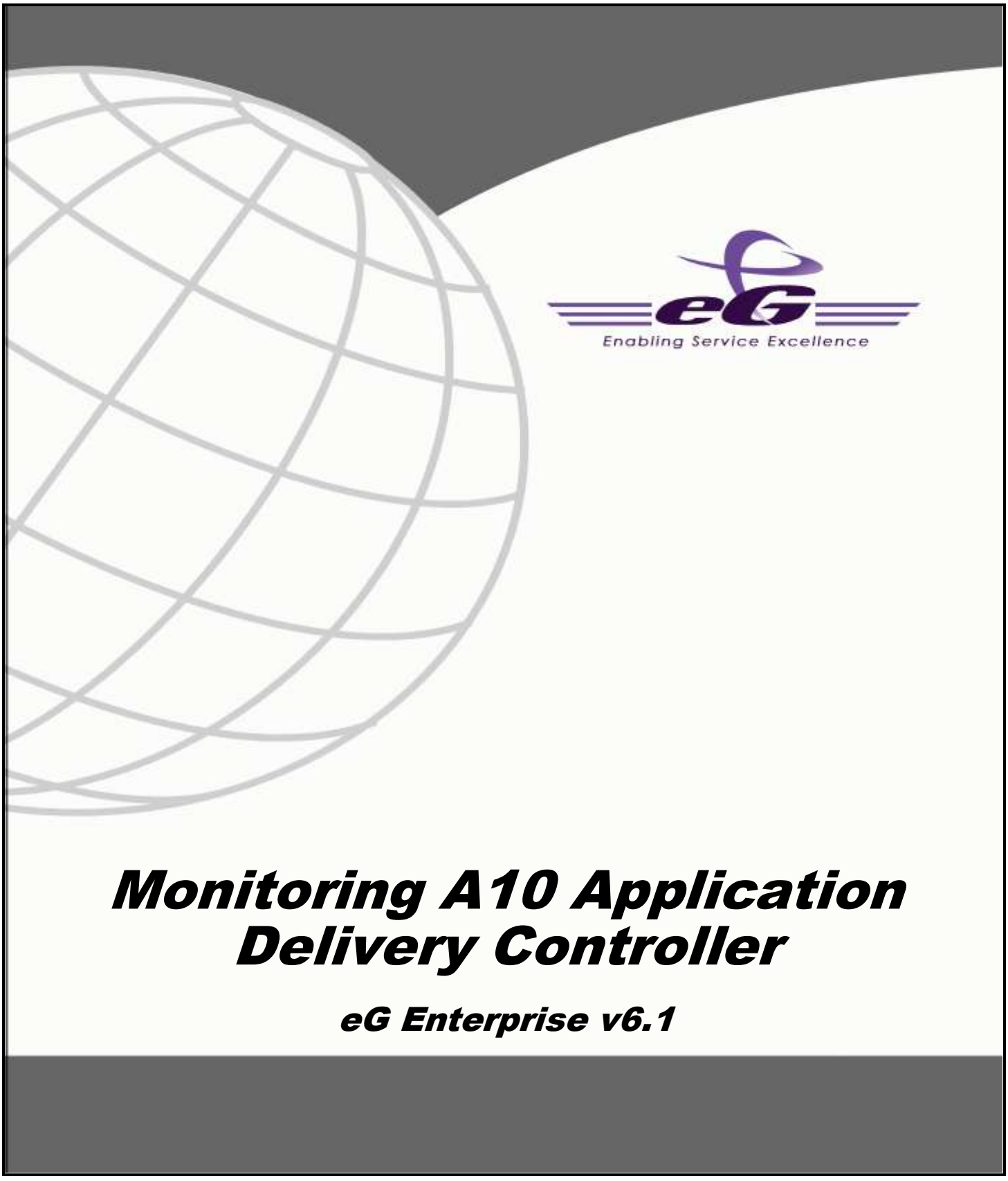

Monitoring A10 Application Delivery Controller

eG Enterprise v6.1

Restricted Rights Legend

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

Trademarks

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

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

Copyright

Table of Contents

1

Monitoring A10 Application Delivery Controller

A10 Application Delivery Controllers (ADCs) are devices that are typically set in front of a web farm within a datacenter. ADCs can off-load common repetitive tasks that are usually performed by web servers, lowering costs while simultaneously increasing speed and improving efficiency.

A10 ADCs can also be thought of as the evolution of server load balancers. ADCs offer advanced features such as content manipulation, Layer 7 health monitoring, and content acceleration.

