Monitoring F5 BIG-IP Load Balancer

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

An F5 BIG-IP load balancer distributes the processing and communications activity evenly across groups of servers in a network, so that no single server is overwhelmed. The BIG-IP load balancer keeps a constant check on the incoming and outgoing traffic of the servers in the server pools. By default, it will route the user requests to the most available server that can best handle them (see Figure 1.1). Moreover, the load balancer maintains network connectivity along multiple ISP paths, and thus ensures high availability of the servers in a pool.

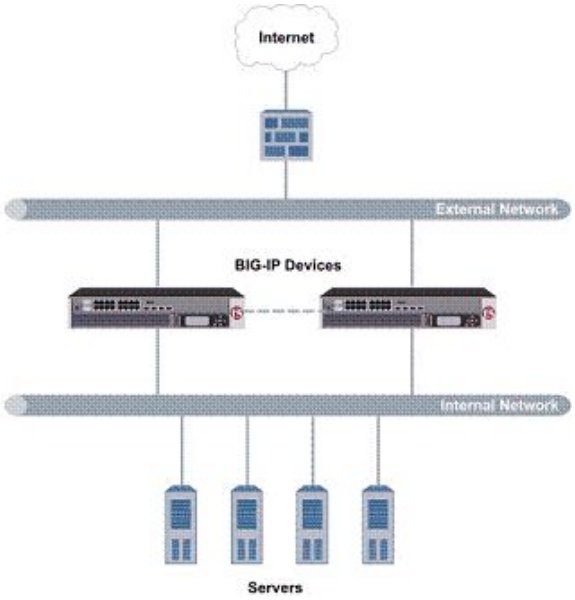

Figure 1.1: How the BIG-IP load balancer works?

Since it plays a critical role in an Internet facing IT infrastructure, even a slight deterioration in the performance of a load balancer can adversely impact the critical IT services of an enterprise, thereby resulting in considerable revenue loss. In order to prevent such adversities, it is imperative that BIG-IP load balancers are continuously monitored. This where the eG Enterprise helps administrators!

Chapter 2: How to Monitor eG Enterprise F5 BIG-IP Load Balancers?

eG Enterprise monitors the F5 BIG-IP Load Balancers using an eG external agent that is deployed on any remote host. This agent periodically polls the SNMP MIB of the F5 BIG-IP Load Balancer and fetching metrics related to the performance of the F5 BIG-IP Load Balancer. The section that follows describes how to manage the F5 BIG-IP Load Balancer.

2.1 Managing the F5 BIG-IP Load Balancers

The eG Enterprise cannot automatically discover a F5 BIG-IP Load Balancer. This implies that you need to manually add the component for monitoring. To manage a F5 BIG-IP Load Balancer component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENTS** page that appears next, select *F5 BIG-IP* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

