative of the existence of road-blocks to rapid reading/writing by the storage device through the port. By observing the variations in these measures over time, you can understand whether the latencies are sporadic or consistent on the port. Consistent delays in reading/writing could indicate that there are persistent bottlenecks (if any) in the port which helps you identify the over-utilized ports.
	Read latency: Indicates the average time to read a block/data through this port upon a user request.	Secs	
	Write operations: Indicates the rate at which data/block is written through this port.	Ops/Sec	
	Write latency: Indicates the average time taken to write a block/data using this port upon a user request.	Secs	
	Authentication failures: Indicates the number of times authentication failure occurred on this port.	Number	
	Link down: Indicates the number of times the Fiber Channel link was lost.	Number	

	Loop failures at receiver: Indicates the number of loop failures detected at the receiver of this FC port.		Loop Initialization is an essential process for allowing new devices onto the loop, assigning Aribrated Loop Physical Addresses (AL_PAs), providing notification of topology changes, and recovering from loop failure. Following loop initilaization, the loop enters a stable monitoring mode and resumes normal activity. Depending on the number of normal ports (NL_Ports) attached to the loop, an entire loop initialization may take a few milliseconds. A loop initialization can be triggered by a number of causes, the most common being the introduction of a new device. The new device could actually be a former device that has been powered on, or an active device that has been moved from one hub port to another. A number of ordered sets have been defined to cover the various conditions that an NL_port may sense as it launches the initialization process. These ordered sets, called **loop initialization primitive** sequences, are referred to collectively as LIPs. An NL_Port issues atleast 12 LIPs to start loop initialization. During loop initialization, each downstream device that are part of the loop receives the LIP stream and enters a state known as **Open-init**, which suspends any current operations and prepares the device for the loop initialization procedure. The LIPs are forwarded along the loop until all NL_ports, including the originator of the loop, are in **Open-init** state. At this point, a **temporary loop master** is selected for conducting the rest of the initialization procedure. The first task of the temporary loop master is to issue a series of four frames that will allow each device on the loop to select a *unique* AL_PA. A LIP reset is used to perform a vendor specific reset at the loop port specified by this AL-PA value. These LIP resets are used to temporarily cure connectivity issues. Prolonged resets should be noted and the underlying actual connectivity issues should be resolved.
	Loop initialization error: Indicates the number of loop initialization errors that occurred on this FC port.	Number	Ideally, the value of this measure should be zero.

	Loss of signal: Indicates the number of times the signal was lost on this FC port.	Number	Ideally, the value of this measure should be zero. A non-zero value for this measure indicates that the port detected a loss of the electrical or optical signal used to transfer data on the port. This is likely an indicator for a faulty connector or cable. These are also caused when the device connected to the port is restarted, replaced or being serviced when the Fibre Channel cable connected to the port is temporarily disconnected. If the port is in the "loss of signal" state for longer than a specific period, the port will get into the link failure state which could degrade the performance of the Fibre Channel link.
	Loss of sync: Indicates the number of times this FC port failed to synchronize.	Number	Ideally, the value of this measure should be zero. A non-zero value for this measure indicates that port went into the "loss of synchronization" state, where it encountered continuous Disparity errors. This is likely an indicator for a faulty connector or cable. These are also caused when the device connected to the port is restarted, replaced or being serviced when the Fibre Channel cable connected to the port is temporarily disconnected. If the port is in the "loss of synchronization" state for longer than a specific period, the port will get into the link failure state which could degrade the performance of the Fibre Channel link.
	Primitive sequence error: Indicates the number of Primitive Sequence protocol errors that occurred on this FC port.	Number	Ideally, the value of this measure should be zero.
	Spurious interrupts: Indicates the number of spurious signals received by this FC port.	Number	
	Virtual link down: Indicates the number of times the virtual Fiber channel link was lost on this FC port.	Number	Ideally, the value of this measure should be zero. A non-zero value for this measure indicates that the port detected a loss of the electrical or optical signal used to transfer data on the port.