A10 ADCs provide the ability to direct Internet 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. To ensure this, eG Enterprise provides a specialized *A10 Application Delivery Controller* model

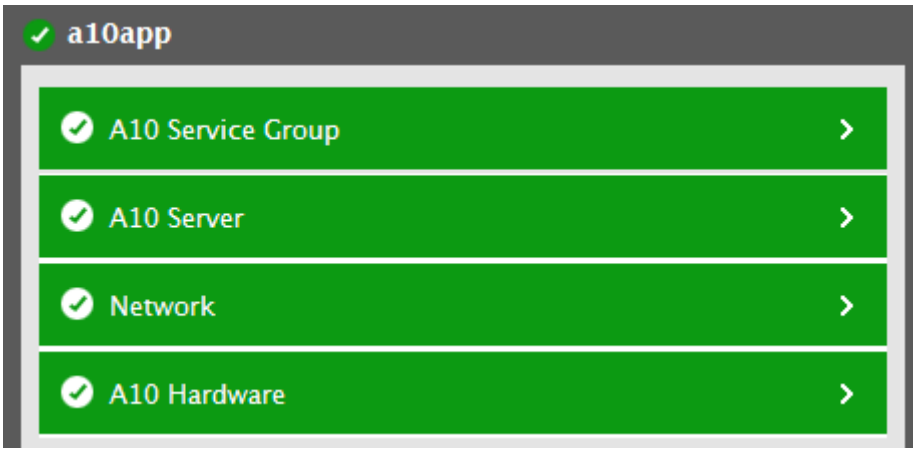

Figure 1: The layer model of the A10 Application Delivery Controller

Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP traps and SNMP MIB of the A10 Application Delivery Controller 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 A10 Application Delivery Controller has been used?
- How well are the disks of the A10 Application Delivery Controller utilized?
- What is the current state of the fans and is any fan running at abnormal speed?
- What is the current status of each power supply unit? Is any power supply unit absent? If so, which ones?
- What is the current state of the sensor of each voltage unit?

- 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?
- What is the current state of the real server port and the virtual server port? Which port is handling the maximum traffic?
- What is the current health state of the service group and service group member of the A10 Application Delivery Controller? How well the client requests are processed by them? Which service group and service group member are handling the maximum amount of traffic?

Since the **Network** layer has been dealt with *Monitoring Web Servers* document, the sections to come will discuss the remaining layers of Figure 1.

1.1 The A10 Hardware Layer

Using the tests mapped to this layer, administrators can identify the resource utilization of the A10 Application Delivery Controller as well as figure out the current state of the hardware components such as the fans, power supply units and the voltage units.

