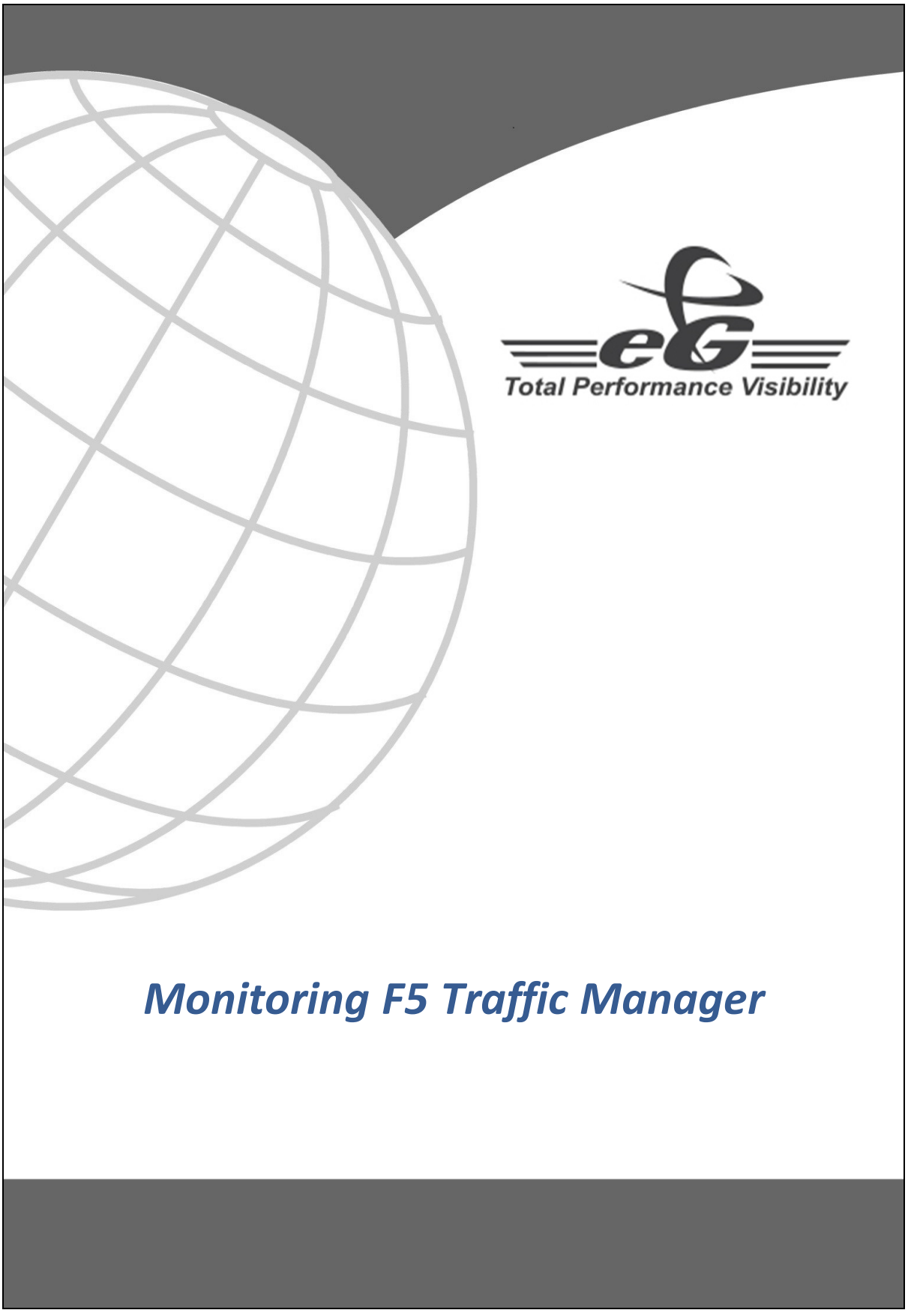

Monitoring F5 Traffic Manager

Table of contents

MONITORING THE BIG-IP LOCAL TRAFFIC MANAGER (LTM) 1
1.1 The F5 TM Hardware Layer 2
1.1.1 F5 CPUs Test 2
1.1.2 F5 Disk Usage Test 4
1.1.3 F5 Fans Test 6
1.1.4 F5 Power Modules Test 8
1.1.5 F5 Temperature Test 10
1.1.6 F5 CPU Usage Test 12
1.1.7 F5 Memory Usage Test 14
1.1.8 The Network Layer 16
1.2 The F5 TM Server Layer 16
1.2.1 F5 Virtual Server Status Test 17
1.2.2 F5 Virtual Servers Test 20
1.3 The F5 TM Service Layer 24
1.3.1 F5 Nodes Test 24
1.3.2 F5 Pools Test 29
1.3.3 F5 Pools Details Test 32
1.3.4 F5 Pool Members Test 35
1.3.5 F5 Traffic Management Module Test 38
CONCLUSION 44

Table of Figures

Figure 1.1: Layer model of the F5 Traffic Manager 1
Figure 1.2: The tests mapped to the F5 TM Hardware layer 2
Figure 1.3: The test mapped to the Network layer 16
Figure 1.4: The tests mapped to the F5 TM Server Layer 17
Figure 1.5: The test mapped to the F5 TM Service Layer 24

Monitoring the BIG-IP Local Traffic Manager (LTM)

The BIG-IP Local Traffic Manager (LTM) is an application delivery networking system that secures, optimizes, and delivers applications.

This system provides a suite of security services that enhance network and protocol level security, filter application attacks, and thus protect your mission-critical applications. In addition, the BIG-IP Local Traffic Manager removes single points of failure and virtualizes the network and applications using industry-leading L7 intelligence. Furthermore, it includes static and dynamic load balancing methods, which track dynamic performance levels of servers in a group and ensures that all sites are always on, more scalable, and easier to manage.

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 LTM is of paramount importance. To ensure this, eG Enterprise provides a specialized *F5 Traffic Manager* model.

Figure 1.1: Layer model of the F5 Traffic Manager

By periodically polling the SNMP MIB of the traffic manager, the eG external agent extracts useful metrics revealing the availability of the manager, the resource usage of the manager, the status of the pools managed by the manager, and more! With the help of these metrics, the following questions can be answered easily and accurately:

- Is the LTM available over the network? If so, how quickly is it responding to requests?
