Monitoring Array Application Delivery Controller

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Array application delivery controllers provide the availability, scalability, performance, security and control essential to keeping applications and servers running in their power band. Integrated local and global server load balancing, as well as link load balancing, ensure the highest levels of resiliency for your applications, while connection multiplexing, SSL offload, caching and compression work together to deliver the fastest end-user experience possible. What's more, by terminating connections on APV Series ADCs, applications are protected behind Array's WebWall® application security suite. Available as physical or virtual appliances, or on popular public clouds, Array ADCs are designed to meet technical requirements while remaining simple enough for any size IT team and affordable enough for any size business.

Array ADCs provide the ability to direct the users to the best performing, most accessible servers. Should one of the servers (or applications on that server) become inaccessible due to any type of failure, the ADC will take that server or application off-line, while automatically re-routing users to other functioning servers. This process is essentially seamless to the user, and critical to servicing the customer.

Since application delivery delays, inefficiencies, and failures can cause prolonged service outages and cost an enterprise money and reputation, the continuous operation and good health of the ADC is of great importance. Therefore, it is imperative that the Delivery Controller should be continuously monitored to avert such eventualities. This is where eG Enterprise helps administrators!

Chapter 2: How to Monitor Array Application Delivery Controller Using eG Enterprise?

eG Enterprise monitors the Array Application Delivery Controller appliance using an eG remote agent that is deployed on a remote Windows host in the environment. This agent is capable of monitoring the performance of the target delivery controller in the following ways:

- By polling the SNMP MIB of the appliance;
- By connecting to the delivery controller via SSH and running CLI commands;

To enable the eG agent to use the aforesaid methodologies, a set of pre-requisites should be fulfilled. These requirements have been discussed in the following section.

2.1 Pre-requisites for Monitoring the Array Application Delivery Controller

To enable the eG agent to collect performance metrics from the Array Application Delivery Controller, the following pre-requisites should be fulfilled:

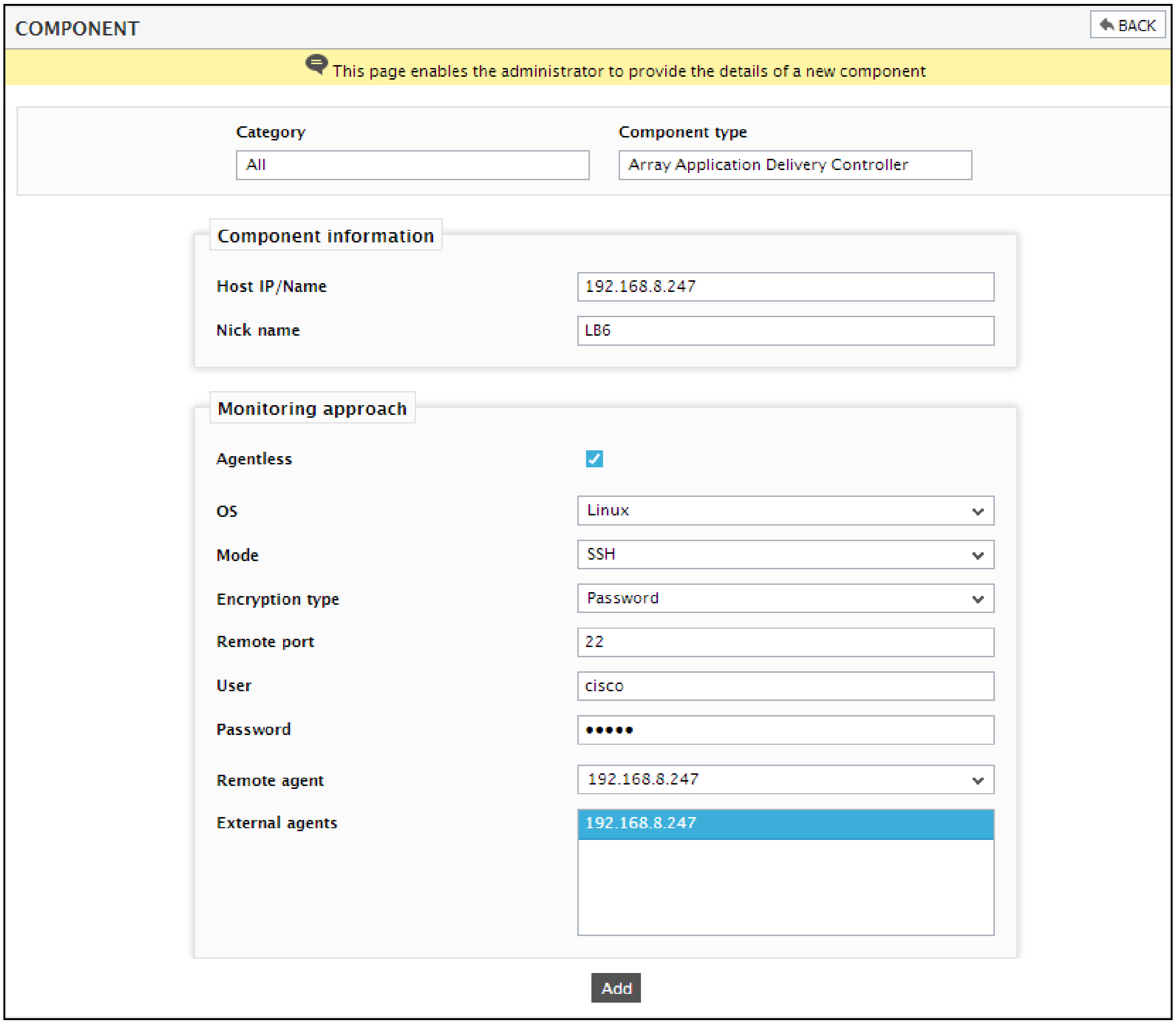
- The target appliance should be SNMP-enabled.
- The eG agent should be able to access the target appliance over the network.
- The eG agent should be able to communicate with the target delivery controller via SSH. For this, specify the SSH port (default port: 22) in the test configuration page and ensure that the SSH port is opened on the firewall (if any) between the agent and the target appliance.
- Configure the credentials of a user who is authorized to access the target delivery controller via the SSH port. This can be achieved when managing the target delivery controller using the eG administrative interface. The same set of credentials should also be specified while configuring the tests.
- To execute majority of the CLI commands on the ArrayOS, the specified user should also have the privilege to issue the CLI commands in the **Enable mode** after logging into the delivery controller. Since the user can access majority of the commands in the **Enable mode**, this mode has been protected with a password to ensure an additional layer of security.