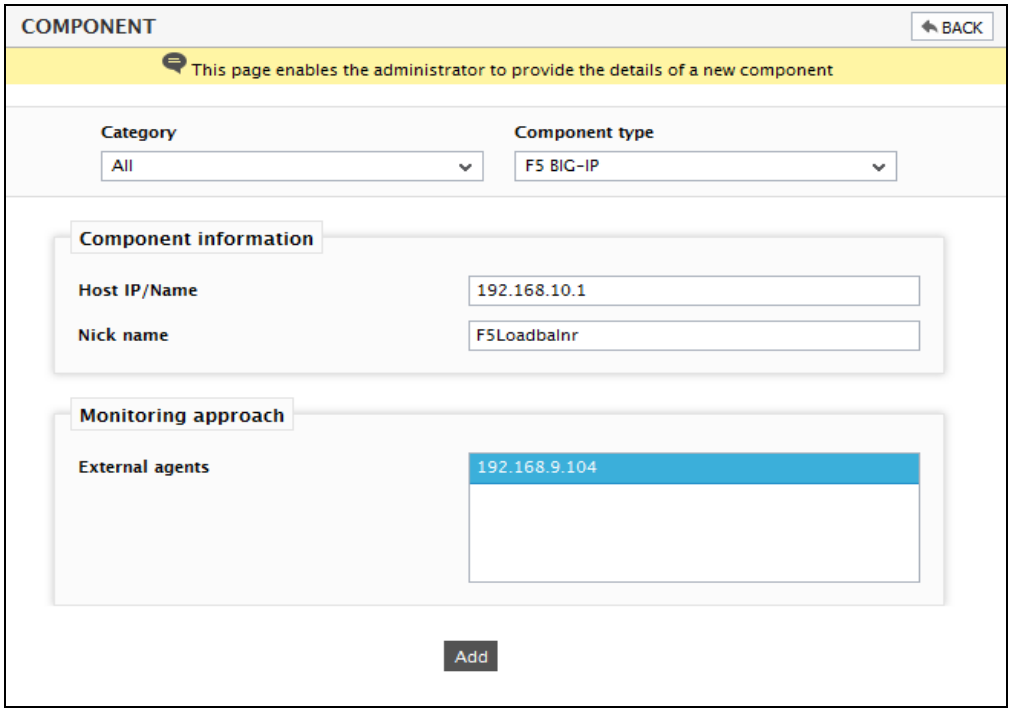

Figure 2.1: Adding a F5 BIG-IP Load Balancer

3. Specify **Host IP/Name** and **Nick name** for the F5 BIG-IP component (see Figure 2.1). Then click on the **Add** button to configure the F5 BIG-IP component.
4. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

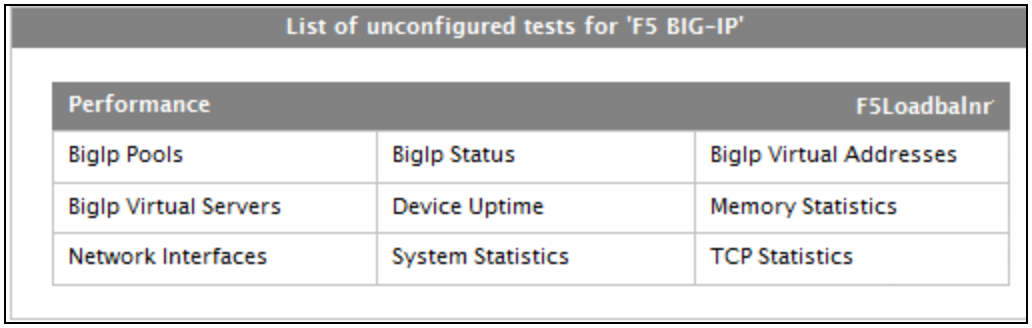

Figure 2.2: A list of unconfigured tests

5. Click on the **BigIp Pools** test to configure it. To know how to configure the test, refer to Section **3.5.1**.
6. Then, try to signout, now you will be prompted to configure the **Device Uptime**, **Network Interfaces** and **TCP Statistics** tests. Refer to *Monitoring Cisco Router* document to know how to configure the **Device Uptime** and **Network Interfaces** tests.
7. Once all the tests are configured, signout of the administrative interface.

Chapter 3: Monitoring F5 BIG-IP Load Balancers

The eG Enterprise suite provides a specialized *F5 BigIp* model (see Figure 3.1) for managing a BIG-IP load balancer.

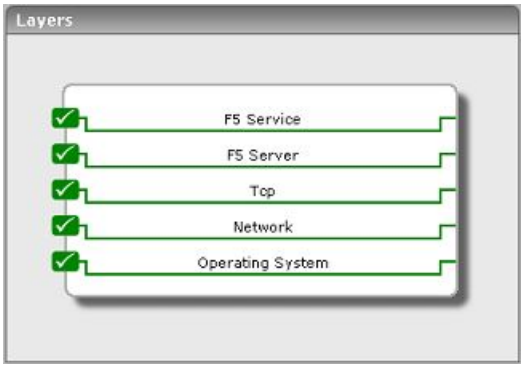

Figure 3.1: The layer model of a BIG-IP load balancer

Every layer of the layer model depicted by Figure 3.1 is mapped to one/more tests, which uses the host's SNMP MIB to extract critical statistics pertaining to the load balancing activity performed by BIG-IP. The performance metrics reported by these measures reveal the following:

System Monitoring	• Is the Big-IP hardware sufficiently sized to handle the incoming load, or is there a CPU or a memory bottleneck? • Is I/O activity on the system abnormal? • Are context switches kept at a minimum, or are there too many threads contending for CPU resources? • How much swap space is currently available in the system? Is it sufficient?
Workload Monitoring	• What is the current total workload on the Big-IP load balancer? Has there been any change in the workload over time? • How much traffic is the load balancer handling? How many connections
Load Distribution monitoring	• Has any of the servers across which the load is being balanced failed? • Is network load balanced across all the servers in the pool? • Is any server in the pool handling more connection requests than

	others?

Each of the layers is discussed in the sections below.

3.1 The Operating System Layer

The tests associated with this layer (see Figure 3.2) provide valuable insights into the memory and CPU usage of the BIG-IP load balancer. From these tests, an administrator can determine if there is a memory or CPU bottleneck on the load balancer.

Figure 3.2: The tests associated with the Operating System layer

3.1.1 Memory Statistics Test

This test monitors the available and used memory of a BIG-IP load balancer. The Net-SNMP MIB is polled by this test to extract the metrics below:

Target of the test : A BIG-IP Load Balancer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the BIG-IP load balancer being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

Parameters	Description
	in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total real memory	Indicates the total real memory space on the host.	MB	
Available memory	Indicates the available real/physical memory space on the host.	MB	Ideally, this value should be high.
Free virtual memory	Indicates available virtual memory on the host.	MB	
Total swap memory	Indicates the total swap size configured for the host.	MB	

Measurement	Description	Measurement Unit	Interpretation
Available swap	Indicates the available swap space on the host.	MB	An unusually low value for the available swap space can indicate a memory bottleneck. Check the memory utilization of individual processes to figure out the process (es) that has (have) maximum memory consumption and look to tune their memory usages and allocations accordingly.
Swap memory errors	Indicates whether adequate swap space is available or not.	Boolean	A value of 1 indicates that there is very little swap space left. A value of 0 indicates normalcy with respect to available swap space.
Shared memory usage	Indicates the total shared memory on the host.	MB	
Buffered memory	Indicates the total buffered memory on the host.	MB	
Cached memory	Indicates the total cached memory on the host.	MB	
Memory swap ins	Indicates the amount of memory swapped in from disk per second.	KB/Sec	
Memory swap outs	Indicates the amount of memory swapped out to disk per second.	KB/Sec	

3.1.2 System Statistics Test

This test measures the key system performance metrics of a BIG-IP load balancer.

Target of the test : A BIG-IP Load Balancer

Agent deploying the test : An external agent

Outputs of the test : One set of results for the BIG-IP load balancer being monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
I/O sent	Indicates the rate of I/O blocks sent to a block device during the last measurement period.	Blocks/Sec	
I/O received	Indicates the rate of I/O blocks sent from a block device during the last	Blocks/Sec	When viewed with the IO_sent measure, this reveals the level of I/O activity on the load balancer.

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
System interrupts	Indicates the number of interrupts per second processed by the system/	Interrupts/Sec	
Context switches	Indicates the rate of context switches that happened on the system during the last measurement period.	ContextSwitches/Sec	Context switches occur when a running thread voluntarily relinquishes the processor, is preempted by a higher priority ready thread, or switches between user-mode and privileged (kernel) mode to use an Executive or subsystem service. If the context switch rate is unusually high, it implies that there is excessive contention for CPU resources.
User CPU utilization	Indicates the current user CPU utilization of the system.	Percent	
System CPU utilization	Indicates the current system CPU utilization of the system.	Percent	An unusually high value indicates a problem and may be due to too many system-level tasks executing simultaneously.