1.5.5 FCP Service Test

The **fcp** family of commands manages the Fibre Channel Target adapters and the FCP target protocol. These commands can start and stop FCP target service, bring target adapter ports up and down, show protocol statistics, and list client adapters connected to the controller on the target NetApp Cluster. If the FCP service is stopped or is currently not available, then all FC ports on the NetApp Cluster are disabled, thus leading to ramification of the HA pairs during cluster failover. For example, if you stop the FCP service on System 1, and System 2 fails over, then System 1 will be unable to service the LUNs of System 2. On the other hand, if System 2 fails over, and you stop the FCP service on System 2 and start the FCP service on System 1, System 1 will successfully service the LUNs of System 2. It is therefore imperative to monitor the status of the FCP service so that any glitch to service the data during cluster failover can be proactively avoided. The **FCP Service** test helps you achieve this!

This test reports the availability of the FCP service and proactively alerts the administrators of possible problems if the FCP service is not available.

Purpose	Reports the availability of the FCP service and proactively alerts the administrators of possible problems if the FCP service is not available
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. 10. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.

<table>
<tr><td></td><td colspan="3">11. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each FCP Service on the NetApp Cluster being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Availability:
Indicates whether/not this FCP service is currently available.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Available</td><td>0</td></tr><tr><td>Unavailable</td><td>1</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating whether this FCP service is available or not. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td></tr>
</table>

1.6 The File Access Protocols Layer

The test mapped to this layer monitors the CIFS operations on the NetApp Cluster and reports I/O processing bottlenecks (if any).

Figure 1.8: The tests mapped to the File Access Protocol layer

1.6.1 CIFS Performance Test

The NetApp Cluster exports data as files through two primary protocols, NFS and CIFS, which correspond to the UNIX and Windows processes.

Key features that CIFS offers are:

- **File Access with integrity**: CIFS supports the usual set of file operations; open, close, read, write and seek.

CIFS also supports file and record lock and unlocking. CIFS allows multiple clients to access and update the same file while preventing conflicts by providing file sharing and file locking.

- **Optimization for Slow Links**: The CIFS protocol has been tuned to run well over slow-speed dial-up lines. The effect is improved performance for users who access the Internet using a modem.
- **Security**: CIFS servers support both anonymous transfers and secure, authenticated access to named files. File and directory security policies are easy to administer.
- **Performance and Scalability**: CIFS servers are highly integrated with the operating system, and are tuned for maximum system performance. CIFS supports all Microsoft platforms after Windows 95. It also supports other popular operation systems such as Unix, VMS, Macintosh, IBM LAN server etc.
- **Unicode File Names**: File names can be in any character set, not just character sets designed for English or Western European languages. Global File Names: Users do not have to mount remote file systems, but can refer to them directly with globally significant names, instead of ones that have only local significance.

By continuously monitoring the read/write operations performed through the CIFS protocol, the **CIFS Performance** test promptly provides you with a heads-up on probable latencies in the processing of I/O requests.

Purpose	By continuously monitoring the read/write operations performed through the CIFS protocol, this test promptly provides you with a heads-up on probable latencies in the processing of I/O requests
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default.

	In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each aggregate on the NetApp Cluster being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	CIFS operations: Indicates the rate at which operations were performed by users through CIFS protocol to access this NetApp Cluster.	Ops/Sec	
	CIFS latency: Indicates the average time taken for performing the operations using the CIFS protocol.	Secs	A low value is desired for this measure.
	CIFS read operations: Indicates the rate at which the read operations are performed across all LUNs of this cluster through the CIFS protocol.	Ops/Sec	Very high values for these measures are indicative of the existence of road-blocks to rapid reading/writing by the storage device. By observing the variations in these measures over time, you can understand whether the latencies are sporadic or consistent. Consistent delays in reading/writing could indicate that there are persistent bottlenecks (if any) in the storage device to speedy I/O processing.
	CIFS read latency: Indicates the average time taken to perform read operations across all LUNs through the CIFS protocol.	Secs	
	CIFS write operations: Indicates the rate at which the write operations were performed across all LUNs of this cluster through the CIFS protocol.	Ops/Sec	
	CIFS write latency: Indicates the average time taken to perform write operations across all LUNs through the protocol.	Secs	

