Monitoring BIG-IP Access Policy Manager (APM)

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

F5 BIG-IP Access Policy Manager (APM) is a secure, flexible, high-performance access management proxy solution that delivers unified global access control for your users, devices, applications, and application programming interfaces (APIs). Through its single management interface, BIG-IP APM converges and consolidates remote, mobile, network, virtual desktops, and web access. With BIG-IP APM, you can create and enforce simple, dynamic, intelligent access policies. BIG-IP APM combines centralized network access control, federated identity, SSO, and adaptive authentication into a single flexible, scalable application delivery solution, simplifying and consolidating your access infrastructure. BIG-IP APM is available on hardware, in the cloud, or as a virtual appliance and provides access control wherever your applications live. APM offers:

- **Identity Federation and SSO** - Creates a single point of policy-based access for cloud and on premise/private applications with MFA support.
- **Client and Web-based SSL VPN Access** - Policy-based access to network VPN service through web-plugins or clients on mobile and desktop operating systems.
- **Web Portal Access to Applications** - Open web applications to users instead of opening up your network. Great for contractors and remote workers who don't need full VPN tunnels.
- **Desktop Application and VDI Support** - Policy-based access to virtualized applications through a single, consolidated gateway along with native VDI support and a customizable, web portal.
- **Access Policy Deployment and Management Solutions** - Using the visual policy editor, administrators create highly customizable security polices allowing granular control over application and network access.
- **Secure Web Gateway Proxy Services** - Provides web-based malware protection and URL filtering through Secure Web Gateway Services.

With the above-mentioned features, the BIG-IP APM offers you with seamless user access to web applications in a highly available and heterogeneous environment, which in turn improves business continuity and boosts user productivity for your organization. Since it plays a critical role in application delivery infrastructures, even a slight slippage in the performance of the APM can adversely impact the critical application delivery, thereby resulting in poor user experience and considerable revenue loss. In order to prevent such adversities, it is imperative that BIG-IP APM are continuously monitored. This where eG Enterprise helps administrators!

Chapter 2: How to Monitor BIG-IP Access Policy Manager (APM) Using eG Enterprise ?

eG Enterprise monitors the BIG-IP Access Policy Manager (APM) using an external agent on any Windows host in the environment. This agent is capable of monitoring the performance of the target APM in the following ways:

- By polling the SNMP MIB of the target APM;
- By connecting to the APM via SSH and running CLI commands;