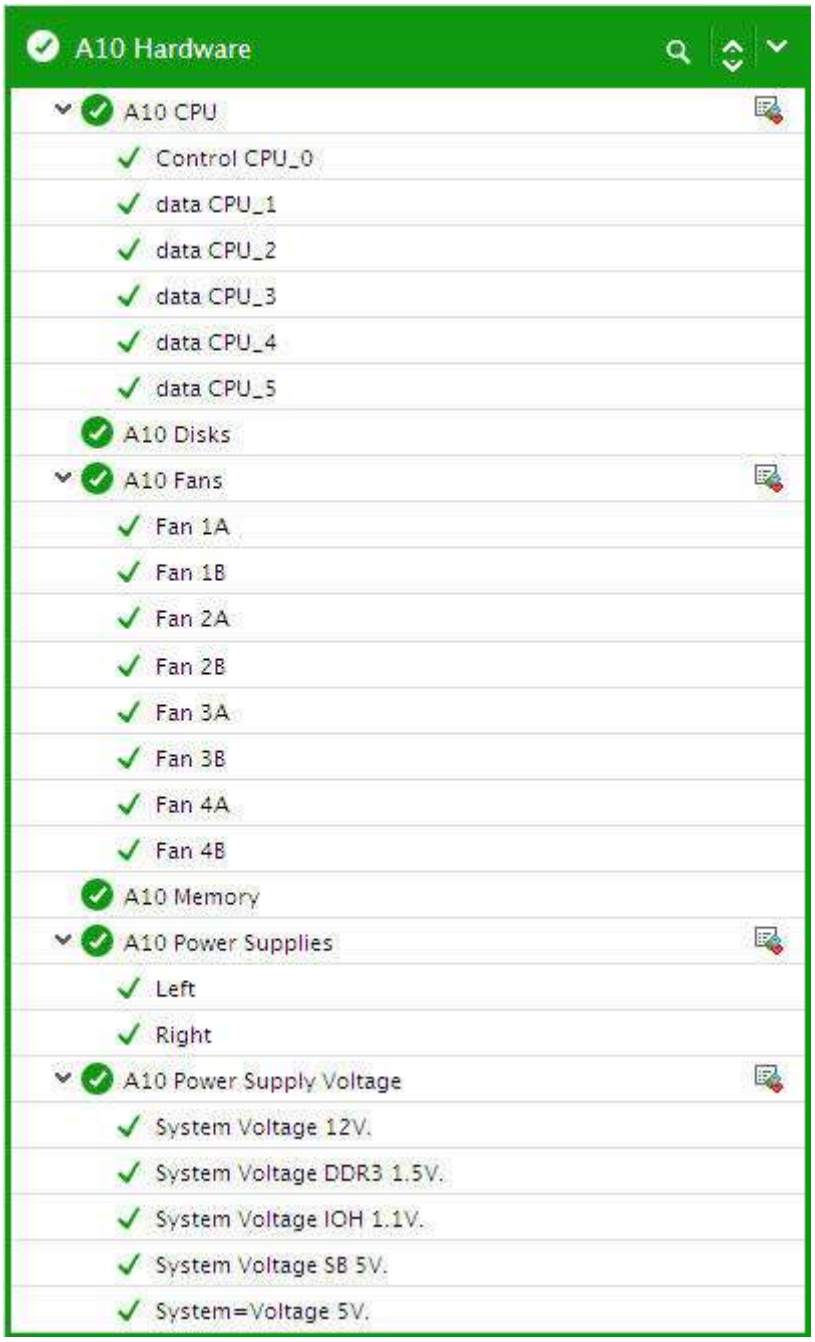

Figure 2: The tests mapped to the A10 Hardware layer

1.1.1 A10 CPU Test

One of the probable reasons for the poor performance of the A10 Application Delivery Controller is excessive CPU usage. Administrators should hence continuously track how well the A10 Application Delivery Controller utilizes CPU resources, so that abnormal usage patterns can be proactively detected and corrected to ensure peak performance of the A10 Application Delivery Controller. This CPU usage check can be performed using the **A10 CPU** test. At configured frequencies, this test monitors the CPU usage levels of the A10 Application Delivery Controller and reports

excessive usage (if any).

Purpose	At configured frequencies, this test monitors the CPU usage levels of the A10 Application Delivery Controller and reports excessive usage (if any).
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for the target A10 Application Delivery Controller

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	CPU usage: Indicates the percentage of CPU used by the A10 Application Delivery Controller.	Percent	A value over 80% is a cause for concern as it indicates excessive CPU usage by the A10 Application Delivery Controller.

1.1.2 A10 Disks Test

This test monitors the space utilization of the disks of the A10 Application Delivery Controller. Using this test, administrators may be proactively alerted to potential space crunch of the disks, if any.

Purpose	Monitors the space utilization of the disks of the A10 Application Delivery Controller. Using this test, administrators may be proactively alerted to potential space crunch of the disks, if any.
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of	One set of results for the target A10 Application Delivery Controller that is to be monitored.

the test			
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total space: Indicates the total capacity of the disks.	GB	
	Used space: Indicates the amount of space used in the disks.	GB	If the value of this measure is close to the Total space measure, then it indicates that the disks are running out of space. To avoid potential space crunch, additional space should be allocated to the disks by the administrators.
	Free space: Indicates the amount of space that is available for use in the disks.	GB	A high value is desired for this measure.
	Space usage: Indicates the percentage of space utilized on the disks of the A10 Application Delivery Controller.	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.

1.1.3 A10 Fans Test

The A10 Application Delivery Controller comprises of fans that helps you to maintain optimal temperature of the core components of the A10 Application Delivery Controller. If one/more fans fail, then the temperature of sensitive hardware may soar causing permanent hardware damage. To avoid such heavy duty damage to the A10 Application delivery Controller, it is necessary to monitor the current state and the operational speed of the fans. This is where the **A10 Fans** test exactly helps! This test auto discovers the fans of the A10 Application Delivery Controller and reports the overall health of each fan and the speed at which the fan operates. This way, administrators can instantly detect a fan failure, initiate remedial measures and proactively prevent any irreparable damage to hardware.

Purpose	Auto discovers the fans of the A10 Application Delivery Controller and reports the overall health of each fan and the speed at which the fan operates
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

<table>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each fan that is operating on the target A10 Application Delivery Controller that is to be 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>Status:
Indicates the current operational state of this fan.</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>Failed</td><td>0</td></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>Not Ready</td><td>2</td></tr><tr><td>Ok</td><td>4,5,6,7</td></tr></table>Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate status of this fan. In the graph of this measure however, the fan status will be represented using the numeric equivalents.</td></tr>
<tr><td></td><td>Speed:
Indicates the current operational speed of this fan.</td><td>Rpm</td><td>The speed of the fan should be well within operable limits. A sudden/significant rise/fall in the value of this measure could be a cause of concern which warrants an investigation.</td></tr>
</table>

1.1.4 A10 Memory Test

This test monitors the memory utilization of the A10 Application Delivery Controller and proactively alerts administrators to potential resource contentions.