3.2 The Network Layer

To know the health of the network connection to the load balancer, and the level of traffic emerging from and flowing to the load balancer, use the tests associated with the **Network** layer.

Figure 3.3: The tests associated with the Network layer

These tests have been elaborately discussed in the Monitoring Cisco Routers document.

3.3 The Tcp Layer

To observe the TCP connections and retransmissions to and from the load balancer, use the **Tcp Statistics** test associated with the Tcp layer. This test is described in the Monitoring Juniper SA Device document.

Figure 3.4: The test associated with the Tcp layer

3.4 The F5 Server Layer

Every physical server in a server pool is mapped by the BIG-IP load balancer to one or more virtual servers. A Virtual Server is a combination of virtual address and virtual port, associated with a content site that is managed by a BIG-IP system. When the load balancer receives requests from clients to a virtual server, it routes them to the appropriate physical server in the pool.

The F5Status test associated with this layer reports the status of incoming and outgoing traffic through a load balancer (see Figure 3.5).

Figure 3.5: The test associated with the F5 Server layer

3.4.1 F5 Status Test

This test provides key indicators of the workload being handled by the load balancer.

Target of the test : A BIG-IP Load Balancer

Agent deploying the test : An external agent

Outputs of the test : One set of results for each load balancer

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2

Parameters	Description
	Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameters	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Incoming traffic	Indicates the rate at which data is received by the load balancer during the last measurement period.	Mbps	An abnormally high rate of incoming traffic may require additional analysis.
Outgoing traffic	Indicates the rate at which responses are being sent from the load balancer during the last measurement period.	Mbps	An abnormally high rate of outgoing traffic may require additional analysis.
Incoming packet rate	Indicates the number of packets received per second by the load balancer during the last measurement period.	Packets/Sec	
Outgoing packet rate	Indicates the number of packets sent out per second by the load balancer during the last measurement period.	Packets/Sec	
Current connections	Indicates the number of	Number	A very useful metric to trend regarding

Measurement	Description	Measurement Unit	Interpretation
	connections currently established by the load balancer with the servers in the pool.		a load balancer is the total number of concurrent connections. This counts the number of sessions the BIG-IP load balancer is handling. This metric is the number of open TCP sessions that users have currently established. UDP is not included in this of course, as UDP is a connectionless protocol.
Connection rate	Indicates the rate at which connections have been handled by the load balancer during the last measurement period	Conns/Sec	The connection rate is the most important metric to keep track of for any load balancer as it is typically the most resource-intensive, especially for web sites with small files and a high rate of connections.
Connection timeouts	Indicates the number of connections that timed out during the last measurement value.	Number	A very high value of this measure indicates frequent connection timeouts. In such a case, you might want to consider resetting the timeout period for connections.
Memory pool total	Represents the total memory pool available on the system.	MB	
Memory pool used	Indicates the total memory pool in use by the system.	MB	If this metric is close to the Memory pool total, this implies that there is a memory bottleneck on the BIG-IP load balancer.
Memory pool utilization	Indicates the percentage of memory in the memory pool that has been utilized.	Percent	Ideally, this value should be low. A value close to 100 denotes a memory bottleneck on the load balancer.
Memory errors	Indicates the total number of memory access errors that occurred during the last measurement period.	Number	Ideally, this value should be 0.

3.5 The F5 Service Layer

Using the tests associated with this layer (see Figure 3.6), eG Enterprise monitors the traffic routed through each of the virtual servers and virtual IP addresses configured on the load balancer.

Figure 3.6: The tests associated with the F5 Service layer

3.5.1 BigIp Pools Test

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load-balancing method. Monitoring of the pools configured for a Big IP load balancer can indicate the relative load on the load balancer from the different pools. The F5 Pools test tracks the status and the traffic on each of the pools configured on the BIG-IP load balancer.