Once the above-said pre-requisites are fulfilled, manage the *Array Application Delivery Controller* component using eG administrative interface. The steps for achieving this are discussed in the Section **2.2**.

2.2 Managing the Array Application Delivery Controller

The Array Application Delivery Controller appliance cannot be automatically discovered by eG Enterprise. This implies that you will have to manually add the target delivery controller into the eG Enterprise system to manage it. Remember that the eG Enterprise automatically manages the components that are added manually. Follow the steps below to achieve the same:

1. Login to the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS** page that appears, select *Array Application Delivery Controller* from the **Component type** drop-down and then click the **Add New Component** button.



COMPONENT

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

Category	Component type
All	Array Application Delivery Controller

Component information

Host IP/Name	192.168.8.247
Nick name	LB6

Monitoring approach

Agentless	☑
OS	Linux
Mode	SSH
Encryption type	Password
Remote port	22
User	cisco
Password	•••••
Remote agent	192.168.8.247
External agents	192.168.8.247

Figure 2.1: Adding a Array Application Delivery Controller

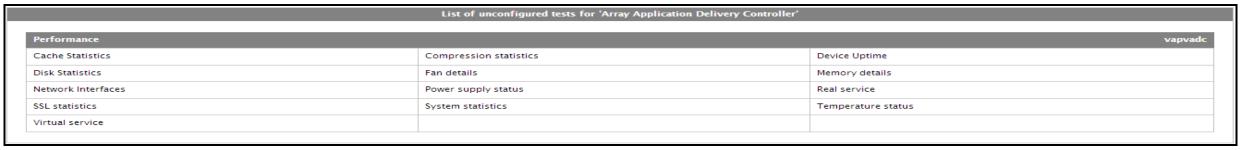
4. Specify the **Host IP/Name** and the **Nick name** of the Array Application Delivery Controller component in Figure 2.1. Since the target delivery controller is monitored in an agentless manner, select **Linux** as the **OS** and **SSH** as the **Mode**.

5. Next, provide the credentials of a user who can run the CLI commands on the target delivery controller via the SSH Port, in the **User** and **Password** text boxes.

6. Then, click the **Add** button to register the changes.

2.3 Configuring the tests

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



List of unconfigured tests for 'Array Application Delivery Controller'

Performance		vapvadc
Cache Statistics	Compression statistics	Device Uptime
Disk Statistics	Fan details	Memory details
Network Interfaces	Power supply status	Real service
SSL statistics	System statistics	Temperature status
Virtual service		

Figure 2.2: List of unconfigured tests to be configured for the Array Application Delivery Controller

2. Click on the tests to configure them. To know how to configure these tests, refer to the **Monitoring the Array Application Delivery Controller** chapter.
3. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Array Application Delivery Controller

To ensure continuous operation and good health of the Array Application Delivery Controller appliance, eG Enterprise provides a specialized Array Application Delivery Controller model (see Figure 3.1).