Purpose	Monitors the memory utilization of the A10 Application Delivery Controller and proactively alerts administrators to potential resource contentions
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of	One set of results for the target A10 Application Delivery Controller that is to be monitored

the test			
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total memory: Indicates the total amount of memory configured for this A10 Application Delivery Controller.	GB	
	Used memory: Indicates the amount of memory that is currently in use.	GB	A value close to the *Total memory* measure indicates that the memory resources are depleting rapidly.
	Free memory: Indicates the amount of memory that is currently available for use.	GB	A sudden decrease in this value could indicate an unexpected/sporadic spike in the memory utilization of the system. A consistent decrease however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
	Memory usage: Indicates the percentage of memory that is currently utilized.	Percent	A value close to 100 indicates that the memory utilization is at its peak. Administrators may therefore be required to add additional memory resources to the A10 Application Delivery Controller.

1.1.5 A10 Power Supplies Test

This test auto discovers the power supply units of the A10 Applciation Delivery Controller and reports the current state of each power supply unit.

Purpose	Auto discovers the power supply units of the A10 Application Delivery Controller and reports the current state of each power supply unit
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each power supply unit of the A10 Application Delivery Controller that is to be 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>Status:
Indicates the current state of this power supply unit.</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>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr><tr><td>Absent</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the current state of this power supply unit. In the graph of this measure however, the status of this power supply unit will be represented using the numeric equivalents.</td></tr>
</table>

1.1.6 A10 Power Supply Voltage Test

This test auto discovers the voltage units present in the A10 Application Delivery Controller and reports the current state of the sensor of each voltage unit.

Purpose	Auto discovers the voltage units present in the A10 Application Delivery Controller and reports the current state of the sensor of each voltage unit
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for each voltage unit of the A10 Application Delivery Controller that is to be 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>Status:
Indicates the current state of the sensor of this voltage unit.</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>Invalid</td><td>0</td></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the current state of the sensor this voltage unit. In the graph of this measure however, the current state of the sensor this voltage unit will be represented using the numeric equivalents.</td></tr>
</table>

1.2 The A10 Server Layer

With the help of the tests mapped to this layer, you can be promptly alerted to the abnormal state of one/more virtual servers /real servers configured on the A10 Application Delivery Controller, and the irregularities in load balancing amongst the virtual servers/real servers. In addition, administrators may be proactively alerted to the status of the ports on the virtual servers/real servers as well as the irregularities in the traffic on the ports.

Figure 3: The tests mapped to the A10 Server layer

1.2.1 A10 Servers Test

Physical servers a.k.a Real servers are those that are bound to a virtual server in a server farm of the A10 Application Delivery Controller. Whenever a client request is received, 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 VIPs 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 IP and the same set of real servers can be pointed to multiple Virtual IPs to provide more flexibility in the architecture and design of the A10 Application Delivery Controller. The A10 Application 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 IP 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 A10 Application 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 **A10 Servers** test exactly helps!

For each real server configured on the A10 Application Delivery Controller, this test continuously monitors the health of the real servers and reveals how well each server processes client requests. In addition, this test detects inconsistencies in load-balancing early on and warns administrators of possible deviations proactively.

Purpose	For each real server configured on the A10 Application Delivery Controller, this test continuously monitors the health of the real servers and reveals how well each server processes client requests. In addition, this test detects inconsistencies in load-balancing early on and warns administrators of possible deviations proactively.
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each server load balanced using the target A10 Application Delivery Controller</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>Health status:
Indicates the current health of this real server.</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>Disabled</td><td>0</td></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate 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 rowspan="2">Data transmitted:
Indicates the rate at which data was transmitted from this real server during the last measurement period.</td><td>MB/Sec</td><td rowspan="2">Compare the values of these measures across nodes to identify the node that is handling maximum traffic.</td></tr>
<tr><td>Data received:
Indicates the rate at which data was received by this real server during the last measurement period.</td><td>MB/Sec</td></tr>
</table>

	Packets transmitted: Indicates the rate at which the packets were transmitted from this real server during the last measurement period.	Packets/Sec	Compare the value of these measures across the real servers to identify the real server that is experiencing the maximum traffic.
	Packets received: Indicates the rate at which packets were received by this real server during the last measurement period.	Packets/Sec	
	Active connections: Indicates the number of connections that are currently active on this real server.	Number	This measure is a good indicator of the load on the real server.
	Total connections: Indicates the total number of connections established on this real server since the start of the A10 Application Delivery Controller.	Number	
	Connection rate: Indicates the rate at which the connections were established on this real server during the last measurement period.	Conns/Sec	A sudden increase in the value of this measure indicates an increase in the load on the real server.
	Connection usage: Indicates the percentage of connections used by this real server.	Percent	A value close to 100% indicates that the real server is currently overloaded.
	Persistent connections: Indicates the number of connections that were persistent on this real server.	Number	TCP connections that are kept open after transactions complete are called *persistent* connections. . Persistent connections stay open across transactions, until either the client or the server decides to close them. These connections when reused can significantly reduce the overload on the new connections to the real server.
	Peak connections: Indicates the maximum number of connections that were established on this real server since the start of the A10 Application Delivery Controller.	Number	