- Is any network interface supported by the LTM consuming bandwidth excessively?
- Which is the faster network interface supported by the LTM?
- Is the CPU temperature very high?
- Are any disk partitions on the LTM over-utilized? If so, which ones?

- Has any chassis fan on the LTM failed? If so, which one?
- Is any chassis fan functioning at abnormal speed?
- Is the temperature of any chassis temperature sensor abnormally high?
- What is the current state of each pool configured on the LTM?
- Is any virtual server disabled currently? If so, was it disabled by the parent?

The sections that will follow will discuss each of the layers depicted by Figure 1.1 above.

1.1 The F5 TM Hardware Layer

This layer monitors the critical hardware components of the traffic manager such as CPUs, disk partitions, fans, and temperature sensors, and proactively alerts administrators to hardware failures.

Figure 1.2: The tests mapped to the F5 TM Hardware layer

1.1.1 F5 CPUs Test

This test reports the temperature and fan speed of the CPU supported by the traffic manager.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU temperature:	Indicates the current temperature of the CPU.	Celcius	A high value of this measure is a cause for concern.
CPU fan speed:	Indicates the current fan speed of the CPU.	Rpm	Ideally, the speed of the fan should be within permissible limits.

1.1.2 F5 Disk Usage Test

This test reports the space usage of each disk partition on the traffic manager, and thus indicates which disk is currently running out of space.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk partition in the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total space:	Indicates the total available space in this disk partition.	MB	
Free space:	Indicates the free space in this disk partition.	MB	
Used space:	Indicates the amount of space that has been used up on this partition.	MB	
Percent free space:	Indicates the percentage of free space in this disk	Percent	Ideally, the value of this measure should be high. A low value is indicative of

Measurement	Description	Measurement Unit	Interpretation
	partition.		excessive space usage on the disk partition. Compare the value of this measure across disk partition to accurately identify which partition is facing a potential space crunch.