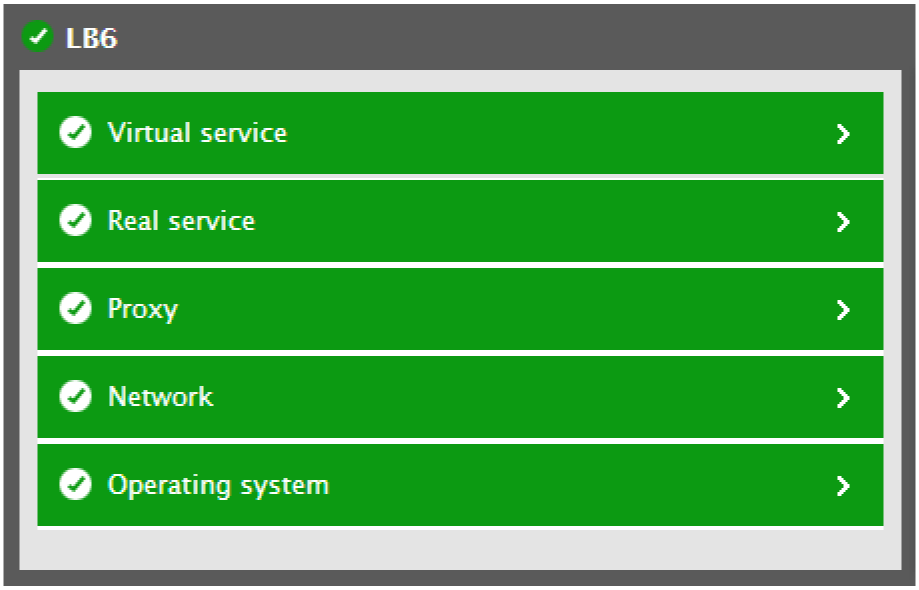


Figure 3.1: The layer model of the Array Application Delivery Controller

Every layer of Figure 3.1 is mapped to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- How well the CPU of the Array Application Delivery Controller has been utilized?
- What is the current state of the fans and is any fan running at abnormal speed?
- What is the current status of the power supplies?
- What is the current health state of each real server and virtual server? How well the real server and virtual server are processing client traffic?
- Which server is handling the maximum traffic?
- How many connections were established to the target delivery controller?
- How many number of requests were processed by the delivery controller per second?

- How many number of SSL connections were accepted by the virtual SSL host?
- How well the client requests are processed by them?

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

3.1 The Operating System Layer

The tests associated with this layer focus on the status of the power supplies on the target Application Delivery Controller, the CPU utilization of the target delivery controller, the size of the data structure items, the number of data structure items that were utilized etc.

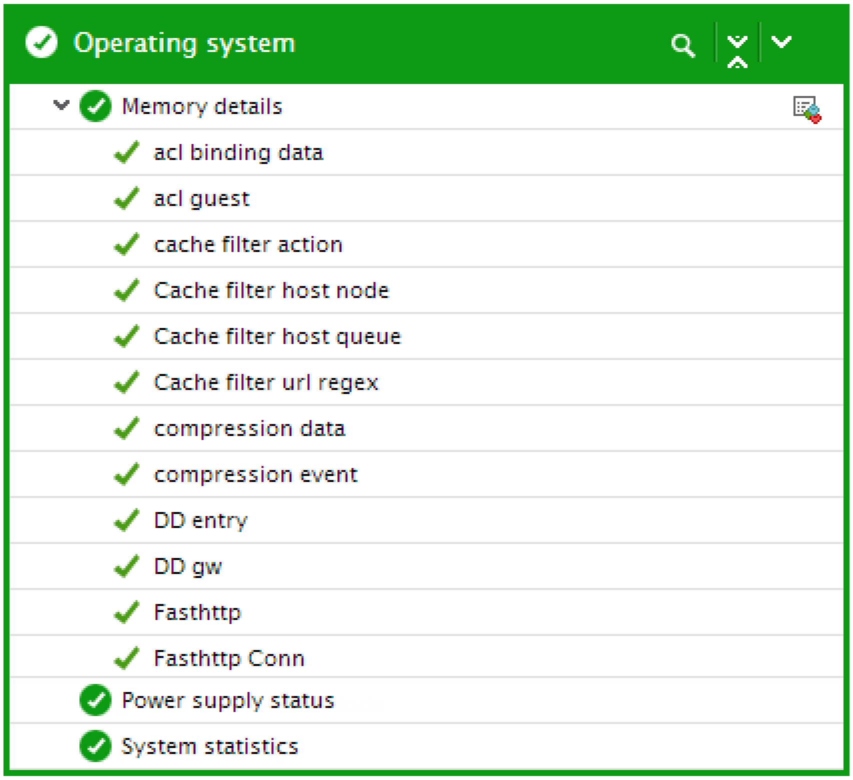


Figure 3.2: The tests associated with the Operating System layer

3.1.1 Memory Details test

Memory resources in the target delivery controller are divided into different types of data structure items. The data structure items are designated with definite size and count. Each data structure item is dedicated to provision memory to a particular process running on the delivery controller. Availability of the data structure items plays vital role in performing.

Each connection owns a “pcb” data structure. There are two kinds of “pcb” data structure; “small pcb” where size is 64 bytes is for TCP connections in “TIME_WAIT” state. “pcb” for all the other TCP connections has bigger size: 288 bytes. The “LIMIT” column tells the total number of data structure items. “USED” refers the number of items in use. The “Free” indicates left items that may be used. The “REQUEST” is the accumulation of total usages and is always incremented.