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

2.1 Pre-requisites for Monitoring the BIG-IP APM

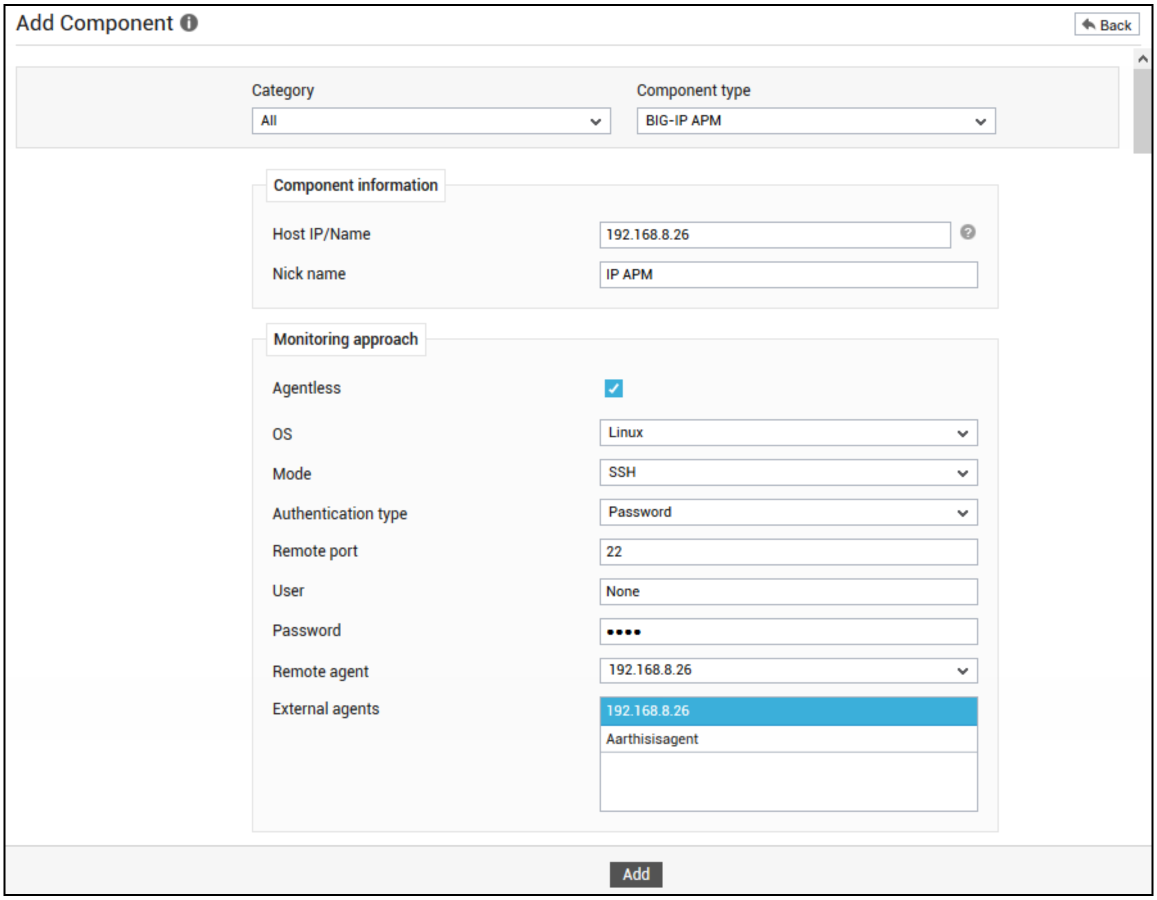
To enable the eG external agent to collect performance metrics from the target APM, the following pre-requisites should be fulfilled:

1. The target APM should be SNMP-enabled.
2. The eG agent should be able to access the target APM over the network.
3. To run the **Session by Access Profile**, **Citrix Sessions**, **F5 Users** and **Other F5 Sessions** tests, the eG agent should be able to communicate with the target APM via SSH. For this purpose, specify the SSH port (default port: 22) and credentials of a SSH user who has *admin* privileges on the target APM while adding a BIG-IP APM component for monitoring. This user should be able to execute the CLI command i.e. *sessiondumb*, on the target APM to run the tests and poll the performance metrics. To know how to configure the above-said details, refer to Managing BIG-IP Access Policy Manager (APM) topic.
4. Also, ensure that the SSH port remains open on the firewall (if any) between the agent and the target APM.

2.2 Managing BIG-IP APM

eG Enterprise is capable of automatically discovering the BIG-IP APM, and also allows you to manually add the component for monitoring. To manage an BIG-IP APM component, do the following:

1. Log into the eG administrative interface.
2. If the BIG-IP APM is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **Components** page. Remember that components manually added are managed automatically.
4. In the **Components** page that appears next, select *BIG-IP APM* as the **Component type**. Then, click the **Add New Component** button. This will invoke 2.2.