1.1.3 F5 Fans Test

This test reports the current state and speed of each fan supported by the traffic manager.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each chassis fan supported by the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
16. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the **DETAILED DIAGNOSIS** capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

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

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurements	Description	Measurement Unit	Interpretation
Chassis fan status:	Indicates the current status of this fan.	Boolean	Ideally, the value for this measure should be 1, which means the Fan is in good state and it is enabled. If this measure reports the value of 0 or 2, then it implies that the fan is in bad state or the fan is not present. Use the detailed diagnosis of this measure to know exactly what state the numeric value reported by the test represents.
Chassis fan speed:	Indicates the actual speed of this chassis fan.	Rpm	Ideally, the speed of the fan should be within permissible limits.

1.1.4 F5 Power Modules Test

This test reports the current status of the chassis power supply thus proactively alerting the administrators of abnormalities in the power supply, if any.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each chassis power supply supported by the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurements	Measurement	Measurement Unit	Interpretation
Chassis power status:	Indicates the current status of this chassis power supply.		The values that this measure can report and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurements</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Bad</td><td>0</td></tr>
<tr><td>Good</td><td>1</td></tr>
<tr><td>Not present</td><td>2</td></tr>
</table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of the chassis power supply. However, the graph of this measure is indicated using the numeric equivalents 0 - 2 only.
</td></tr>
</table>

1.1.5 F5 Temperature Test

This test reports the current temperature of the chassis temperature sensor. **Note that this test is only supported on those platforms in which the sensor data is available**.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **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.
12. **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
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurements	Measurement	Measurement Unit	Interpretation
Chassis temperature:	Indicates the current temperature of the chassis temperature sensor.	Celsius	Ideally, the value should be low. A high value could be a cause for concern.

1.1.6 F5 CPU Usage Test

This test reports the current utilization of each CPU available in the Traffic Manager. Using this test, administrators can be proactively alerted to abnormal CPU utilization so that further investigation could be warranted and the real cause of resource contention be identified.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each CPU of the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has

access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.

8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **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.
12. **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
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization:	Indicates the percentage	Percent	Ideally, the value should be low. An

Measurement	Description	Measurement Unit	Interpretation
	utilization of this CPU in the traffic manager.		unusually high value or a consistent increase in this value is indicative of abnormal CPU usage which requires further investigation.

1.1.7 F5 Memory Usage Test

This test monitors the memory utilization of the Traffic Manager and proactively alerts administrators to potential resource contention.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for the traffic manager being monitored

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurements	Description	Measurement Unit	Interpretation
Total memory:	Indicates the current memory that is available in this traffic manager.	MB	
Used memory:	Indicates the amount of memory that is already used by this traffic manager.	MB	A low value is desired for this measure.
Memory utilization:	Indicates the percentage of memory that is utilized by this traffic manager.	Percent	A low value is desired for this measure. While sporadic spikes in memory usage could be caused by one/more rogue processes on the traffic manager, a consistent increase in this

Measurements	Description	Measurement Unit	Interpretation
			value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources.
Free memory:	Indicates the amount of memory that is available for use in this traffic manager.	MB	A sudden decrease in this value could indicate an unexpected/sporadic spike in the memory utilization of the traffic manager. A consistent decrease however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.

1.1.8 The Network Layer

Use the **Network** test mapped to this layer to assess the health of network connections to and from the traffic manager. Since this test has been discussed adequately in the *Monitoring Unix and Windows servers* document, let us proceed to the next layer.

Figure 1.3: The test mapped to the Network layer

1.2 The F5 TM 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 in the pools configured on the traffic manager, and the irregularities in load balancing amongst the virtual servers.

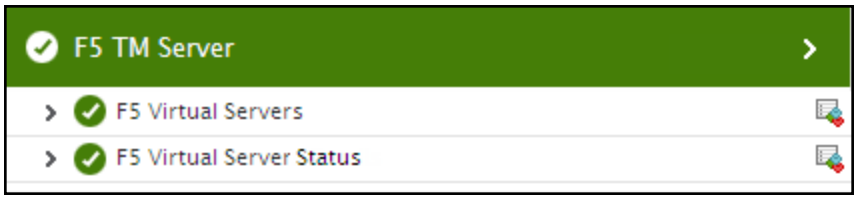

Figure 1.4: The tests mapped to the F5 TM Server Layer

The section that will follow will discuss the **F5 Virtual Server Status** test alone, as the **TcpPortStatus** test has been dealt with extensively in the previous chapters.