This test auto-discovers the types of data structure items and, for each type, reports the size of the data structure items, the count of the items and the number of data structure items that are utilized. This way, administrators can figure out the data structure item that is most commonly used.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each data structure item on the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP

Parameter	Description
	context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some

Parameter	Description
	environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Size	Indicates the size of the data structure items of this type in the delivery controller.	MB	
Limit	Indicates the total number of the data structure items of this type.	Number	
Used	Indicates the number of the data structure items of this type that are utilized in the delivery controller.	Number	By comparing the value of this measure across the types, the data structure items that are most commonly used can be identified.
Free	Indicates the number of the data structure items of this type that are available for use in the delivery controller.	Number	

3.1.2 Power Supply Status Test

The availability and proper functioning of power supplies is critical to the uninterrupted operations of the target delivery controller. Irrecoverable errors, power failures, or erratic voltage fluctuations experienced by the power supplies can halt operations of the delivery controller for hours and slow down or completely suspend the delivery of the applications. If such an unpleasant eventuality is to be pre-empted, administrators must be able to proactively detect potential problems with the power supply and take remedial action before anything untoward happens. The **Power Supply Status** test helps administrators achieve this end.

This test continuously monitors the power supplies of the target delivery controller and reports the current state of all the power supplies.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the A10 Application Delivery Controller that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the

Parameter	Description
	Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current state of the power supplies of the target delivery controller.</td><td></td><td>The values of this measure and their corresponding numeric values are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Ok</td><td>0</td></tr>
<tr><td>Failed</td><td>1</td></tr>
</table>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Value</b>s listed in the table above to indicate the current state of the power supplies. In the graph of this measure however, the status of the power supplies will be represented using the numeric equivalents.</td></tr>
</table>

3.1.3 Temperature Status Test

This test tracks the current temperature of CPU and system and reports the average temperature value that is computed using the CPU temperature and system temperature. Using this test, administrators can ensure whether the temperature of the target delivery controller is in admissible range and take remedial measures if violations are detected.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed

Parameter	Description
Host	The IP address of the Application Delivery Controller that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the monitored target. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm

Parameter	Description
	- **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: - **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU and System temperature	Indicates the average temperature of the CPU and the system.	Celsius	Ideally, the value of this measure should be in a permissible range. A sudden rise/fall in the value of this measure could be a cause for concern.

3.1.4 System Statistics Test

This test continuously monitors the target delivery controller and measures the key performance metrics such as CPU utilization, the number of connections established to the delivery controller per second and the number of requests made to the delivery controller in one second.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SSH Username and SSH Password	Specify the credentials of a user who has the right to execute CLI (command-line interface) commands on the target delivery controller and pull out metrics via SSH.
Confirm Password	Confirm the SSH Password by retyping it here.
SSH Port	Specify the SSH port of the target delivery controller here; The default value is *22*.
SSH Enable Password	The delivery controller offers three levels or modes using which the user can simply execute CLI commands on the ArrayOS. The modes are given below: • **User Mode** - In this mode, the user can execute the commands to perform the authorized and basic operations and non-critical functions on the ArrayOS. • **Enable Mode** - This mode enables the user to run the majority of commands for viewing data. To prevent unauthorized access to this mode, access should be password protected. • **Config Mode** - Using this mode, the user can change the configuration of the delivery controller for global configuration and access (Using commands). The user can select any of these modes depending on his/her needs. If the user has selected the Enable Mode, he/she should specify a password in the SSH Enable Password text box to execute the commands. In order to have access to most of the commands on the ArrayOS, administrator should

Parameter	Description
	select the Enable mode. Normally, you should enter a password to enter the Enable mode to restrict access to this mode. enable secret password uses stronger encryption when it is stored in the configuration file and it is more safe.
Confirm Password	Confirm the SSH Enable Password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the percentage of CPU utilized by the delivery controller.	Percent	A high value for this measure is a cause of concern.
Connection per second	Indicates the number of connections established to the delivery controller in one second.	Number	
Request per second	Indicates the number of requests made to the delivery controller in one second.	Number	

3.1.5 Disk Statistics Test

This test monitors the space utilization of the disks on the target delivery controller. Using this test, administrators may be proactively alerted to potential space crunch of the disks, if any.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

Parameter	Description
	- **MD5** – Message Digest Algorithm - **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: - **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total diskspace	Indicates the total capacity of the disks of the delivery controller.	MB	
Used diskspace	Indicates the amount of space used in the disks.	MB	If the value of this measure is close to the *Total diskspace* measure, then it indicates that the disks are running out

Measurement	Description	Measurement Unit	Interpretation
			of space. To avoid potential space crunch, additional space should be allocated to the disks by the administrators.
Free diskspace	Indicates the amount of space that is available for use in the disks.	MB	A high value is desired for this measure.
Used diskspace utilization	Indicates the percentage of space utilized on the disks.	Percent	A value close to 100% can indicate a potential problem situation where applications executing on the system may not be able to write data to the disk(s) with very high usage.

3.1.6 Fan Details Test

Fans ensure that the temperature of the core components of the Array Application Delivery Controller are well-within operable limits. A sudden rise/fall of the fan's speed may lead to fan failures or rapid temperature rise within the delivery controller. This in turn, may cause permanent damage to the sensitive components of the delivery controller. To avoid such heavy duty damage, it is necessary to monitor the health of the fans in terms of operational speed at regular intervals. This is where the **Fan Details** test exactly helps!