Category	All
Component type	BIG-IP APM

Component information

Host IP/Name	192.168.8.26
Nick name	IP APM

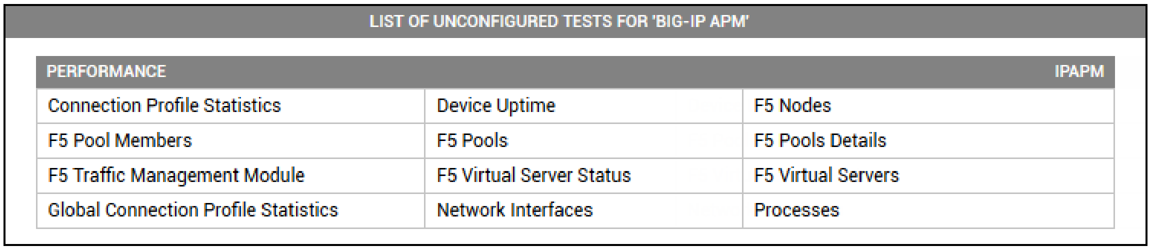
Monitoring approach

Agentless	☑
OS	Linux
Mode	SSH
Authentication type	Password
Remote port	22
User	None
Password	••••
Remote agent	192.168.8.26
External agents	192.168.8.26 Aarthisisagent

Figure 2.1: Adding the BIG-IP APM component

5. Specify the **Host IP/Name** and the **Nick name** for the *BIG-IP APM* component. By default, the *BIG-IP APM* component is monitored in an agentless manner. Therefore, the **Agentless** check box is selected, by default.

6. Next, select **Linux** as the **OS** and **SSH** as the **Mode**. The SSH Remote port will be set as 22 by default. Change the remote port if the target APM is listening on a different SSH port.
7. Specify the credentials of a root user in the User and Password text boxes.
8. Select the **Remote agent** that will be monitoring the target Big-IP APM.
9. Choose an external agent for the target APM by picking an option from the **External agents** list box.
10. Then, click the **Add** button to register the changes (see Figure 2.1).
11. The BIG-IP APM component so added will be managed automatically by eG Enterprise. Now, try to sign out of the user interface. Doing so, will invoke Figure 2.2 prompting you to configure a list of unconfigured tests for the new BIG-IP APM component.



LIST OF UNCONFIGURED TESTS FOR 'BIG-IP APM'

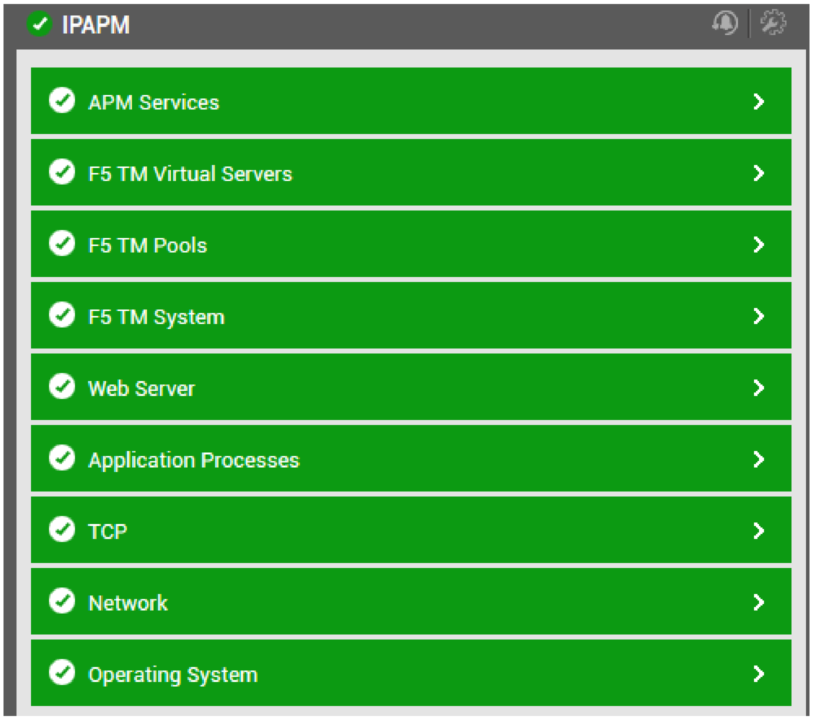
PERFORMANCE		IPAPM
Connection Profile Statistics	Device Uptime	F5 Nodes
F5 Pool Members	F5 Pools	F5 Pools Details
F5 Traffic Management Module	F5 Virtual Server Status	F5 Virtual Servers
Global Connection Profile Statistics	Network Interfaces	Processes

Figure 2.2: The list of unconfigured tests that need to be configured for the BIG-IP APM

12. Click on any test in the list of unconfigured tests. To know how to configure the tests, refer to Monitoring the BIG-IP APM.
13. Finally, signout of the eG admin interface.