	L7 requests: Indicates the number of L7 requests currently processed by this real server.	Number	Both these measures serve as effective pointers to the L7 requests processing in the A10 Application Delivery Controller. Layer-7 load balancing, also known as application-level load balancing, is to parse L7 requests in application layer and distribute L7 requests to the servers based on different types of request content, so that it can provide quality of service requirements for different types of content and improve overall performance.
	L7 request rate: Indicates the rate at which the L7 requests were processed by this real server.	Requests/Sec	
	Successful L7 requests: Indicates the number of L7 requests that were processed successfully by this real server.	Number	Ideally the value of this measure should be high.

1.2.2 A10 Server Ports Test

When client requests are sent to the real servers from the Virtual IP of the A10 Application Delivery Controller, the ports at the real servers receive such requests. If the ports are not available or if the ports are already processing too many requests, then the newer client requests may have to wait resulting in poor load balancing capabilities of the A10 Application Delivery Controller. To avoid such discrepancies, it is essential to monitor the current state and the client requests processing statistics of each port on the real servers. This is where the A10 Server Ports helps!

For each port of the real server configured on the A10 Application Delivery Controller, this test continuously monitors the current state of the port and reveals how well each port processes client requests. This way, administrators can detect inconsistencies in load-balancing early on and proactively take remedial measures before end users start complaining.

Purpose	For each port of the real server configured on the A10 Application Delivery Controller, this test continuously monitors the current state of the port and reveals how well each port processes client requests. This way, administrators can detect inconsistencies in load-balancing early on and proactively take remedial measures before end users start complaining.
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the real server port of the target A10 Application Delivery Controller that is to be 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>Port status:
Indicates the current health of this port of the real server.</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>Disabled</td><td>0</td></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the current health of this port of the real server. In the graph of this measure however, the port status will be represented using the numeric equivalents.</td></tr>
<tr><td>Data transmitted:
Indicates the rate at which data was transmitted through this port during the last measurement period.</td><td>MB/Sec</td><td rowspan="2">Compare the values of these measures across the port to identify the port that is handling the maximum traffic.</td></tr>
<tr><td></td><td>Data received:
Indicates the rate at which data was received by this port during the last measurement period.</td><td>MB/Sec</td></tr>
</table>

	Packets transmitted: Indicates the rate at which the packets were transmitted through this port during the last measurement period.	Packets/Sec	Compare the value of these measures across the port to identify the port that is handling the maximum traffic.
	Packets received: Indicates the rate at which packets were received by this port during the last measurement period.	Packets/Sec	
	Active connections: Indicates the number of active connections that were established through this port.	Number	This measure is a good indicator of the load on the real server.
	Total connections: Indicates the total number of connections established this port since the start of the A10 Application Delivery Controller.	Number	
	Connection rate: Indicates the rate at which the connections were established through this port during the last measurement period.	Conns/Sec	A sudden increase in the value of this measure indicates an increase in the traffic handled by the port of the real server.
	Connection usage: Indicates the percentage of active connections that were established through this port.	Percent	A value close to 100% indicates that the traffic through the port is abnormally high. Compare the value across the ports to identify the port through which the maximum number of connections were established.
	Persistent connections: Indicates the number of connections that were persistent on this port.	Number	TCP connections that are kept open after transactions complete are called *persistent* connections. Persistent connections stay open across transactions, until either the client or the server decides to close them. These connections when reused can significantly reduce the traffic overload on the port.
	Peak connections: Indicates the maximum number of connections that were established through this port to the real server since the start of the A10 Application Delivery Controller.	Number	

	L7 requests: Indicates the number of L7 requests currently processed through this port.	Number	Both these measures serve as effective pointers to the L7 requests processing in the A10 Application Delivery Controller. Layer-7 load balancing, also known as application-level load balancing, is to parse L7 requests in application layer and distribute L7 requests to the servers based on different types of request content, so that it can provide quality of service requirements for different types of content and improve overall performance.
	L7 request rate: Indicates the rate at which the L7 requests were processed through this port.	Requests/Sec	
	Successful L7 requests: Indicates the number of L7 requests that were processed successfully through this port.	Number	Ideally the value of this measure should be high.