This test reports the current speed of the fans in the target delivery controller. Using the speed value reported by this test, administrators can figure out the fans that do not operate within the admissible speed range and replace the same to maintain smooth operation of the delivery controller.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target delivery controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified Username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm

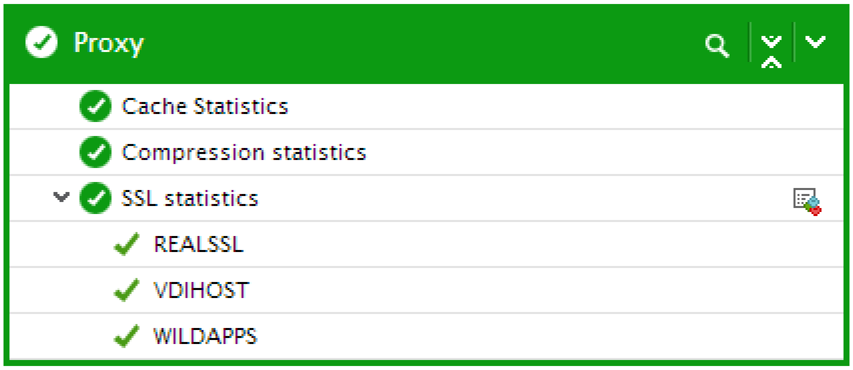
Parameter	Description
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Speed	Indicates the current operational speed of the fans in the delivery controller.	Rpm	The speed of the fan should be well within admissible limits. A sudden/significant rise/fall in the value of this measure could be a cause of concern which warrants an investigation.

3.2 The Proxy Layer

The tests associated with this layer focus on the request processing ability of the cache on the target Application Delivery Controller, the accurate amount of data sent for compression, data sent and received during compression, the statistics pertaining to the SSL connections etc.



Proxy

Cache Statistics

Compression statistics

SSL statistics

REALSSL

VDIHOST

WILDAPPS

Figure 3.3: The tests associated with the Proxy layer

3.2.1 Cache Statistics Test

The Array application delivery controller serves frequently requested content from cache for increased performance and to help scale the capacity for Web - based application services. The cache is said to be effectively utilized only if it is able to service the maximum number of requests; this greatly reduces direct disk accesses and related overheads, and thus improves performance. On the contrary, ineffective cache usage can be the key contributor to a slowdown or degradation in performance, as it increases disk accesses. To understand how the caches are utilized and to promptly capture abnormalities in cache usage, administrators have to continuously monitor the requests processed in the cache. This is what exactly the **Cache Statistics** test does!

This test continuously tracks the cache on the target delivery controller and reports the total number of requests that were received by the cache. In addition, this test also reveals the number of GET, HEAD, PURGE and POST requests that were received by the cache and the hit ratio of the cache. This way, administrator can figure out the ineffective request processing patterns of the cache, which may contribute to a slowdown in operations.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SSH Username and SSH Password	Specify the credentials of a user who has the right to execute CLI (command-line interface) commands on the target delivery controller and pull out metrics via SSH.
Confirm Password	Confirm the SSH Password by retyping it here.
SSH Port	Specify the SSH port of the target delivery controller here; The default value is *22*.
SSH Enable Password	The delivery controller offers three levels or modes to the ArrayOS. The modes are given below: • **User Mode** - In this mode, user can perform the authorized and basic operations and non-critical functions. • **Enable Mode** - When this mode is selected, the user can run majority of commands for view data. • **Config Mode** - Using this level, the user can change the configuration of the delivery controller for global configuration and access (Using CLI commands). The SSH Enable password is the password that is needed for the user to access the commands when the Enable Mode is selected.
Confirm Password	Confirm the SSH Enable Password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Requests received	Indicates the total number of requests received by the cache in the target delivery controller during the last measurement period.	Number	
Requests with get method	Indicates the number of GET requests received by	Number	Using the GET method, you can retrieve specific information from the

Measurement	Description	Measurement Unit	Interpretation
	the cache during the last measurement period.		cache. When the cache receives the GET request, it returns the requested data as the entity in response.
Requests with head method	Indicates the number of HEAD requests received by the cache during the last measurement period.	Number	The HEAD method is identical to GET except that the cache will not return a message-body in the response.
Requests with purge method	Indicates the number of PURGE requests received by the cache during the last measurement period.	Number	A purge is what happens when you pick out an object from the cache and discard it along with its variants. Usually a purge is invoked through HTTP with the method PURGE. HTTP Purge sends a request to delete the cached data of a page or post every time it it modified. This happens when updating, publishing, commenting on, or deleting an post HTTP Purge sends a request to delete the cached data of a page or post every time it modified. This happens when updating, publishing, commenting on, or deleting an post
Requests with post method	Indicates the number of POST requests received by the cache during the last measurement period.	Number	
Hit ratio	Indicates the percentage of requests that were successfully retrieved from the cache during the last measurement period.	Percent	

3.2.2 Compression Statistics Test

The application delivery controller can efficiently compress in - line and deliver packet dynamic/static contents over the network. You can enable the compression feature of the delivery controller using the CLI commands or via the delivery controller console. When the compression feature is enabled, HTTP responses received from the servers are compressed on the delivery controller by dividing the response data into smaller packets. The divided packets are then combined into larger packets and sent to compression- aware browsers on the network. The compression feature of the delivery controller also allows compressing the application payload within each packet. This in turn, reduces download time and network bandwidth consumption of the delivery controller without degrading content quality and improves overall experience of the end-users .