Chapter 3: Monitoring BIG-IP APM

Figure 3.1 shows the dedicated BIG-IP APM monitoring model offered by eG Enterprise .



IPAPM

- ✓ APM Services
- ✓ F5 TM Virtual Servers
- ✓ F5 TM Pools
- ✓ F5 TM System
- ✓ Web Server
- ✓ Application Processes
- ✓ TCP
- ✓ Network
- ✓ Operating System

Figure 3.1: The layer model of the BIG-IP APM

Every layer of Figure 3.1 is mapped to a variety of tests which connect to the target APM via SNMP and SSH to collect critical metrics pertaining to its performance. With the help of these metrics, administrators can find quick and accurate answers to the following performance queries:

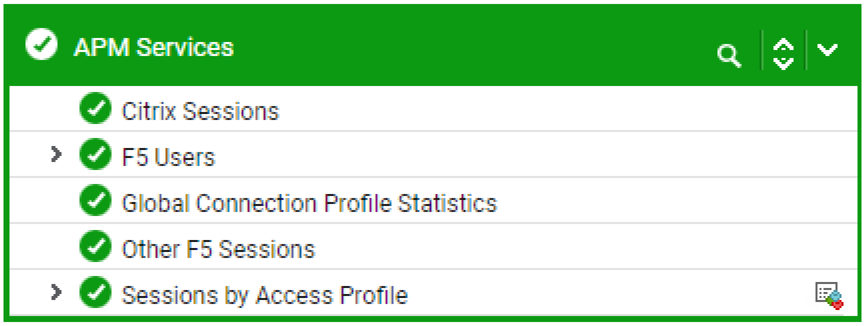
- Which access profile is widely used to connect to the target APM?
- Which access profile is prone to errors?
- Which connectivity profile imposed maximum workload on the target APM?
- Which connectivity profile was frequently used to establish connections to transmit/receive raw data and compressed data?
- How many Citrix sessions were established by each user?
- Which user established the maximum number of Citrix sessions?
- How much of data was received/transmitted by each user?

- How many Citrix sessions were logged out during the last measurement period?
- How many F5 sessions were established by each user on the target APM?
- How many sessions were established for each access profile?
- How many sessions were terminated for each access profile due to reasons such as user logouts, occurrence errors and logouts by the administrator?
- How many sessions were allowed/denied by the access control policies defined on each access profile?
- Through which access profile were the maximum number of sessions allowed/denied by the access control policies?

Since the tests pertaining to the **Operating System, Network, TCP** and **Application processes** layers have already been discussed in the *Monitoring Unix and Windows Servers* document, the **Web Server** layer has already been discussed in the *Monitoring IIS Web Servers* document, the **F5 TM System**, **F5 TM Pools** and the **F5 Virtual Servers** layers have already been discussed in the *Monitoring F5 Traffic Manager* document, the sections to come will discuss the tests associated with the **APM Services** layer alone.

3.1 APM Services Layer

Using the tests associated with this layer (see Figure 3.2), eG Enterprise monitors the sessions established using the Access profiles and Connectivity profiles. In addition, the tests also reveal the session load caused by Citrix users and other F5 users.



APM Services
Citrix Sessions
F5 Users
Global Connection Profile Statistics
Other F5 Sessions
Sessions by Access Profile

Figure 3.2: The tests associated with the APM Services layer

3.1.1 Citrix Sessions Test

When BIG-IP APM is integrated with Citrix, it performs authentication to control access to Citrix-published applications and remote desktops. BIG-IP APM Citrix integration simplifies the Citrix environment by replacing some of core services, including the Citrix Web Interface server, Citrix

Access Gateway, Netscaler and Citrix Secure Ticketing Authority service. This way, establishing Citrix sessions through the BIG-IP APM is made easier for users who have privileges to login to the Citrix environment and access the published applications. In such environments, it is necessary for administrators to ensure that the user experience with the Citrix environment is good at all times. Sometimes, the user experience may get affected by the overload condition (if any) on the target APM due to the Citrix sessions. To avoid such eventualities, administrators may want to proactively detect the count of Citrix sessions established through the target BIG-IP APM at regular intervals. The **Citrix Sessions** test helps administrators in this regard!