1.2.1 F5 Virtual Server Status Test

A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients on an external network can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions. The main purpose of a virtual server is often to balance traffic load across a pool of servers on an internal network. Virtual servers increase the availability of resources for processing client requests.

Not only do virtual servers distribute traffic across multiple servers, they also treat varying types of traffic differently, depending on your traffic-management needs. Therefore, the avalibility of the virtual servers in the system is imperative for balancing the load. The **F5 virtual Servers** test exactly helps administrators in identifying the availiabity status of the virtual servers.

This test reports the current availability status of each virtual server in a pool and if the virtual server is available, this tests reports the current activity status of each virtual server.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each virtual server in the pools configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurements	Description	Measurement Unit	Interpretation
Virtual server available status:	Indicates the current status of this virtual server.		The values that this measure can report and its numeric equivalents are

<table>
<tr><th>Measurements</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>None</td><td>0</td></tr><tr><td>Available</td><td>1</td></tr><tr><td>Currently not available</td><td>2</td></tr><tr><td>Offline</td><td>3</td></tr><tr><td>Unknown</td><td>4</td></tr><tr><td>Unlicensed</td><td>5</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of the virtual server. However, the graph of this measure is indicated using the numeric equivalents 0 - 5 only.</td></tr>
<tr><td>Virtual server activity status:</td><td>Indicates the current activity status of this virtual server as specified by the user.</td><td></td><td>This measure appears only if the Virtual server available status measure reports the Measure ValueAvailable.
The values that this measure can report and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>None</td><td>0</td></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>2</td></tr><tr><td>Disabled by parent</td><td>3</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current activity status of</td></tr>
</table>

Measurements	Description	Measurement Unit	Interpretation
			the virtual server. However, the graph of this measure is indicated using the numeric equivalents 0 - 3 only.

1.2.2 F5 Virtual Servers Test

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 load balancing system.To avoid this, you can configure the periodic execution of the **F5 Virtual Servers** test. For each virtual server configured on the traffic manager, 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 : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each pool configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager

3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 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. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **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.
12. **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

13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
17. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the **DETAILED DIAGNOSIS** capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.
    The option to selectively enable/disable the **DETAILED DIAGNOSIS** capability will be available only if the following conditions are fulfilled:
    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurements	Description	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data is transmitted from this virtual server during the last measurement period.	MB/Sec	Compare the value of these measures across the virtual servers to identify the server that is experiencing the maximum traffic.
Data received:	Indicates the rate at which data is received by this virtual server during the last measurement period.	MB/Sec	
Packets transmitted:	Indicates the rate at which 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 handling maximum traffic.

Measurements	Description	Measurement Unit	Interpretation
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 restart of the traffic manager.	Number	
Connection during the last measure period:	Indicates the rate at which connections were established during the last measurement period.	Conns/Sec	
Connection usage:	Indicates the percentage of connections that were used by this virtual server.	Percent	A value close to 100% indicates that the virtual server is currently overloaded.
Maximum connections established:	Indicates the maximum number of connections that were established on this virtual server since the start of the traffic manager.	Number	
Requests:	Indicates the rate at which requests were processed by this virtual server.	Requests/sec	
CPU usage:	Indicates the percentage of time this virtual server was busy during the past minute.	Percent	A value close to 100 is a cause of concern.

Measurements	Description	Measurement Unit	Interpretation
Average time for all connections:	Indicates the average time required for establishing all the connections to this virtual server.	Milliseconds	A sudden/gradual increase in the value of this measure may indicate connection issues to the virtual server.

1.3 The F5 TM Service Layer

Quickly detect changes in the status of the pools configured on the traffic manager using the test mapped to this layer.

Figure 1.5: The test mapped to the F5 TM Service Layer

1.3.1 F5 Nodes Test

Nodes are the network devices to which a BIG-IP® local traffic management system passes traffic. You can explicitly create a node, or you can instruct the BIG-IP system to automatically create one when you add a pool member to a load balancing pool. Nodes are the basis for creating a load balancing pool. For any server that you want to be part of a load balancing pool, you must first create a node i.e., designate that server as a node. After designating the server as node, you can add the node to a pool as a pool member. Therefore it becomes essential to check the status of each node and the load through each node in the system so that load balancing is maintained consistently. This test exactly does the same.