1.7 The Logical Storage Layer

Using the tests associated with this layer, the following can be monitored:

- Usage of volumes to isolate the over-used and overloaded volumes;
- Disk and file usage quotas
- Space usage in LUNs
- Usage of LUNs to isolate the LUN that is used excessively

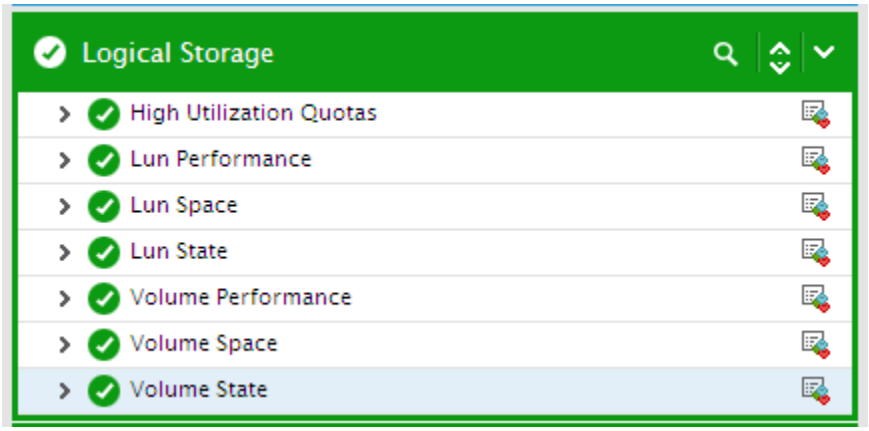

Figure 1.9: The tests mapped to the Logical Storage layer

1.7.1 High Utilization Quotas Test

Quotas are specified for the following reasons:

- To limit the amount of disk space or the number of files that can be used by a user or group, or that can be contained by a qtree.
- To track the amount of disk space or the number of files used by a user, group, or qtree, without imposing a limit.
- To warn users when their disk usage or file usage is high

You specify quotas using the */etc/quotas* file. Quotas are applied to a specific volume or qtree.

When Data ONTAP receives a request to write to a volume, it checks to see whether quotas are activated for that volume. If so, Data ONTAP determines whether any quota for that volume (and, if the write is to a qtree, for that qtree) would be exceeded by performing the write operation. If any hard quota would be exceeded, the write operation fails, and a quota notification is sent. If any soft quota would be exceeded, the write operation succeeds, and a quota notification is sent.

This test reports the number of Windows/Unix users and Unix user groups that crossed the disk space (both hard and soft) and file usage quotas set. With the help of these metrics, you can promptly detect abnormal disk space and file usage at the volume/qtree-level.

Purpose	Reports the number of Windows/Unix users and Unix user groups that crossed the disk space (both hard and soft) and file usage quotas set
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. 10. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 11. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.

<table>
<tr><td></td><td colspan="3">12. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
o The eG manager license should allow the detailed diagnosis capability
o 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 type of quota set at the volume/qtree-level</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Quotas:
Indicates the number of quotas of this type.</td><td>Number</td><td>The detailed diagnosis of this measure indicates whether the quota has been set for a user/group/qtree, the target of the quota, the volume on which the quota is applied, the qtree on which the quota is applied, the percentage of disk limit used, the percentage of file limit used, and the number of windows users, unix users and unix group users who violated each type of quota.</td></tr>
<tr><td>Windows users:
Indicates the number of windows users involved in quota violation of this quota type.</td><td>Number</td><td rowspan="3">Ideally, the value of these measures should be low. A high value indicates that there is space constraint in the disk/volume/LUN which in turn will affect the users who are accessing them.</td></tr>
<tr><td></td><td>Unix users:
Indicates the number of unix users involved in quota violation of this quota category.</td><td>Number</td></tr>
<tr><td></td><td>Unix groups:
Indicates the number of unix groups involved in quota violation of this quota category.</td><td>Number</td></tr>
</table>

1.7.2 Lun Performance Test

This test auto-discovers the LUNs configured on the NetApp Cluster, monitors the processing ability of each LUN, and reports the following:

- Is I/O load uniformly balanced across all LUNs, or is any LUN overloaded?