At configured intervals, this test reports the total number of sessions established by the Citrix users through the BIG- IP APM, and warns administrators of a probable overload condition (if any). Additionally, the test also reports the count of sessions that were newly established and logged out.

Target of the test : A Big-IP Access Policy Manager (APM)

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Big-IP APM that is being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
Timeout	Specify the duration (in seconds) beyond which this test should time out in this text box. The default is 10 seconds.
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

Measurement	Description	Measurement Unit	Interpretation
Total sessions	Indicates the total number of Citrix sessions established through the target BIG-IP APM.	Number	This measure is a good indicator of session load caused by authorized Citrix users. Using the detailed diagnosis of this measure, you can identify following: • User name used by the client to connect Citrix remote server. • IP address of the client. • Name of the Access profile through which user is connected • Virtual server configured on the access profile. • Port number of the virtual server. • IP address of the Citrix remote server • Time duration in minutes since the session has been started.
New sessions	Indicates the number of new Citrix sessions established during the last measurement period.	Number	A consistent zero value could indicate an issue such as authentication failure, poor connection, etcc.
New sessions percentage	Indicates the percentage of new Citrix sessions established during the last measurement period.	Percent	
Logged out sessions	Indicates the number of Citrix sessions that logged out.	Number	If all the current sessions suddenly log out, it may indicate a problem condition that requires investigation.

3.1.2 Connection Profile Statistics Test

A connectivity profile defines connectivity and client settings for a Network Access session to the BIG-IP APM. Each connectivity profile contains:

- Compression settings for network access connections and application tunnels
- Citrix client settings
- Virtual servers and DNS-location awareness settings for BIG-IP® Edge Client® for Windows, Mac, and Linux
- Password caching settings for BIG-IP Edge Client for Windows, Mac, and mobile clients
- Settings for mobile clients

Using the connectivity profiles, administrators can configure client (SSL/VPN) connections for a network access tunnel, application access tunnel, and clients. The connectivity profiles help administrators to establish multiple client connections without having to define settings for each connection. This way, administrators can maintain unique settings across all connections and control data traffic through each connection.

This test monitors the connectivity profiles on the target BIG-IP APM and reveals the total number of connections established using each connectivity profile. In addition, this test also reports the amount of compressed data/raw data transferred via the connections established using each connectivity profile. This way, administrators can identify the connectivity profile that imposes maximum load on the target BIG-IP APM and also find out what type of data was transferred through the connections.

Target of the test : A Big-IP Access Policy Manager (APM)

Agent deploying the test : An external agent

Outputs of the test : One set of results for each connection profile defined the target APM.

Configurable parameters for the test

Parameter	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

Parameter	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

Parameter	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**.
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	Description	Measurement Unit	Interpretation
Total connections	Indicates the total number of connections established using this connectivity profile.	Number	This is a good indicator of connection workload created by each connectivity profile.
Current connections	Indicates the number of connections that are currently using this connectivity profile.	Number	
Raw data received	Indicates the amount of raw data received over the connections that are established using this connectivity profile.	MB	Comparing these measures across connectivity profiles will help administrators in identifying the connectivity profile that was frequently used to establish the connections to transmit/receive raw data.
Raw data transmitted	Indicates the amount of raw data transmitted over the connections that are established using this connectivity profile.	MB	
Compressed data received	Indicates the amount of compressed data received over the connections that are established using this connectivity profile.	MB	Comparing these measures across connectivity profiles will help administrators in identifying the connectivity profile that was frequently used to establish the connections to transmit/receive compressed data.
Compressed data transmitted	Indicates the amount of compressed data transmitted over the connections that are established using this connectivity profile.	MB	