1.2.3 A10 Virtual Servers Test

The A10 Application Delivery Controller consists of a virtual server (also referred to as a virtual cluster, virtual IP or VIP) which, in turn, consists of an IP address and port. This virtual server is bound to a number of physical servers a.k.a real servers within a server farm. On the A10 Application Delivery Controller, a virtual server (VIP) is typically a publicly facing IP address which responds to user requests. Typically, load balancing, content switching and persistence rules and methods are assigned on a per-VIP basis. A virtual server is capable of performing the following:

- Distribute client requests across multiple servers to balance server load;
- Apply various behavioral settings to a specific type of traffic;
- Enable persistence for a specific type of traffic;
- Direct traffic according to user-written iRules®

In addition, virtual servers can also be used in the following ways:

- Directing traffic to a load balancing pool;
- Sharing an IP address with a VLAN node;
- Forwarding traffic to a specific destination IP address;
- Increasing the speed of processing HTTP traffic;
- Increasing the speed of processing Layer 4 traffic;
- Relaying DHCP traffic

Since the virtual servers are able to manage the traffic and divert client 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 A10 Application Delivery Controller. To avoid this, you can configure the periodic execution of the **A10 Virtual Servers** test. For each virtual server configured on the A10 Application Delivery Controller, this test continuously monitors the load on the load-balancing virtual servers and reveals how well each server processes client requests. In addition, this test detects inconsistencies in load-balancing early on and warns administrators of possible deviations proactively.

Purpose	For each virtual server configured on the A10 Application Delivery Controller, this test continuously monitors the load on the load-balancing virtual servers and reveals how well each server processes client requests. In addition, this test detects inconsistencies in load-balancing early on and warns administrators of possible deviations proactively.
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the target Virtual server configured on the A10 Application Delivery Controller that is to be monitored</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>Health status:
Indicates the current health of this virtual server.</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>Disabled</td><td>0</td></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate status of this virtual server. In the graph of this measure however, the current health will be represented using the numeric equivalents.</td></tr>
<tr><td>Data transmitted:
Indicates the rate at which data was transmitted from this virtual server during the last measurement period.</td><td>MB/Sec</td><td rowspan="2">Compare the values of these measures across the virtual servers to identify the server that is handling maximum traffic.</td></tr>
<tr><td>Data received:
Indicates the rate at which data was received by this virtual server during the last measurement period.</td><td>MB/Sec</td></tr>
</table>

	Packets transmitted: Indicates the rate at which the packets were transmitted from this virtual server during the last measurement period.	Packets/Sec	Compare the value of these measures across the virtual servers to identify the server that is experiencing the maximum traffic.
	Packets received: Indicates the rate at which packets were received by this virtual server during the last measurement period.	Packets/Sec	
	Active connections: Indicates the number of connections that are currently active on this virtual server.	Number	This measure is a good indicator of the load on the virtual server.
	Total connections: Indicates the total number of connections established on this virtual server since the start of the A10 Application Delivery Controller.	Number	
	Connection rate: Indicates the rate at which the connections were established on this virtual server during the last measurement period.	Conns/Sec	A sudden increase in the value of this measure indicates an increase in the load on the virtual server.
	Connection usage: Indicates the percentage of connections used by this virtual server.	Percent	A value close to 100% indicates that the virtual server is currently overloaded.
	Persistent connections: Indicates the number of connections that were persistent on this virtual server.	Number	TCP connections that are kept open after transactions complete are called *persistent* connections. . Persistent connections stay open across transactions, until either the client or the server decides to close them. These connections when reused can significantly reduce the overload on the new connections to the virtual server.
	Peak connections: Indicates the maximum number of connections that were established on this virtual server since the start of the A10 Application Delivery Controller.	Number	

	L7 requests: Indicates the number of L7 requests currently processed by this virtual server.	Number	Both these measures serve as effective pointers to the L7 requests processing in the A10 Application Delivery Controller. Layer-7 load balancing, also known as application-level load balancing, is to parse L7 requests in application layer and distribute L7 requests to the servers based on different types of request content, so that it can provide quality of service requirements for different types of content and improve overall performance.
	L7 request rate: Indicates the rate at which the L7 requests were processed by this virtual server.	Requests/Sec	
	Successful L7 requests: Indicates the number of L7 requests that were processed successfully by this virtual server.	Number	Ideally the value of this measure should be high.

1.2.4 A10 Virtual Server Ports Test

The client requests are received through the ports of the Virtual servers. If the port is down or if the port is handling too much of traffic, then the client requests may have to wait until the time the port can handle the requests. This time lag may gradually affect the load balancing capability of the A10 Application Delivery Controller. To keep check on how well the ports are handling the client requests, you may want to use the A10 Virtual Server Ports test. For each virtual server port, this test monitors the current state of the port and reveals how well the port is processing the client requests. This way, administrators may be alerted to the discrepancies in the port and remedial measures can be taken proactively without compromising on the load balancing capability of the A10 Application Delivery Controller.

