F5 STUDY GUIDE

201 – TMOS Administration

Eric Mitchell
Channel SE, East US and Federal
F5 Networks

Contents

Overview

Welcome to the TMOS Administration compiled Study Guide. The purpose of this guide is to help you prepare for the F5 201 - TMOS Administration exam. The contents of this document are based on the 201 - TMOS Administration Blueprint Guide. The majority of the information is compiled from F5 sources that are located on Internet. This study guide provides students with some of the basic foundational knowledge required to pass the exam.

The resources for study also include the TMOS Administration Study Guide. The Study Guide is a list of additional reading material that will help any student build a broad base of general knowledge that can assist in not only their exam success but in becoming a well rounded systems engineer. The Study Guide will be available to the candidate once they are qualified for the TMOS Administration exam.

Hands on experience with the BIG-IP platform will reinforce many of the topics contained in the TMOS Administration exam.

This study guide is a collection of information and therefore not a completely original work. The information was found mostly in F5 resources. All of the information locations are referenced at each topic instead of in an Appendix of this document. This was done to help the reader access the reference the linked information easier without having to search through a formal appendix.

This guide was prepared by an F5 employee but is not an official F5 document and is not supported by F5 Networks.

Reading = Knowledge = Power

SECTION 1 – TROUBLESHOOT BASIC VIRTUAL SERVER CONNECTIVITY ISSUES

Objective - 1.01 - Given a connectivity troubleshooting situation, consider the packet and virtual server processing order

Virtual Server Intro:

Before we get into the study points of this section, there is some basic information you should know about virtual servers and the BIG-IP platform.

TMOS Concepts 11-1-0
Virtual Server Intro

A BIG-IP platform is a default deny device. This means that the device will not accept traffic and process it unless you have configured it to do so.

A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service (port number). 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. For example, a virtual server can enable compression on HTTP request data as it passes through the BIG-IP system, or decrypt and re-encrypt SSL connections and verify SSL certificates. For each type of traffic, such as TCP, UDP, HTTP, SSL, SIP, and FTP, a virtual server can apply an entire group of settings, to affect the way that Local Traffic Manager manages that traffic type.

A virtual server can also enable session persistence for a specific traffic type. Through a virtual server, you can set up session persistence for HTTP, SSL, SIP, and MSRDP sessions, to name a few.

Finally, a virtual server can apply an iRule, which is a user-written script designed to inspect and direct individual connections in specific ways. For example, you can create an iRule that searches the content of a TCP connection for a specific string and, if found, directs the virtual server to send the connection to a specific pool or pool member.

To summarize, a virtual server can do 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®

You can use virtual servers in any of several distinct ways:

Directing traffic to a load balancing pool

A Standard virtual server (also known as a load balancing virtual server) directs client traffic to a load balancing pool and is the most basic type of virtual server. When you first create the virtual server, you assign an existing default pool to it. From then on, the virtual server automatically directs traffic to that default pool.

Sharing an IP address with a VLAN node

You can set up a Forwarding (Layer 2) virtual server to share the same IP address as a node in an associated VLAN. To do this, you must perform some additional configuration tasks. These tasks consist of: creating a VLAN group that includes the VLAN in which the node resides, assigning a self-IP address to the VLAN group, and disabling the virtual server on the relevant VLAN.

Forwarding traffic to a specific destination IP address

A Forwarding (IP) virtual server is just like other virtual servers, except that a forwarding virtual server has no pool members to load balance. The virtual server simply forwards the packet directly to the destination IP address specified in the client request. When you use a forwarding virtual server to direct a request to its originally specified destination IP address, Local Traffic Manager adds, tracks, and reaps these connections just as with other virtual servers. You can also view statistics for a forwarding virtual server.

Increasing the speed of processing HTTP traffic

A Performance (HTTP) virtual server is a virtual server with which you associate a Fast HTTP profile. Together, the virtual server and profile increase the speed at which the virtual server processes HTTP requests.