This test reports the current status of each of the nodes configured on the traffic manager and tracks the data/packet traffic through each node. In addition, this test also reports how well the connections are utilized by the nodes and the active connections on each node.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each node configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

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

    The option to selectively enable/disable the **DETAILED DIAGNOSIS** capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurements	Measurement	Measurement Unit	Interpretation
Node available status:	Indicates the current status of this node.	Boolean	The values that this measure can report and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** **None** / 0 **Available** / 1 **Currently not available** / 2 **Offline** / 3 **Unknown** / 4 **Unlicensed** / 5 Note: By default, this measure can report the **Measure Value**s mentioned above while indicating the current status of the node. However, the graph of this measure is indicated using the numeric

<table>
<tr><th>Measurements</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>equivalents 0 - 5 only.</td></tr>
<tr><td>Node activity status:</td><td>Indicates the current activity status of this pool as specified by the user.</td><td></td><td>The values that this measure can report and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>None</td><td>0</td></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>2</td></tr><tr><td>Disabled by parent</td><td>3</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current activity status of the node. However, the graph of this measure is indicated using the numeric equivalents 0 - 3 only.</td></tr>
<tr><td>Data transmitted:</td><td>Indicates the rate at which data is transmitted from this node 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:</td><td>Indicates the rate at which data is received in this node during the last measurement period.</td><td>MB/Sec</td></tr>
<tr><td>Packets transmitted:</td><td>Indicates the rate at which packets were</td><td>Packets/Sec</td><td>Compare the values of these measures to identify the node that is experiencing maximum</td></tr>
</table>

Measurements	Measurement	Measurement Unit	Interpretation
	transmitted from this node during the last measurement period.		traffic.
Packets received:	Indicates the rate at which packets were received in this node during the last measurement period.	Packets/Sec	
Active connections:	Indicates the number of connections that are currently active on this node.	Number	
Total connections:	Indicates the total number of connections established on this node since the start of the traffic manager.	Number	
Connection usage:	Indicates the percentage of connections that were used by this node.	Percent	
Connection during the last measure period:	Indicates the rate at which connections were established during the last measurement period.	Conns/Sec	
Maximum connections established:	Indicates the maximum number of connections that were established on this node since the start of the traffic manager.	Number	
Requests:	Indicates the rate at which the requests were processed by this node.	Requests/Sec	This measure is a good indicator of the workload on the node. Comparing the value of this measure across

Measurements	Measurement	Measurement Unit	Interpretation
			nodes will help you determine whether all the requests have been processed or not. Request processing bottlenecks if any, can thus be isolated and resolved.

1.3.2 F5 Pools 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. A load balancing pool is a logical set of devices, 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, Local Traffic Manager sends the request to any of the servers that are members of that pool. 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 availability of the load balancing pools. This is where the **F5 Pools** test helps.

This test reports the current status of each of the pools configured on the traffic manager and if the pool is available, this test reports the activity status of each pool.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each pool configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
16. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

    The option to selectively enable/disable the **DETAILED DIAGNOSIS** capability will be available only if the following conditions are fulfilled:

    - The eG manager license should allow the detailed diagnosis capability
    - Both the normal and abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurements</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Pool available status:</td><td>Indicates the current status of this pool.</td><td></td><td>The values that this measure can report and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>None</td><td>0</td></tr><tr><td>Available</td><td>1</td></tr><tr><td>Currently not available</td><td>2</td></tr><tr><td>Offline</td><td>3</td></tr><tr><td>Unknown</td><td>4</td></tr><tr><td>Unlicensed</td><td>5</td></tr></table>Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of the pool. However, the graph of this measure is indicated using the numeric equivalents 0 - 5 only.</td></tr>
<tr><td>Pool activity status:</td><td>Indicates the current activity status of this pool as specified by the user.</td><td></td><td>The values that this measure can report and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>None</td><td>0</td></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>2</td></tr><tr><td>Disabled by parent</td><td>3</td></tr></table>Note:
By default, this measure can report the Measure Values mentioned above while indicating the current activity status of the pool. However, the graph of this measure is indicated using the numeric</td></tr>
</table>

Measurements	Description	Measurement Unit	Interpretation
			equivalents 0 - 3 only.