Purpose	For each virtual server port, this test monitors the current state of the port and reveals how well the port is processing the client requests
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each virtual server port of the target A10 Application Delivery Controller that is to be 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>Port status:
Indicates the current state of this port of the virtual server.</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>Disabled</td><td>0</td></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the current health of this port of the virtual server. In the graph of this measure however, the status of the port will be represented using the numeric equivalents.</td></tr>
<tr><td>Data transmitted:
Indicates the rate at which data was transmitted through this port during the last measurement period.</td><td>MB/Sec</td><td rowspan="2">Compare the values of these measures across the port to identify the port that is handling the maximum traffic.</td></tr>
<tr><td></td><td>Data received:
Indicates the rate at which data was received by this port during the last measurement period.</td><td>MB/Sec</td></tr>
</table>

	Packets transmitted: Indicates the rate at which the packets were transmitted through this port during the last measurement period.	Packets/Sec	Compare the value of these measures across the port to identify the port that is handling the maximum traffic.
	Packets received: Indicates the rate at which packets were received by this port during the last measurement period.	Packets/Sec	
	Active connections: Indicates the number of active connections that were established through this port.	Number	This measure is a good indicator of the load on the virtual server.
	Total connections: Indicates the total number of connections established this port since the start of the A10 Application Delivery Controller.	Number	
	Connection rate: Indicates the rate at which the connections were established through this port during the last measurement period.	Conns/Sec	A sudden increase in the value of this measure indicates an increase in the traffic handled by the port of the virtual server.
	Connection usage: Indicates the percentage of active connections that were established through this port.	Percent	A value close to 100% indicates that the traffic through the port is abnormally high. Compare the value across the ports to identify the port through which the maximum number of connections were established.
	Persistent connections: Indicates the number of connections that were persistent on this port.	Number	TCP connections that are kept open after transactions complete are called *persistent* connections. Persistent connections stay open across transactions, until either the client or the server decides to close them. These connections when reused can significantly reduce the traffic overload on the port.
	Peak connections: Indicates the maximum number of connections that were established through this port to the real server since the start of the A10 Application Delivery Controller.	Number	

	L7 requests: Indicates the number of L7 requests currently processed through this port.	Number	Both these measures serve as effective pointers to the L7 requests processing in the A10 Application Delivery Controller. Layer-7 load balancing, also known as application-level load balancing, is to parse L7 requests in application layer and distribute L7 requests to the servers based on different types of request content, so that it can provide quality of service requirements for different types of content and improve overall performance.
	L7 request rate: Indicates the rate at which the L7 requests were processed through this port.	Requests/Sec	
	Successful L7 requests: Indicates the number of L7 requests that were processed successfully through this port.	Number	Ideally the value of this measure should be high.

1.3 The A10 Service Group Layer

With the help of the tests mapped to this layer, you can be promptly alerted to the abnormal state of one/more service groups/service group members configured on the A10 Application Delivery Controller, and the irregularities in load balancing amongst the service groups/service group members.

Figure 4: The tests mapped to the A10 Service Group layer

1.3.1 A10 Service Groups Test

In a typical client – server scenario, a client request is directed to the destination IP address specified in the header of the request. For sites with huge volumes of traffic, the destination server may be quickly overloaded, Therefore, it is imperative to create a load balancing pool which is in other words called a service group in an A10 Application Delivery Controller. A service group is a logical set of real servers, such as web servers, that you group together to receive and process traffic. Instead of sending client traffic to the destination IP address specified in the client request, the Virtual server of the A10 Application Delivery Controller sends the request to any of the servers that are members of that service group. This helps to efficiently distribute the load on your server resources. In order to efficiently distribute the load across the servers, it is essential to constantly monitor the health and request processing capability of the service groups. This is where the **A10 Service Group** test helps.

For each service group configured on the A10 Application Delivery Controller, this test monitors the current health and reveals the request processing ability of the service groups. Using this test, administrator can figure out the service group that is handling the maximum requests and also identify the exact cause on why a service group is slow in processing the requests

Purpose	For each service group configured on the A10 Application Delivery Controller, this test monitors the current health and reveals the request processing ability of the service groups
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each service group on the target A10 Application Delivery Controller 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>Health status:
Indicates the current health of this service group.</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>Disabled</td><td>0</td></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the current health of the service group. In the graph of this measure however, the health of the service group will be represented using the numeric equivalents.</td></tr>
<tr><td rowspan="2">Data transmitted:
Indicates the rate at which data was transmitted from this service group during the last measurement period.</td><td>MB/Sec</td><td rowspan="2">Compare the values of these measures across service groups to identify the service group that is handling maximum traffic.</td></tr>
<tr><td>Data received:
Indicates the rate at which data was received by this service group during the last measurement period.</td><td>MB/Sec</td></tr>
</table>