- Are the LUNs able to process the I/O requests quickly? Is any LUN experiencing processing bottlenecks?
- How many errors are encountered by each LUN?

Purpose	This test auto-discovers the LUNs configured on the NetApp Cluster, monitors the processing ability of each LUN, and reports the following: ➢ Is I/O load uniformly balanced across all LUNs, or is any LUN overloaded? ➢ Are the LUNs able to process the I/O requests quickly? Is any LUN experiencing processing bottlenecks? ➢ How many errors are encountered by each LUN?
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. 10. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.

<table>
<tr><td></td><td colspan="3">11. EXCLUDE LUNS – If you wish to exclude certain LUNs from the scope of monitoring, specify a list of comma-separated LUNs in this text box. By default, none will be displayed here.
12. RECORDS PER CALL - The eG agent by default, executes the API commands in order to query the LUNs in the target environment. In critical infrastructures spanning large number of LUNs, a single execution by the eG agent may query (or download) a sizeable amount of monitoring data, thereby adding to the cluster load. To avoid this, you can tweak the RECORDS PER CALL parameter to enable the eG agent to obtain monitoring data iteratively in chunks instead of retrieving the entire amount of monitoring data in a single go. Say for example, the eG agent is required to query 1000 LUNs, then specifying the value 100 in this text box will enable the eG agent to query 100 LUNs at a time for 10 times to obtain monitoring data from all the LUNs. By default, the value of this parameter is 10.
13. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each LUN configured on the NetApp Cluster being monitored</td></tr>
<tr><td rowspan="6">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Other operations:
Indicates the rate at which operations other than read and write were performed on this LUN.</td><td>Ops/Sec</td><td></td></tr>
<tr><td>Read operations:
Indicates the rate at which the read operations were performed on this LUN.</td><td>Ops/Sec</td><td>A high value is desired for this measure. A consistent decrease in this value could indicate a processing bottleneck.</td></tr>
<tr><td>Write operations:
Indicates the rate at which the write operations were performed to this LUN.</td><td>Ops/Sec</td><td>A high value is desired for this measure. A consistent decrease in this value could indicate a processing bottleneck.</td></tr>
<tr><td>Average latency:
Indicates the average time taken for executing an operation in this LUN.</td><td>Secs</td><td>A high value indicates that the LUN is taking too long to process the I/O requests to it.
Compare the value of this measure across LUNs to isolate the slow LUNs.</td></tr>
<tr><td>Average read latency:
Indicates the average time taken to execute a read request in this LUN.</td><td>Secs</td><td>A low value is desired for this measure. A high value indicates that the requests take too long to execute which directly affects the performance of the LUNs.</td></tr>
</table>

	Average write latency: Indicates the average time taken to execute a write request in this LUN.	Secs	
	Scsi errors: Indicates the total number of SCSI errors encountered on this LUN.	Number	Ideally, the value of this measure should be zero.

1.7.3 Lun Space Test

This test auto-discovers the LUNs configured on the NetApp Cluster, monitors the space utilization of each LUN, and proactively alerts administrators on potential space crunch on the LUNs.

Purpose	Auto-discovers the LUNs configured on the NetApp Cluster, monitors the space utilization of each LUN, and proactively alerts administrators on potential space crunch on the LUNs
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default.