Increasing the speed of processing Layer 4 traffic

A Performance (Layer 4) virtual server is a virtual server with which you associate a Fast L4 profile. Together, the virtual server and profile increase the speed at which the virtual server processes Layer 4 requests.

Relaying DHCP traffic

You can create a type of virtual server that relays Dynamic Host Control Protocol (DHCP) messages between clients and servers residing on different IP networks. Known as a DHCP relay agent, a BIG-IP system with a DHCP Relay type of virtual server listens for DHCP client messages being broadcast on the subnet and then relays those messages to the DHCP server. The DHCP server then uses the BIG-IP system to send the responses back to the DHCP client. Configuring a DHCP Relay virtual server on the BIG-IP system relieves you of the tasks of installing and running a separate DHCP server on each subnet.

When you create a virtual server, you specify the pool or pools that you want to serve as the destination for any traffic coming from that virtual server. You also configure its general properties, some configuration options, and other resources you want to assign to it, such as iRules or session persistence types.

1.01 – Explain how a packet is processed once it arrives on the device

SOL6459 - Order of precedence for virtual server matching

In version 4.x, which was just prior to version 9.x (when TMOS was created), the BIG-IP system used a virtual server precedence to define the order in which it routes a packet to a specific virtual server in the event that the packet matches multiple virtual server definitions.

The order of virtual server precedence was (from the highest precedence to the lowest precedence) as follows:

- ip:port
- ip:any
- network:port
- any:port
- network:any
- vlan:port
- vlan:any
- any:any

Many things have changed since then.

In Version 9.x through 11.2.1, (which covers this version of the exam) the BIG-IP system determines the order of precedence applied to new inbound connections using an algorithm that places a higher precedence on the address netmask and a lesser emphasis on the port. BIG-IP LTM sets virtual server precedence according to the following criteria:

- The first precedent of the algorithm chooses the virtual server that has the longest subnet match for the incoming connection.
- If the number of bits in the subnet mask match, the algorithm chooses the virtual server that has a port match.
- If no port match is found, the algorithm uses the wildcard server (if a wildcard virtual server is defined).
- A wildcard address has a netmask length of zero; thus, it has a lower precedence than any matching virtual server with a defined address.

This algorithm results in the following order of precedence:

- <address>:<port>
- <address>:*
- <network>:<port>
- <network>:*
- *:<port>
- *:*

Example of VIP precedence behavior

For example, for a BIG-IP system with the following VIPs configured on the inbound VLAN:

`10.0.0.0/8:80`

`10.10.0.0/16:80`

`10.10.10.10/32:80`

`20.0.0.0/8:*`

`20.0.0.0/8:80`

`*:80` (alternatively noted as `0.0.0.0/0:80`)

`*:*` (alternatively noted as `any:any, 0.0.0.0/0:any`)

The following table illustrates how inbound destination addresses map to the configured VIPs:

Inbound destination address	VIP
`10.10.10.10:80`	`10.10.10.10/32:80` - address match and port match
`10.10.10.11:80`	`10.10.0.0/16:80` - most specific address match and port match
`10.1.10.10:80`	`10.0.0.0/8:80` - most specific address match and port match
`20.0.0.0:80`	`20.0.0.0/8:80` - most specific address match and port match
`20.0.0.0:443`	`20.0.0.0/8:*` - most specific address match with wildcard port
`1.1.1.1:443`	`*:*` - wildcard address and wildcard port

Further changes in the order of precedence applied to new inbound connections are in Version 11.3 and later. If you care to read on this it can be found at the following location.

SOL14800: Order of precedence for virtual server matching (11.3.0 and later)

1.01 – Explain how a virtual server processes a request

SOL8082: Overview of TCP connection setup for BIG-IP LTM virtual server types

Standard virtual server

The BIG-IP LTM TMOS operating system implements ”full proxy” architecture for virtual servers configured with a TCP profile. By assigning a custom TCP profile to the virtual server, you can configure the BIG-IP LTM to maintain compatibility to disparate server operating systems in the data center. At the same time, the BIG-IP LTM can leverage its TCP/IP stack on the client side of the connection to provide independent and optimized TCP connections to client systems.