1.3.3 F5 Pools Details Test

The Local Traffic Manager can be configured to perform a number of different operations for a load balancing pool such as:

- Associate health monitors with pools and pool members
- Enable or disable SNAT connections
- Rebind a connection to a different pool member if the originally-targeted pool member becomes unavailable
- Specify a load balancing algorithm for a pool
- Set the Quality of Service or Type of Service level within a packet
- Assign pool members to priority groups within a pool

With the help of the load balancing pool, client requests can be evenly distributed across the servers of the pool. Sometimes, the load balancing pools may not be able to handle the client requests owing to performance issues or lack of resources which may inturn cause irregularities in load balancing. To avoid such a situation, you need to monitor the load balancing pools at periodic intervals. The **F5 Pools Details** test exactly does the same. Using this test, administrators can determine the following:

- How well each load balancing pool is handling the data/packet traffic?;
- How many connections are handled by the pool and how many are currently active on the pool?;
- How many connections have been used and how many maximum connections are established in the pool since the start of the traffic manager?

This way, administrators can constantly keep a vigil on the load balancing pool and proactively avoid performance and load balancing issues, if any.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each pool configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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 Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set **to** No.

Measurements made by the test

Measurements	Decription	Measurement Unit	Interpretation
Data transmitted:	Indicates the rate at which data is transmitted from this pool during the last measurement period.	MB/Sec	Compare the values of these measures across the pools to identify the pool that is experiencing the maximum traffic.
Data received:	Indicates the rate at which data is received in this pool during the last measurement period.	MB/Sec	
Packets transmitted:	Indicates the rate at which packets were transmitted from this pool during the last measurement period.	Packets/Sec	Compare the values of these measures across the pools to identify the pool that is handling maximum amount of traffic.
Packets received:	Indicates the rate at which packets were received in this pool during the last measurement period.	Packets/Sec	
Active connections:	Indicates the number of connections that are currently active in this pool.	Number	
Total connections:	Indicates the total number of connections established on this pool since the start of the traffic manager.	Number	
Connection during the last measure period:	Indicates the rate at which connections were established during the last measurement period.	Conns/Sec	
Connection usage:	Indicates the percentage of connections that were used by this pool.	Percent	
Maximum	Indicates the maximum number	Number	

Measurements	Decription	Measurement Unit	Interpretation
connections established:	of connections that were established on this pool since the start of the traffic manager.		

1.3.4 F5 Pool Members Test

This test auto-discovers the members of each load balancing pool and reports the data /packet traffic through each member, the number of active connections and total connections. In addition, this test reports how well the conenctions are used by each member. This way, administrators can figure out how well each pool member handles the load and proactively detect load balancing irregularities, if any.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each pool configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the

management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.

8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **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.
12. **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
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
16. **DATA OVER TCP** – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
17. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the **DETAILED DIAGNOSIS** capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

    The option to selectively enable/disable the **DETAILED DIAGNOSIS** capability will be available only if the following conditions are fulfilled:

- The eG manager license should allow the detailed diagnosis capability
- Both the normal and abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurements	Descriptions	Measurement Unit	Interpretation
Connection during the last measure period:	Indicates the rate at which connections were established during the last measurement period.	Conns/Sec	
Data transmitted:	Indicates the rate at which data is transmitted from this member during the last measurement period.	MB/Sec	Comparing the value of these measures across the pool members will help you identify the pool member that is handling maximum traffic.
Data received:	Indicates the rate at which data is received in this member during the last measurement period.	MB/Sec	
Packets transmitted:	Indicates the rate at which packets were transmitted from this member during the last measurement period.	Packets/Sec	Compare the value of these measures across the pool members to identify the pool member that is experiencing the maximum traffic.
Packets received:	Indicates the rate at which packets were received in this member during the last measurement period.	Packets/Sec	
Active connections:	Indicates the number of connections that are currently active in this member.	Number	
Connection usage:	Indicates the percentage of connections that were used by this member.	Percent	

Measurements	Descriptions	Measurement Unit	Interpretation
Maximum connections established:	Indicates the maximum number of connections that were established on this member since the restart of the traffic manager.	Number	

1.3.5 F5 Traffic Management Module Test

In large infrastructures where too many servers are connected to the traffic manager, monitoring the individual statistics of each server becomes tedious for the administrators. Therefore, administrators would need a unified system where they would be able to view the overall load balancing statistics of their infrastructure. This is where the **F5 Traffic Management Module** test helps. This test periodically alerts the administrators of the data/packet traffic to and from the client/server, connections that are currently active on the client/server, total connections from the client/server etc. This way, administrators will be able to view the overall performance and effieicieny of the traffic manager and be alerted proactively on load balancing issues, if any.