	In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **EXCLUDE LUNS –** If you wish to exclude certain LUNs from the scope of monitoring, specify a list of comma-separated LUNs in this text box. By default, *none* will be displayed here. 11. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each LUN configured on the NetApp Cluster being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total space: Indicates the total size of this LUN.	GB	
	Available space: Indicates the space that is currently available for use in this LUN.	GB	A high value is desired for this measure. If the value of this measure is decreasing gradually, then it indicates that the LUN is currently running out of space.
	Max used space: Indicates the maximum space used by this LUN.	GB	If the value of this measure is close to that of the *Total space* measure, it indicates potential space crunch in the LUN. Administrators may increase the size of the LUN so that the space utilization of the LUN is optimal.
	Percentage max used space: Indicates the percentage of maximum space used by this LUN.	Percent	A high value for this measure indicates that the LUN is running out of space.

1.7.4 Lun State Test

This test auto-discovers the LUNs configured on the NetApp Unified Storage system and monitors the current state of each LUN. In addition, this test will report the alignment state of each available LUN.

Purpose	Auto-discovers the LUNs configured on the NetApp Unified Storage system and monitors the current state of each LUN. In addition, this test will report the alignment state of each available LUN
Target of the test	A NetApp Cluster
Agent deploying the	An external/remote agent

<table>
<tr><td>test</td><td colspan="3"></td></tr>
<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 controller cluster.
3. PORT – The port number at which the specified HOST listens to. By default, this is NULL.
4. USER – Here, specify the name of the user who possesses the readonly role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document.
5. PASSWORD - Specify the password that corresponds to the above-mentioned USER.
6. CONFIRM PASSWORD – Confirm the PASSWORD by retping it here.
7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. EXCLUDE LUNS – If you wish to exclude certain LUNs from the scope of monitoring, specify a list of comma-separated LUNs in this text box. By default, none will be displayed here.
11. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each LUN configured on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td rowspan="2">test</td>
<td>State:
Indicates the current state of this LUN.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Online</td><td>0</td></tr>
<tr><td>Offline</td><td>1</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current state of this LUN. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
<tr>
<td>Alignment state:
Indicates the alignment state of this LUN.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Aligned</td><td>0</td></tr>
<tr><td>Partial Writes</td><td>1</td></tr>
<tr><td>Indeterminate</td><td>2</td></tr>
<tr><td>Misaligned</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the alignment state of this LUN. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 0 to 3.</td>
</tr>
</table>

1.7.5 Volume Performance Test

Volumes are provisioned on an aggregate on a cluster node, and the combination of all the volumes constitutes the entire namespace or resource pool for LUNs. Volumes contain file systems that hold user data that is accessible using one or more of the access protocols supported by clustered Data ONTAP, including NFS, CIFS, HTTP, FTP, FC, and iSCSI.

For users to be able to read from/write data into volumes quickly, the I/O requests should be processed rapidly by the volumes. Slowdowns in data retrieval can be attributed to I/O processing bottlenecks. In the event of such slowdowns, administrators need to swiftly isolate the following:

- Which volumes are over-utilized?
- Which volumes are overloaded?
- Which volumes are experiencing serious latencies?
- When were these latencies observed most frequently – while reading or writing?
- What type of operations registered the maximum latency – CIFS, NFS, or iSCSI?

The **Volume Performance** test provides accurate answers to these questions. With the help of these answers, you can quickly diagnose the root-cause of slowdowns when reading from/writing into a volume.

Purpose	Helps quickly identify problematic volumes and accurately diagnose the root-cause of slowdowns when reading from/writing into a volume
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not.

<table>
<tr><td></td><td>
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.

In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.

10. EXCLUDE VOLUMES – If you wish to exclude certain volumes from the scope of monitoring, specify a list of comma-separated volumes in this text box. By default, none will be displayed here.

11. RECORDS PER CALL - The eG agent by default, executes the API commands in order to query the volumes in the target environment. In critical infrastructures spanning large number of volumes, a single execution by the eG agent may query(or download) a sizeable amount of monitoring data, thereby adding to the cluster load. To avoid this, you can tweak the RECORDS PER CALL parameter to enable the eG agent to obtain monitoring data iteratively in chunks instead of retrieving the entire amount of monitoring data in a single go. Say for example, the eG agent is required to query 1000 volumes, then specifying the value 100 in this text box will enable the eG agent to query 100 volumes at a time for 10 times to obtain monitoring data from all the volumes. By default, the value of this parameter is 10.

12. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.

•
</td></tr>
<tr><td>Outputs of the test</td><td>One set of results for each volume configured on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>
<table>
<tr><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Total operations:
Indicates the rate at which operations (including read and write) were performed on this volume.</td><td>Ops/Sec</td><td>This measure is a good indicator of how busy the volume is.

Comparing the value of this measure across volumes will enable you to quickly detect load-balancing irregularities (if any).</td></tr>
<tr><td>Write operations:
Indicates the rate at which write operations were performed on this volume.</td><td>Ops/Sec</td><td></td></tr>
</table>
</td></tr>
</table>

	Read operations: Indicates the rate at which read operations were performed from this volume.	Ops/Sec	
	Average latency: Indicates the average time taken by the WAFL filesystem to process all the operations performed on this volume.	Secs	The value of this measure excludes the request processing time and the network communication time of the volume. A high value of this measure is a cause for concern, as it indicates a processing bottleneck.
	Read latency: Indicates the average time taken by the WAFL filesystem to process the read requests of this volume.	Secs	The value of these measures exclude the request processing time and the network communication time of the volume. If the *Average latency* of a volume is high, then you can compare the value of these measures for that volume to know when the latency occurred – while reading or writing?
	Write latency: Indicates the average time taken by the WAFL filesystem to process the write requests made to this volume.	Secs	
	Data read: Indicates the rate at which data bytes were read from this volume.	MB/Sec	
	Date written: Indicates the rate at which data bytes were written to this volume	MB/Sec	
	CIFS operations: Indicates the rate at which the CIFS operations were performed on this volume.	Ops/Sec	This measure is inclusive of all the CIFS operations i.e., read, write and other miscellaneous CIFS operations. By comparing the value of this measure with that of the *NFS operations* and *SAN operations* measures for a volume, you can figure out which type of operation imposed the maximum load on that volume.

	NFS operations: Indicates the rate at which the NFS operations were performed on this volume.	Ops/Sec	This measure is inclusive of all the NFS operations i.e., read, write and other miscellaneous NFS operations. By comparing the value of this measure with that of the *CIFS operations* and *SAN operations* measures for a volume, you can figure out which type of operation imposed the maximum load on that volume.
	SAN operations: Indicates the rate at which the SAN operations were performed on this volume.	Ops/Sec	This measure is inclusive of all the SAN operations i.e., read, write and other miscellaneous SAN operations. By comparing the value of this measure with that of the *CIFS operations* and *NFS operations* measures for a volume, you can figure out which type of operation imposed the maximum load on that volume.
	CIFS latency: Indicates the average time taken for performing the CIF operations (including read, write and other miscellaneous CIF operations) on this volume.	Secs	The value of these measures exclude the request processing time and the network communication time of the volume. Ideally, the value of these measures should be low. If the *Avg latency* of a volume is very high, then, you can compare the value of these measures for that volume to determine the reason for the latency – is it because of processing bottlenecks experienced by CIFS operations? NFS operations? Or SAN operations?
	NFS latency: Indicates the average time taken for performing the NFS operations (including read, write and other miscellaneous NFS operations) on this volume.	Secs	
	SAN latency: Indicates the average time taken for performing the block protocol operations (including read, write and other miscellaneous block protocols operations) on this volume.	Secs	

1.7.6 Volume Space Test

This test auto-discovers the volumes configured on the NetApp Cluster, monitors the space utilization of each volume, and proactively alerts administrators on potential space crunch on the volumes.