3.1.3 F5 Users Test

In a large and shared application delivery environment, BIG-IP APM enables multiple users connect to the environment and access a wide variety of applications in a seamless ans secure way. In such environments, excessive load imposed by a single user could impact the performance for other users. Therefore, continuous monitoring of the activities of each and every user accessing the applications through the target APM is critical. Towards this end, the **F5 Users** test auto-discovers the users who access the applications through the target APM and reports the total number of F5 sessions established by each user. In the process, this test reveals the count of Citrix sessions established by each user. These results can be used to proactively detect the total work load imposed by each user and also isolate the workload on the target APM due to the Citrix sessions. In addition, for each user, this test also reports the amount of data and number of packets received/transmitted. This way, administrators can identify the user who created maximum traffic on the target APM.

Target of the test : A Big-IP Access Policy Manager (APM)

Agent deploying the test : An external agent

Outputs of the test : One set of results for each user connecting to the Big-IP APM that is being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
Timeout	Specify the duration (in seconds) beyond which this test should time out in this text box. The default is 10 seconds.
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

Measurement	Description	Measurement Unit	Interpretation
Total F5 sessions	Indicates the total number of F5 sessions established by this user.	Number	This measure is a good indicator of F5 session load created by each user. Using the detailed diagnosis of this measure, you can identify following: • IP address of the client. • Name of the access profile through which the user is connected to the target APM • Virtual server configured on the access profile • Port number of the virtual server • Type of the sessions
Total Citrix sessions	Indicates the total number of Citrix sessions established by this user.	Number	This measure reveals the workload caused by the Citrix sessions
Data received	Indicates the amount of data received by this user during the last measurement period.	MB	Compare the value of these measures across users to figure out the user who is transmitting/receiving the maximum amount of data. The user who is most active can thus be determined.
Data transmitted	Indicates the amount of data transmitted by this user during the last measurement period.	MB	
Packets received	Indicates the number of packets received by this user during the last measurement period.	Packets	Compare the value of these measures across users to figure out the user who is transmitting/receiving the maximum packets.
Packets transmitted	Indicates the number of packets transmitted by this user during the last measurement period.	Packets	

3.1.4 Global Connection Profile Statistics Test

To cater to the needs of different users, administrators create multiple connectivity profiles to help them establish connections to the BIG-IP APM. Sometimes, to efficiently manage the load on the target APM, administrators may want to know the load imposed via the connections made using the connectivity profiles. For this purpose, administrators can use the **Global Connection Profile Statistics** test. This test monitors the connectivity profiles available on the target BIG-IP APM and reports the aggregated statistics revealing the data traffic handled via the connections established using the connectivity profiles. This way, administrators can find out the load received on the target BIG-IP APM via the connections made using the connectivity profiles.

The **Global Connection Profile Statistics** test gives you these statistics for each connective profile on the target BIG-IP APM.

Target of the test : A Big-IP Access Policy Manager (APM)

Agent deploying the test : An external agent

Outputs of the test : One set of results for the BIG-IP APM being monitored.

Configurable parameters for the test

Parameter	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

Parameter	Description
	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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.

Parameter	Description
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**.
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	Description	Measurement Unit	Interpretation
Total connections	Indicates the total number of connections established on the target APM using the connectivity profiles.	Number	This measure is a good indicator of connection load on the APM.
Current connections	Indicates the number of connections that are currently using the connectivity profiles.	Number	
Raw data received	Indicates the amount of raw data received over the connections that are established using the	MB	

Measurements	Description	Measurement Unit	Interpretation
	connectivity profiles.		
Raw data transmitted	Indicates the amount of raw data transmitted over the connections that are established using connectivity profiles.	MB	
Compressed data received	Indicates the amount of compressed data received over the connections that are established using the connectivity profiles.	MB	
Compressed data transmitted	Indicates the amount of compressed data transmitted over the connections that are established using the connectivity profiles.	MB	

3.1.5 Other F5 Sessions Test

At configured intervals, this test monitors the sessions established by the F5 users using the Access Profiles on the BIG-IP APM and reports the total number of F5 sessions established on the target APM. This way, the test warns administrators of a probable overload condition (if any) caused only by the F5 users. Additionally, the test also reports the count of sessions that were newly established and logged out during the last measurement period. This will enable administrators to analyze the current and potential overload conditions, and take pre-emptive action against the same.