The real test of the effectiveness of the compression feature lies in how much data is compressed and how quickly the compression is performed. This can be easily measured using the **Compression statistics** test. By periodically running this test, administrators can accurately assess the amount of data that was sent for compression and received after the compression process. In addition, this test also reveals the rate at which the data was sent and received during the compression process. In the process, the count of active HTTP connections and the compression ratio are also reported.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SSH Username and SSH Password	Specify the credentials of a user who has the right to execute CLI (command-line interface) commands on the target delivery controller and pull out metrics via SSH.
Confirm Password	Confirm the SSH Password by retyping it here.
SSH Port	Specify the SSH port of the target delivery controller here; The default value is *22*.
SSH Enable Password	The delivery controller offers three levels or modes to the ArrayOS. The modes are given below: • **User Mode** - In this mode, user can perform the authorized and basic operations and non-critical functions. • **Enable Mode** - When this mode is selected, the user can run majority of commands for view data.

Parameter	Description
	• **Config Mode** - Using this mode, the user can change the configuration of the delivery controller for global configuration and access (Using CLI commands). If the user has selected the Enable Mode, The SSH Enable password is the password that is needed for the user to access the commands when the is selected.
Confirm Password	Confirm the SSH Enable Password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted to client	Indicates the total amount of data transmitted to the client from the delivery controller during the last measurement period.	MB	
Data transmitted to compression	Indicates the amount of data transmitted out for compression process to the delivery controller during the last measurement period.	MB	The compression process is performed using either the software compression method or hardware compression method.
Data received from compression	Indicates the amount of data received by the delivery controller after the compression process during the last measurement period.	MB	
Data transmitted	Indicates the rate at which the bytes are sent out for the compression process.	Bytes/sec	
Data received	Indicates the rate at which the bytes are received after the compression process.	Bytes/sec	
Active transaction	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
	HTTP connections that are currently active on the delivery controller.		
Compression ratio	Indicates the ratio of the data sent out for compression and the data received after the compression process.	Percent	

3.2.3 SSL Statistics Test

Administrators create SSL Virtual Hosts (also referred as SSL engine) on the target delivery controller using SSL setup. The SSL Virtual Hosts hold SSL - related information and handle traffic with the associated certificate and private key. The SSL Virtual Host can be associated with multiple SLB Virtual Services and different application types on top of SSL support, such as HTTPS, FTPS or TCPS. Tracking the connections made through the SSL Virtual Host, administrators are able to figure out the load on the target delivery controller. This could be done using the **SSL Statistics** test.

For each virtual host on the target delivery controller, this test reports the number of SSL connections that were open on the virtual host and the count of SSL connections that were requested and accepted by the virtual host. In the process, this test also reveals the number of sessions that were resumed and ready to be resumed.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each virtual host on the target delivery controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SSH Username and SSH Password	Specify the credentials of a user who has the right to execute CLI (command-line interface) commands on the target delivery controller and pull out metrics via SSH.

Parameter	Description
Confirm Password	Confirm the SSH Password by retyping it here.
SSH Port	Specify the SSH port of the target delivery controller here; The default value is *22*.
SSH Enable Password	The delivery controller offers three levels or modes using which the user can simply execute CLI commands on the ArrayOS. These modes are given below: • **User Mode** - In this mode, the user can execute the commands to perform the authorized and basic operations and non-critical functions on the ArrayOS. • **Enable Mode** - This mode lets the user to run the majority of commands on the ArrayOS. Since the user has access to the majority of commands, it becomes necessary that the mode be password protected. This is to prevent unauthorized access to this mode, access should be password protected. • **Config Mode** - Using this mode, the user can change the configuration of the delivery controller for global configuration and access (Using commands). The user can select any of these modes depending on his/her needs. If the user has selected the Enable Mode, he/she should specify a password in the SSH Enable Password text box to execute the commands. In order to have access to most of the commands on the ArrayOS, administrator should select the Enable mode. Normally, you should enter a password to enter the Enable mode to restrict access to this mode. enable secret password uses stronger encryption when it is stored in the configuration file and it is more safe.
Confirm Password	Confirm the SSH Enable Password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