Purpose	Auto-discovers the volumes configured on the NetApp Cluster, monitors the space utilization of each volume, and proactively alerts administrators on potential space crunch on the volumes

Target of the test	A NetApp Cluster		
Agent deploying the test	An external/remote agent		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here. 7. **AUTHENTICATION MECHANISM -** In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the *LOGIN_PASSWORD* authentication mechanism. This is why, *LOGIN_PASSWORD* is displayed as the default **AUTHENTICATION MECHANISM**. 8. **USE SSL -** Set the USE SSL flag to **Yes**, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and **No** if it is not. 9. **API PORT -** By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to **No**), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to **Yes**), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the **API PORT** parameter is set to *default* by default. In some environments however, the default ports 80 or 443 might not apply. In such a case, against the **API PORT** parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster. 10. **EXCLUDE VOLUMES –** If you wish to exclude certain volumes from the scope of monitoring, specify a list of comma-separated volumes in this text box. By default, *none* will be displayed here. 11. **TIMEOUT -** Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds. •		
Outputs of the test	One set of results for each volume configured on the NetApp Cluster being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Total space:** Indicates the total size of this volume.	GB	
	Available space: Indicates the space that is currently available for use in this volume.	GB	If the value of this measure is alarmingly decreasing, then it indicates that the volume is currently running out of space.
	Max used space: Indicates the maximum space that is used by this volume.	GB	If the value of this measure is close to that of the *Total space* measure, it indicates potential space crunch in the volume. Administrators may increase the size of the volume so that the space utilization of the volume is optimal.
	Percentage max used space: Indicates the percentage of maximum space used by this volume.	Percent	A high value for this measure indicates that the volume was running out of space.

1.7.7 Volume State Test

This test auto-discovers the volumes on the NetApp Cluster and monitors the current state of each volume. In addition, this test reports if the current state of the volume is *Inconsistent/Unrevoverable/Invalid* along with throwing insights on whether the *NVFAIL* flag is enabled on the volume.

Purpose	Auto-discovers the volumes on the NetApp Cluster and monitors the current state of each volume. In addition, this test reports if the current state of the volume is *Inconsistent/Unrevoverable/Invalid* along with throwing insights on whether the *NVFAIL* flag is enabled on the volume.
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST -** The IP address of the storage controller cluster. 3. **PORT** – The port number at which the specified **HOST** listens to. By default, this is *NULL*. 4. **USER** – Here, specify the name of the user who possesses the *readonly* role. If such a user does not pre-exist, then, you can create a special user for this purpose using the steps detailed in Section 1.1.2.1 of this document. 5. **PASSWORD -** Specify the password that corresponds to the above-mentioned **USER**. 6. **CONFIRM PASSWORD –** Confirm the **PASSWORD** by retping it here.

<table>
<tr><td></td><td colspan="3">7. AUTHENTICATION MECHANISM - In order to collect metrics from the NetApp Cluster, the eG agent connects to the ONTAP management APIs over HTTP or HTTPS. By default, this connection is authenticated using the LOGIN_PASSWORD authentication mechanism. This is why, LOGIN_PASSWORD is displayed as the default AUTHENTICATION MECHANISM.
8. USE SSL - Set the USE SSL flag to Yes, if SSL (Secured Socket Layer) is to be used to connect to the NetApp Unified Storage System, and No if it is not.
9. API PORT - By default, in most environments, NetApp Cluster listens on port 80 (if not SSL-enabled) or on port 443 (if SSL-enabled) only. This implies that while monitoring the NetApp Cluster, the eG agent, by default, connects to port 80 or 443, depending upon the SSL-enabled status of the NetApp Cluster - i.e., if the NetApp Cluster is not SSL-enabled (i.e., if the USE SSL flag above is set to No), then the eG agent connects to the NetApp Cluster using port 80 by default, and if the NetApp Cluster is SSL-enabled (i.e., if the USE SSL flag is set to Yes), then the agent-NetApp Cluster communication occurs via port 443 by default. Accordingly, the API PORT parameter is set to default by default.
In some environments however, the default ports 80 or 443 might not apply. In such a case, against the API PORT parameter, you can specify the exact port at which the NetApp Cluster in your environment listens, so that the eG agent communicates with that port for collecting metrics from the NetApp Cluster.
10. EXCLUDE VOLUMES – If you wish to exclude certain volumes from the scope of monitoring, specify a list of comma-separated volumes in this text box. By default, none will be displayed here.
11. TIMEOUT - Specify the duration (in seconds) beyond which the test will timeout if no response is received from the device. The default is 120 seconds.
•</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each aggregate on the NetApp Cluster being monitored</td></tr>
<tr><td>Measurements made by the</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
</table>