Target of the test : A Big-IP Access Policy Manager (APM)

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Big-IP APM that is being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.

Parameter	Description
Host	The IP address of the host that is being monitored.
Timeout	Specify the duration (in seconds) beyond which this test should time out in this text box. The default is 10 seconds.
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

Measurement	Description	Measurement Unit	Interpretation
Total sessions	Indicates the total number of F5 sessions established through the target BIG-IP APM.	Number	This measure is a good indicator of session load caused by authorized Citrix users. Using the detailed diagnosis of this measure, you can identify following: • User name used by the client to connect Citrix remote server. • IP address of the client. • Name of the Access profile through which user is connected • Virtual server configured on the access profile. • Port number of the virtual

Measurement	Description	Measurement Unit	Interpretation
			server. • IP address of the Citrix remote server • Time duration in minutes since the session has been started.
New sessions	Indicates the number of new F5 sessions established during the last measurement period.	Number	A consistent zero value could indicate an issue such as authentication failure, poor connection, etc.
New sessions percentage	Indicates the percentage of new F5 sessions established during the last measurement period.	Percent	
Logged out sessions	Indicates the number of F5 sessions that logged out during the last measurement period.	Number	If all the sessions suddenly log out, it may indicate a problem condition that requires investigation.

3.1.6 Sessions By Access Profiles Test

BIG-IP APM lets you design access policies for authentication and authorization, and, as an option, endpoint security checks, enforcing user compliance with corporate policies and industry regulations. You can define one access profile for all connections coming from any device, or you can create multiple access profiles for different access methods from various devices. The access profile contains:

- Access policy timeout and concurrent user settings
- Accepted language and default language settings
- Single Sign-On information and domain cookie information for the session
- Exchange profile for Microsoft Exchange service settings
- List of access controls

Owing to the benefits that the access profiles offer, administrators widely use them to easily establish the sessions on the BIG-IP APM. If the sessions established using the access profiles suddenly logged out due to errors, it will affect the user experience and productivity. To ensure better user experience with the sessions established using the access profiles, it is important for administrators to track the sessions at regular intervals. This can be easily achieved using the **Session By Access Profile** test!

This test auto-discovers the session profiles on the target APM and reveals the statistics related to the sessions established using each access profile. These statistics help administrators to identify the access profile that is prone to errors and rapidly take necessary actions to eliminate the issues.

Target of the test : A Big-IP Access Policy Manager (APM)

Agent deploying the test : An external agent

Outputs of the test : One set of results for each access profile defined the target APM.

Configurable parameters for the test

Test Period	How often should the test be executed.
Host	The IP address of the host that is being monitored.
Timeout	Specify the duration (in seconds) beyond which this test should time out in this text box. The default is 10 seconds.
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	Description	Measurement Unit	Interpretation
Current established sessions	Indicates the number of sessions that are currently	Number	

Measurements	Description	Measurement Unit	Interpretation
	established using this access profile.		
Current active sessions	Indicates the number of sessions, established using this access profile, that are active.	Number	
Current pending sessions	Indicates the number of sessions that are currently pending.	Number	
Sessions terminated by user logouts	Indicates the number of sessions terminated due to user logouts.	Number	
Sessions terminated by admin	Indicates the number of sessions terminated by the administrator.	Number	
Sessions terminated by error	Indicates the number of sessions terminated due to the occurrence of errors.	Number	
Sessions allowed by ACL	Indicates the maximum number of sessions allowed by the access control policies defined in this access profile.	Number	
Sessions denied by ACL	Indicates the maximum number of sessions denied by the access control policies defined in this access profile.	Number	

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.