Target of the test : A BIG-IP Load Balancer

Agent deploying the test : An external agent

Outputs of the test : One set of results for every pool configured for the BIG-IP load balancer being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameters	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Incoming traffic	Indicates the rate at which requests are routed through this pool during the last measurement period.	Mbps	An abnormally high rate of incoming traffic may require additional analysis. By comparing the values of this metric with the outgoing rate, you can easily identify which pools are experiencing high traffic.
Outgoing traffic	Indicates the rate at which responses from the servers are transmitted by the pool during the last measurement period.	Mbps	An abnormally high rate of outgoing traffic may require additional analysis.
Incoming packet rate	Indicates the number of packets per second routed to the physical server(s) in the pool during the last	Packets/Sec	Both these measure serve as effective indicators of the data load on the load balancer.

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Outgoing packet rate	Indicates the number of packets per second sent out through the pool during the last measurement period.	Packets/Sec	
Current connections	Indicates the number of connections currently established for this pool.	Number	Comparison of this metric across pools indicates which of the pools is handling a higher load.
Connection rate	Indicates the rate at which connections have been established via a pool during the last measurement period.	Conns/Sec	

3.5.2 BigIp Virtual Addresses Test

This test tracks the status and the traffic on each of the virtual IP addresses configured on the BIG-IP load balancer.

Target of the test : A BIG-IP Load Balancer

Agent deploying the test : An external agent

Outputs of the test : One set of results for every virtual IP configured on the BIG-IP load balancer being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameters	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates whether this virtual IP address is currently active or inactive.	Number	While the value 0 indicates that the virtual IP is inactive, 1 indicates that it is active.
Incoming traffic	Indicates the rate at which requests are routed through this virtual IP during the last measurement period.	Mbps	An abnormally high rate of incoming traffic may require additional analysis. A comparison of the values of this metric with the outgoing rate can be used to identify which of the virtual addresses is seeing high traffic rates.
Outgoing traffic	Indicates the rate at which responses from the servers are transmitted by the virtual IP during the last measurement period.	Mbps	An abnormally high rate of outgoing traffic may require additional analysis.
Incoming packet rate	Indicates the number of	Packets/Sec	

Measurement	Description	Measurement Unit	Interpretation
	packets per second routed to the physical server(s) in the pool through this virtual IP during the last measurement period.		
Outgoing packet rate	Indicates the number of packets per second sent out through this virtual IP during the last measurement period.	Packets/Sec	
Current connections	Indicates the number of connections currently established via this virtual IP.	Number	Comparison of this metric across virtual IPs indicates which of the virtual IPs is handling a higher load.
Connection rate	Indicates the rate at which connections have been established via this virtual IP during the last measurement period.	Conns/Sec	

3.5.3 BigIp Virtual Servers Test

A virtual server is a combination of virtual IP address and port, through which incoming traffic to a server pool is load balanced by the BIG-IP load balancer. This test monitors the status and traffic on every virtual server configured on the BIG-IP.

Target of the test : A BIG-IP Load Balancer

Agent deploying the test : An external agent

Outputs of the test : One set of results for every virtual server configured on the BIG-IP load balancer being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates whether this virtual server is active or inactive.	Number	While the value 0 indicates that the virtual server is inactive, 1 indicates that it is active.
Incoming traffic	Indicates the rate at which traffic was routed through this virtual server during the last measurement period.	Mbps	An abnormally high rate of incoming traffic may require additional analysis.

Measurement	Description	Measurement Unit	Interpretation
Outgoing traffic	Indicates the rate at which traffic was transmitted from a virtual server in the last measurement period.	Mbps	An abnormally high rate of outgoing traffic may require additional analysis.
Incoming packet rate	Indicates the number of packets per second routed to the physical server(s) in the pool through this virtual server.	Packets/Sec	
Outgoing packet rate	Indicates the number of packets per second sent out through this virtual server.	Packets/Sec	
Current connections	Indicates the number of connections currently established via this virtual server.	Number	
Connection rate	Indicates the rate at which connections have been established via this virtual server during the last measurement period.	Conns/Sec	Comparison of this metric across virtual servers indicates which of the virtual servers is handling a higher load.

About eG Innovations

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

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

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

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