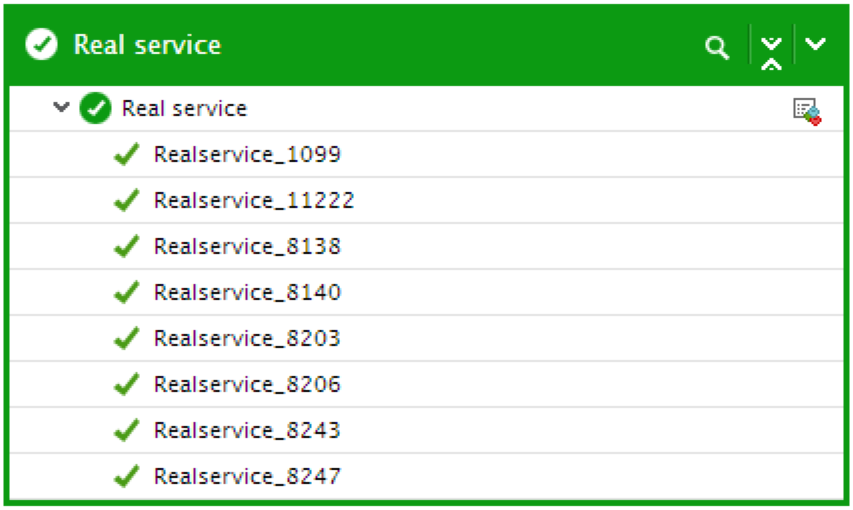
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Open SSL connections	Indicates the number of SSL connections that were open between on this virtual host during the last measurement period.	Number	
Accepted SSL	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
connections	SSL connections that were accepted by this virtual host during the last measurement period.		
Requested SSL connections	Indicates the number of SSL connections that were requested from this virtual host during the last measurement period.	Number	
5 minutes requested rate	Indicates the rate at which SSL connections were requested from this virtual host in last 5 minutes.	Connections/Sec	
Resume SSL sessions	Indicates the number of SSL sessions that were resumed on this virtual host during the last measurement period.	Number	
Resumable SSL sessions	Indicates the number of SSL sessions that were ready to be resumed on this virtual host during the last measurement period.	Number	
Session misses	Indicates the number of SSL sessions that were missed on this virtual host during the last measurement period.	Number	

3.3 The Real Service Layer

The tests associated with this layer reveals the current state of the real servers and also reveals how well each server transmits and receives data.


Real service

Real service

Realservice_1099

Realservice_11222

Realservice_8138

Realservice_8140

Realservice_8203

Realservice_8206

Realservice_8243

Realservice_8247

Figure 3.4: The tests associated with the Real Service layer

3.3.1 Real Service Test

Physical servers a.k.a Real Services (also referred as real server) are those that are bound to a virtual server in a server farm of the vAPV Application Delivery Controller. Whenever a request is received from a user, the virtual server bound to the real server responds to those requests by channelizing the requests to the real servers that are currently available. Since multiple virtual hosts can be pointed to the same set of real servers, having a good number of supported VIPs presents more flexibility in the architecture and design of the site or application. There may be upto 100 real servers connected to a single virtual host and the same set of real servers can be pointed to multiple virtual hosts to provide more flexibility in the architecture and design of the delivery controller. The delivery controller installed in large environments often receives thousands of client requests per second, which should be responded without any time delay. In such cases, the virtual host sends the requests continuously to the available real servers bound to it. If the real server is experiencing any technical glitch or a slowdown or if the real server is currently overloaded, the delivery controller may not be effective in responding to the client requests thus causing inconsistencies in the load balancing functionality. To avoid such inconsistencies, it is necessary to monitor the health and the request processing details of the real servers. This is where the **Real Service** test exactly helps!

For each real server configured on the delivery controller, this test continuously monitors the current state of the real servers and also reveals how well each server transmits and receives data. In addition, this test detects inconsistencies in load-balancing early on and warns administrators of possible deviations proactively.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each real server on the Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SSH Username and SSH Password	Specify the credentials of a user who has the right to execute CLI (command-line interface) commands on the target delivery controller and pull out metrics via SSH.
Confirm Password	Confirm the SSH Password by retyping it here.
SSH Port	Specify the SSH port of the target delivery controller here; The default value is *22*.
SSH Enable Password	The delivery controller offers three levels or modes to the ArrayOS. The modes are given below: • **User Mode** - In this mode, user can perform the authorized and basic operations and non-critical functions. • **Enable Mode** - When this mode is selected, the user can run majority of commands for view data. • **Config Mode** - Using this level, the user can change the configuration of the delivery controller for global configuration and access (Using CLI commands). The SSH Enable password is the password that is needed for the user to access the commands when the Enable Mode is selected.
Confirm Password	Confirm the SSH Enable Password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this real server.		The values of this measure and their corresponding numeric values are listed below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
<b>Note:</b>
By default, this measure reports one of the <b>Measure Value</b>s listed in the table above to indicate the current status of this real server. In the graph of this measure however, the real server status will be represented using the numeric equivalents.</td></tr>
<tr><td>Data transmitted</td><td>Indicates the amount of data that was transmitted from this real server during the last measurement period.</td><td>KB</td><td rowspan="2">Compare the values of these measures across nodes to identify the server that is handling maximum traffic.</td></tr>
<tr><td>Data received</td><td>Indicates the amount of data that was received by this real server during the last measurement period.</td><td>KB</td></tr>
<tr><td>Packets transmitted</td><td>Indicates the number of packets that were transmitted from this real server during the last measurement period.</td><td>Number</td><td rowspan="2">Compare the value of these measures across the real servers to identify the real server that is experiencing the maximum traffic.</td></tr>
<tr><td>Packets received</td><td>Indicates the number of packets that were received by this real server during the last measurement period.</td><td>Number</td></tr>
<tr><td>Maximum connection count</td><td>Indicates the maximum number of connections that are established on this real server.</td><td>Number</td><td>This measure is a good indicator of the load on the real server.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Current connection count	Indicates the number of connections that are currently active on this real server.	Number	
Outstanding request count	Indicates the number of requests that are currently in an outstanding state on this real server.	Number	
Hits	Indicates the number of requests received by this real server.	Number	A value close to 100% indicates that the real server is currently overloaded.
Average bandwidth transmitted	Indicates the rate at which data is transmitted from this real server.	Bits/second	
Average bandwidth received	Indicates the rate at which data is received by this real server.	Bits/second	
Average response time	Indicates the average time taken by this real server to respond to the requests.	Millisecond	