In a full proxy architecture, the BIG-IP LTM appears as a TCP peer to both the client and the server by associating two independent TCP connections with the end-to-end session. Although certain client information such as the source IP address or source TCP port, may be re-used on the server side of the connection; the BIG-IP LTM system manages the two sessions independently, making itself transparent to the client and server.

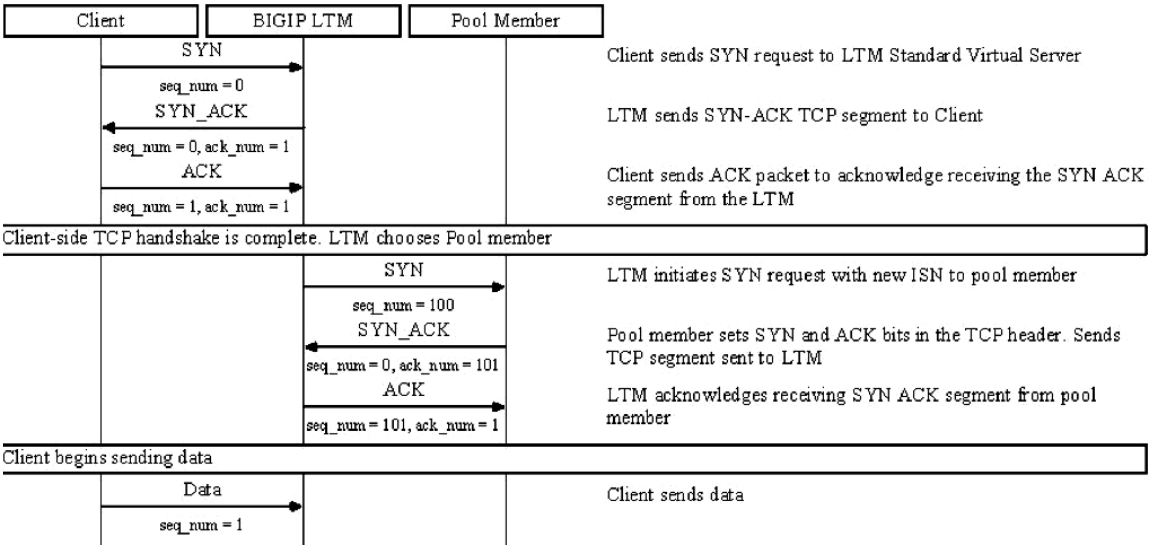
The Standard virtual server requires a TCP or UDP profile, and may optionally be configured with HTTP, FTP, or SSL profiles if Layer 7 or SSL processing is required.

The TCP connection setup behavior for a Standard virtual server varies depending on whether a TCP profile or a TCP and Layer 7 profile, such as HTTP, is associated with the virtual server.

Standard virtual server with a TCP profile

The TCP connection setup behavior for a Standard virtual server operates as follows: the three-way TCP handshake occurs on the client side of the connection before the BIG-IP LTM initiates the TCP handshake on the server side of the connection.

A Standard virtual server processes connections using the full proxy architecture. The following TCP flow diagram illustrates the TCP handshake for a Standard virtual server with a TCP profile:



1.01 – Given a specific connectivity issue, isolate where the problem might be according to the processing order

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

In general, all trouble shooting should be done in an order that allows for narrowing of the possible issue. When there is an issue with connectivity to a virtual server, there can be many reasons. Gather what you know. When you or the client tried to connect to the virtual server, how was it done? Was it through a browser or another application? What was the path that was used? (ie https://www.yoursite.com)

Starting out with checking to see if you have IP connectivity to the virtual server is a good place to start. This is a sort of “divide and conquer” approach to solve the issue. Can you reach the virtual servers IP address from your location on the network? Start with a ping of the virtual server address. If you can ping the IP we know that the F5 is listening. Now are you connecting to the port number the virtual server is listening on?

If you were browsing to https://www.yoursite.com, does the DNS name of www.yoursite.com resolve to the IP the address the virtual server is configured on? If not, is it the NAT address of the firewall that translates to the virtual server address?