<table>
<tr>
<td rowspan="2">test</td>
<td>State:
Indicates the current state of this volume.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Online</td><td>0</td></tr>
<tr><td>Mixed</td><td>1</td></tr>
<tr><td>Restricted</td><td>2</td></tr>
<tr><td>Offline</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current state of this volume. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 to 3.</td>
</tr>
<tr>
<td>Is inconsistent?:
Indicates whether/not the state of this volume is Inconsistent.</td>
<td></td>
<td>This measure reports a value Yes if this volume is inconsistent and No if otherwise.
The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>0</td></tr>
<tr><td>Yes</td><td>1</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating whether the volume is inconsistent or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>Is invalid?:
Indicates whether/not the state of this volume is Invalid.</td>
<td></td>
<td>This measure reports a value Yes if the state of this volume is invalid and No if otherwise.
The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>0</td></tr>
<tr><td>Yes</td><td>1</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating whether the volume is invalid or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
<tr>
<td></td>
<td>Is unrecoverable?:
Indicates whether/not the state of this volume is Uncoverable.</td>
<td></td>
<td>This measure reports a value Yes if the state of this volume is Unrecoverable and No if otherwise.
The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>0</td></tr>
<tr><td>Yes</td><td>1</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating whether the state of this volume is Unrecoverable or not. However, in the graph of this measure, Measure Values will be represented using the corresponding numeric equivalents i.e., 0 or 1.</td>
</tr>
</table>

	Is nvfailed?: Indicates whether/not the *NVFAIL* flag is enabled on this volume.		This measure reports a value *Yes* if the NVFAIL flag is enabled and *No* if otherwise. The values that this measure can report and their corresponding numeric values have been listed in the table below. **Measure Value** / **Numeric Value**: No = 0; Yes = 1 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating whether the *NVFAIL* flag is enabled or not. However, in the graph of this measure, **Measure Value**s will be represented using the corresponding numeric equivalents i.e., *0 or 1*.

1.8 The Cluster Service Layer

To monitor the failover state of the cluster system and the partner system, use the test mapped to this layer.

Figure 1.10: The tests mapped to the Cluster Service layer

1.8.1 Cluster Failover State Test

This test reports the current failover state of the NetApp Cluster and the partner system. In addtition, this test reports the current state of the storage failover interconnect link.

Purpose	Reports the current failover state of the NetApp Cluster and the partner system. In addtition, this test reports the current state of the storage failover interconnect link
Target of the test	A NetApp Cluster
Agent deploying the test	An external/remote agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the NetApp Cluster 3. **SNMPPORT** – The SNMP Port number of the NetApp Cluster (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: ➢ **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: ➢ **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 NetApp Cluster over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

16. **DETAILED DIAGNOSIS -** To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

- 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.

Outputs of the test: One set of results for the NetApp Cluster being monitored

Measurements made by the test

Measurement	Measurement Unit	Interpretation
State: Indicates the current failover state of the NetApp Cluster.		The values that this measure can report and their corresponding numeric values have been listed in the table below. **Measure Value** / **Numeric Value** Dead – 1 Can takeover – 2 Cannot takeover – 3 Takeover – 4 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating the current failover state of the cluster. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., *1 to 4.*

<table>
<tr>
<td></td>
<td>Partner state:
Indicates the current failover state of the partner system.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>May be down</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Dead</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current failover state of the partner system. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>Interconnect state:
Indicates the current state of the storage failover interconnect link.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values have been listed in the table below.
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>May be down</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Dead</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current failover state of the partner system. However, in the graph of this measure, states will be represented using the corresponding numeric equivalents i.e., 1 to 3.</td>
</tr>
</table>

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 **NetApp Cluster**. 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.