3.4 The Virtual Service Layer

The tests associated with this layer focus on the performance of the UPS battery, and helps administrators decide whether the battery configuration needs to be changed or the battery needs to be replaced to ensure peak performance.

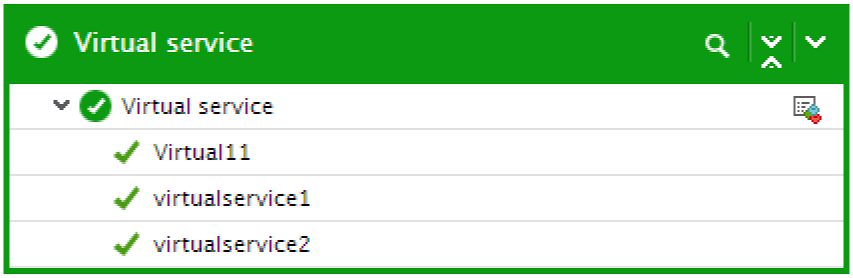


Figure 3.5: The tests associated with the Virtual Service layer

3.4.1 Virtual Service Test

On the Application Delivery Controller appliance, a virtual service (also referred to as a virtual server or virtual host) is configured by specifying a Virtual IP/Port and the protocol for the load balancing operations. The virtual server is bound to a number of real services (also called as real servers) within a server farm and associated with a number of groups. The virtual server is typically a publicly facing IP address which responds to user requests. Whenever the requests are received from users, the virtual server responds to those requests by channelizing the requests to the real servers. This way, the appliance will load balance the requests to different real services.

Since the virtual servers are able to manage the traffic and divert user requests to servers that are managing fewer requests, poor performance and outages can be avoided. Irregularities in load balancing can cause significant delay in request processing thus affecting the user experience with the target delivery controller. To avoid this, you can configure the periodic execution of the **Virtual Services** test.

For each virtual service (server) configured on the delivery controller, this test continuously monitors the load on the load-balancing virtual servers and reveals how well each server processes user requests. In addition, this test detects inconsistencies in load-balancing early on and warns administrators of possible deviations proactively.

Target of the test : An Array Application Delivery Controller

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each virtual server on the target Array Application Delivery Controller that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
SSH Username and SSH Password	Specify the credentials of a user who has the right to execute CLI (command-line interface) commands on the target delivery controller and pull out metrics via SSH.
Confirm Password	Confirm the SSH Password by retyping it here.
SSH Port	Specify the SSH port of the target delivery controller here; The default value is *22*.
SSH Enable	The delivery controller offers three levels or modes to the ArrayOS. The modes are

Parameter	Description
Password	given below: • **User Mode** - In this mode, user can perform the authorized and basic operations and non-critical functions. • **Enable Mode** - When this mode is selected, the user can run majority of commands for view data. • **Config Mode** - Using this level, the user can change the configuration of the delivery controller for global configuration and access (Using CLI commands). The SSH Enable password is the password that is needed for the user to access the commands when the Enable Mode is selected.
Confirm Password	Confirm the SSH Enable Password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of groups associated	Indicates the number of groups associated with this virtual server.	Number	
Number of real services associated	Indicates the number of real servers that are associated with this virtual server.	Number	
Data transmitted	Indicates the amount of data that was transmitted from this virtual server during the last measurement period.	KB	Compare the values of these measures across virtual servers to identify the server that is handling maximum traffic.
Data received	Indicates the amount of data that was received by this virtual server during the last measurement period.	KB	

Measurement	Description	Measurement Unit	Interpretation
Packets transmitted	Indicates the number of packets that were transmitted from this virtual server during the last measurement period.	Number	Compare the value of these measures across the real servers to identify the virtual server that is experiencing the maximum traffic.
Packets received	Indicates the number of packets that were received by this virtual server during the last measurement period.	Number	
Maximum connection count	Indicates the maximum number of connections that are established on this real server.	Number	This measure is a good indicator of the load on the virtual server.
Current connection count	Indicates the number of connections that are currently active on this virtual server.	Number	
Outstanding request count	Indicates the number of requests that are currently in an outstanding state on this virtual server.	Number	
Hits	Indicates the number of requests received by this virtual server.	Number	A value close to 100% indicates that the real server is currently overloaded.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.