If all the network connectivity looks good, is the virtual server configured correctly for the type of traffic that is trying to pass? Perhaps the administrator has applied a profile to the virtual server telling it to process http traffic when the virtual server is set to listen on 443. Without terminating the SSL traffic the virtual server cannot process http traffic and the virtual server will not work correctly.

These are just a few of the scenarios that you can be faced with trying to figure out why a connection to an application may not be working. Spending time on the vLabs and getting comfortable with interface and configuring virtual servers will help you understand how the BIG-IP LTM works.

Objective - 1.02 - Identify the reason for an unresponsive virtual server

1.02 - Determine the state of a virtual server (offline, enabled, etc.)

LTM Virtual Concepts

At any time, you can determine the status of a virtual server or virtual address, using the Configuration utility. You can find this information by displaying the list of virtual servers or virtual addresses and viewing the Status column, or by viewing the Availability property of the object.

The Configuration utility indicates status by displaying one of several icons, distinguished by shape and color:

- The shape of the icon indicates the status that the monitor has reported for that node.
- The color of the icon indicates the actual status of the node.

To understand these icons with respect to status, see the table below.

Table 2.5 Explanation of status icons for virtual servers and virtual addresses

Status indicator	Explanation
	The virtual server or virtual address is **enabled** and able to receive traffic.
	The virtual server or virtual address is enabled but is **currently unavailable**. However, the virtual server or virtual address might become available later, with no user action required. An example of a virtual server or virtual address showing this status is when the objects connection limit has been exceeded. When the number of connections falls below the configured limit, the virtual server or virtual address becomes available again.
	The virtual server or virtual address is enabled but **offline** because an associated object has marked the virtual server or virtual address as unavailable. To change the status so that the virtual server or virtual address can receive traffic, you must actively enable the virtual server or virtual address.
	The virtual server or virtual address is operational but set to **Disabled**. To resume normal operation, you must manually enable the virtual server or virtual address.
	The status of the virtual server or virtual address is **unknown**.

1.02 - Determine if a virtual server is configured with the proper IP address configuration

GUI Study in the vLabs

LTM Virtual Concepts

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

A virtual address is the IP address with which you associate a virtual server. For example, if a virtual server's IP address and service are `10.10.10.2:80`, then the IP address `10.10.10.2` is a virtual address.

You can create a many-to-one relationship between virtual servers and a virtual address. For example, you can create the three virtual servers `10.10.10.2:80, 10.10.10.2:443`, and `10.10.10.2:161` for the same virtual address of `10.10.10.2`.

You can enable and disable a virtual address. When you disable a virtual address, none of the virtual servers associated with that address will receive incoming network traffic.

You create a virtual address indirectly when you create a virtual server. When this happens, Local Traffic Manager internally associates the virtual address with a MAC address. This in turn causes the BIG-IP system to respond to Address Resolution Protocol (ARP) requests for the virtual address, and to send gratuitous ARP requests and responses with respect to the virtual address.

If the address you entered is not the correct address that your clients are attempting to connect to, the symptom will seem as if the BipIP is not working. This is a very common issue when DNS entries that resolve a name to the virtual server IP address do not correlate. If your clients are connecting to a DNS name make sure that it resolves to the intended virtual server IP address or NAT address on the firewall that maps to the virtual server IP address.

1.02 - Determine if a virtual server is configured for the proper listening port

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

When you configure a virtual server and define the virtual address and service port; this is how the virtual server is listening on the network. If the service port you have configured is not the appropriate port number for the type of connection that your clients are attempting to make, the connection will likely fail. Understanding how your clients intend to connect to the virtual server is usually a good sanity check on the configuration.

1.02 - Determine if the virtual server is configured with the appropriate profiles

A virtual server has a number of properties and settings that you can configure to affect the way that a virtual server manages traffic. You can also assign certain resources to a virtual server, such as a load balancing pool and a persistence profile. Together, these properties, settings, and resources represent the definition of a virtual server, and most have default values. When you create a virtual server, you can either retain the default values or adjust them to suit your needs.