	Packets transmitted: Indicates the rate at which the packets were transmitted from this service group during the last measurement period.	Packets/Sec	Compare the value of these measures across the service groups to identify the service group that is experiencing the maximum traffic.
	Packets received: Indicates the rate at which packets were received by this service group during the last measurement period.	Packets/Sec	
	Active connections: Indicates the number of connections that are currently active on this service group.	Number	This measure is a good indicator of the load on the service group.
	Total connections: Indicates the total number of connections established on this service group since the start of the A10 Application Delivery Controller.	Number	
	Connection rate: Indicates the rate at which the connections were established on this service group during the last measurement period.	Conns/Sec	A sudden increase in the value of this measure indicates an increase in the load on the service group.
	Connection usage: Indicates the percentage of connections used by this service group.	Percent	A value close to 100% indicates that the service group is currently overloaded.
	Persistent connections: Indicates the number of connections that were persistent on this service group.	Number	TCP connections that are kept open after transactions complete are called *persistent* connections. Persistent connections stay open across transactions, until either the client or the server decides to close them. These connections when reused can significantly reduce the overload on the new connections to the service group.
	Peak connections: Indicates the maximum number of connections that were established on this service group since the start of the A10 Application Delivery Controller.	Number	

	L7 requests: Indicates the number of L7 requests currently processed by this service group.	Number	Both these measures serve as effective pointers to the L7 requests processing in the A10 Application Delivery Controller. Layer-7 load balancing, also known as application-level load balancing, is to parse L7 requests in application layer and distribute L7 requests to the servers based on different types of request content, so that it can provide quality of service requirements for different types of content and improve overall performance.
	L7 request rate: Indicates the rate at which the L7 requests were processed by this service group.	Requests/Sec	
	Successful L7 requests: Indicates the number of L7 requests that were processed successfully by this service group.	Number	Ideally the value of this measure should be high.

1.3.2 A10 Service Group Members Test

A typical service group comprises of a number of real servers that are termed as service group members. A real server may be part of any number of service groups thus providing better load balancing capabilities. For each service group member, this test reports the current health status of the service group and reveals how well each service group member is capable of handling client requests. This way, administrators can detect any discrepancy with load balancing and rectify the same before end users start complaining.

Purpose	For each service group member, this test reports the current health status of the service group and reveals how well each service group member is capable of handling client requests.
Target of the test	An A10 Application Delivery Controller
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the A10 Application Delivery Controller. 3. **SNMPPORT** – The SNMP Port number of the A10 Application Delivery Controller (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 A10 Application delivery Controller over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each service group: service group member of the target A10 Application Delivery Controller 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>Health status:
Indicates the current health of this service group member.</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>Disabled</td><td>0</td></tr><tr><td>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table>
Note:
By default, this measure reports one of the Measure Values listed in the table above to indicate the current health of the service group member. In the graph of this measure however, the health of the service group member will be represented using the numeric equivalents.</td></tr>
<tr><td>Data transmitted:
Indicates the rate at which data was transmitted from this service group member during the last measurement period.</td><td>MB/Sec</td><td rowspan="2">Compare the values of these measures across service group members to identify the member that is handling maximum traffic.</td></tr>
<tr><td></td><td>Data received:
Indicates the rate at which data was received by this service group member during the last measurement period.</td><td>MB/Sec</td></tr>
</table>

	Packets transmitted: Indicates the rate at which the packets were transmitted from this service group member during the last measurement period.	Packets/Sec	Compare the value of these measures across the service group members to identify the member that is experiencing the maximum traffic.
	Packets received: Indicates the rate at which packets were received by this service group member during the last measurement period.	Packets/Sec	
	Active connections: Indicates the number of connections that are currently active on this service group member.	Number	This measure is a good indicator of the load on the service group member.
	Total connections: Indicates the total number of connections established on this service group member since the start of the A10 Application Delivery Controller.	Number	
	Connection rate: Indicates the rate at which the connections were established on this service group member during the last measurement period.	Conns/Sec	A sudden increase in the value of this measure indicates an increase in the load on the service group member.
	Connection usage: Indicates the percentage of connections used by this service group member.	Percent	A value close to 100% indicates that the service group member is currently overloaded.
	Persistent connections: Indicates the number of connections that were persistent on this service group member.	Number	TCP connections that are kept open after transactions complete are called *persistent* connections. Persistent connections stay open across transactions, until either the client or the server decides to close them. These connections when reused can significantly reduce the overload on the new connections to the service group member.

	Peak connections: Indicates the maximum number of connections that were established on this service group member since the start of the A10 Application Delivery Controller.	Number	
	L7 requests: Indicates the number of L7 requests currently processed by this service group member.	Number	Both these measures serve as effective pointers to the L7 requests processing in the A10 Application Delivery Controller. Layer-7 load balancing, also known as application-level load balancing, is to parse L7 requests in application layer and distribute L7 requests to the servers based on different types of request content, so that it can provide quality of service requirements for different types of content and improve overall performance.
	L7 request rate: Indicates the rate at which the L7 requests were processed by this service group member.	Requests/Sec	
	Successful L7 requests: Indicates the number of L7 requests that were processed successfully by this service group member.	Number	Ideally the value of this measure should be high.

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 **A10 Application Delivery Controller**. 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.