Target of the test : A Big-IP/F5 Local Traffic Manager

Agent deploying the test : An external agent

Outputs of the test : One set of results for each pool configured on a traffic manager

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the traffic manager
3. **SNMPPORT** – The port at which the traffic manager exposes its SNMP MIB; the default is 161.
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. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **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
11. **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.
12. **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
13. **ENCRYPTPASSWORD**– Specify the encryption password here.
14. **CONFIRM PASSWORD**– Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –**By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Traffic manager over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
17. **DETAILED DIAGNOSIS** – To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the

detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

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

- The eG manager license should allow the detailed diagnosis capability
- Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurements	Measurement	Measurement Unit	Interpretation
Data transmitted from client:	Indicates the rate at which data is transmitted from the client to the server through this TMM during the last measurement period.	MB/Sec	
Data received from client:	Indicates the rate at which data is received from the client by the server through this TMM during the last measurement period.	MB/Sec	
Packets transmitted from client:	Indicates the rate at which packets were transmitted from the client through this TMM during the last measurement period.	Packets/Sec	
Packets received from client:	Indicates the rate at which packets were received from the client in this TMM during the last measurement period.	Packets/Sec	
Active connections from client:	Indicates the number of connections from the client that are currently active in this TMM.	Number	

Measurements	Measurement	Measurement Unit	Interpretation
Total connections from client:	Indicates the total number of connections from the client that were established on this TMM since the restart of the traffic manager.	Number	
Connection during the last measure period from client:	Indicates the rate at which connections from the client were established during the last measurement period.	Conns/Sec	
Connection usage from client:	Indicates the percentage of connections from the client that were used by this TMM.	Percent	
Max connections established from client:	Indicates the maximum number of client connections that were established on this TMM since the restart of the traffic manager.	Number	
Data transmitted from server:	Indicates the rate at which data is transmitted from the server through this TMM during the last measurement period.	MB/Sec	
Data received from server:	Indicates the rate at which data is received from the server by this TMM during the last measurement period.	MB/Sec	
Packets transmitted from server:	Indicates the rate at which packets were transmitted from the server through this	Packets/Sec	

Measurements	Measurement	Measurement Unit	Interpretation
	TMM during the last measurement period.		
Packets received from server:	Indicates the rate at which packets were received from the server by this TMM during the last measurement period.	Packets/Sec	
Active connections from server:	Indicates the number of connections from the server that are currently active on this TMM.	Number	
Total connections from server:	Indicates the total number of connections from the server that were established since the start of the traffic manager.	Number	
Connection during the last measure period from server:	Indicates the rate at which connections from the server were established during the last measurement period.	Conns/Sec	
Connection usage from server:	Indicates the percentage of connection from the server that were used by this TMM.	Percent	
Max connections established from server:	Indicates the maximum number of connections that were eatablished from the server since the start of the traffic manager.	Number	
CPU usage:	Indicates the percentage of time the CPU of this TMM was busy during the	Percent	A value close to 100 is a cause of concern.

Measurements	Measurement	Measurement Unit	Interpretation
	last 1 minute.		
Total memory:	Indicates the total memory allocated to this TMM.	MB	
Used memory:	Indicates the amount of memory that is already utilized by this TMM.	MB	A low value is desired for this measure.
Free memory:	Indicates the amount of memory available for use by this TMM.	MB	A high value is desired for this measure. A sudden/gradual decrease in the value of this measure is an indication for the administrators to provide additional resources to the TMM.
Memory utilization:	Indicates the percentage of memory utilized by this TMM.	Percent	
Http request rate:	Indicates the rate at which HTTP requests passed through this TMM during the last measurement period.	Requests/sec	
Packets dropped:	Indicates the rate at which packets were dropped by this TMM during the last measurement period.	Packets/sec	A low value is desired for this measure.

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 **F5 Traffic manager**. 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.