In addition to assigning various traffic profiles to a virtual server, you can also assign a pool, an iRule, and two persistence profiles. The pool, iRule, and persistence profiles that you assign to a virtual server are known as resources.

If you have created a virtual server that is a load balancing type of virtual server, one of the resources you must assign to the virtual server is a default load balancing pool. A default pool is the pool to which Local Traffic Manager sends traffic if no iRule exists specifying a different pool. Note that if you plan on using an iRule to direct traffic to a pool, you must assign the iRule as a resource to the virtual server.

In the Configuration utility, virtual server settings are grouped into three categories: General properties, configuration settings (basic and advanced), and resources (basic and advanced). The following sections describe the settings that these three categories contain.

How profiles are assigned to the virtual server can affect the virtual servers ability to process the traffic that is passing through it. For instance if you create a virtual server that is listening on `10.10.10.2:443`, and you also assign an http profile to process the http traffic according to your needs. The virtual server will not respond to connections as expected. The virtual server settings say to take in encrypted traffic on port 443 and then process and possible manipulate the http headers. This is impossible without first terminating the encrypted traffic with a clientside SSL profile to make the encrypted traffic clear text for the BIG-IP to then apply the http profile. If you apply a visual map of the OSI model to the functional parts of the virtual server's configuration it is easier to see what may be needed or may be conflicting with each other. This is covered in depth in the F5 Certified Training course.

1.02 - Determine if the pool configuration has an effect on virtual server state

GUI Study in the vLabs

If all pool members are offline or misconfigured the virtual server's state can be affected. All heath status information trickles up to the virtual server.

This means that if a node is not online due to a monitor marking the node offline, any pool member using that node will be marked offline as well. And if all members of a pool are maked offline by a failing health monitor the virtual server will have no available resources so it will be marked offline as well.

To see if a virtual server is not available due to a lack of resources look in the GUI under Local Traffic and click on the Network Map/Show Map and search for the virtual server in question. If it is down you can see in the same pane if the resources are also offline.

1.02 - Determine which tools to use in order to diagnose the issue

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

There are multiple tools you can use to check to see if a server behind the BIG-IP is working as expected.

If you have a workstation on the local server subnet you can make a direct connection to the server to see the response. Or if you have a route to the server's IP subnet from your current network location you can try to connect to the server directly. If it is responding then look to see if the pool member is configured to match how you just connected to the server (IP:port).

You can see if the BIG-IP has connectivity to the IP address of the server using the ping command from the command line interface of the BIG-IP.

If there is IP connectivity then you can try to use the CURL command to see if the BIG-IP can connect to the website on the server or FTP if the server is listening for FTP traffic.

1.02 - Explain the difference between the virtual servers status definitions

GUI Study in the vLabs

A virtual servers status icon is a quick way to see the high level status of the virtual server. The five different status levels are Enabled, Offline, Currently Unavailable, Unknown and Disabled. Each of these levels are pretty self explanatory.

- Enabled means that the virtual server is up and available for traffic (monitors are succeeding) and is represented by a green circle icon.
- Offline means that the resource for the virtual server is not available (likely a failing monitor) and is represented by a red diamond icon.
- Currently Unavailable means that the virtual server or all of it's resources have reached a restricting connection limit that has been set by the administrator and the virtual server currently has no further capacity for traffic until the current connections fall below the connection limit settings. A yellow triangle icon represents the Currently Unavailable status.

- Unknown means that there is not any monitors set for the resources of the virtual server, so there is no status to show and is represented by a blue square icon. This status does not mean that the virtual server will not respond to traffic. A virtual server with an Unknown status will take in traffic and send it on to the resources even if they are not online.
- Disabled means that the administrator has marked the virtual server down so that it will not process traffic. The status icon will be a shape that represents the current monitor status of the virtual server but will always be colored black. Examples of this status icon would be; if the virtual server has succeeding monitors but is disabled the icon would be a black circle, or if the virtual server has failing monitors but is disabled the icon would be a black diamond or if the virtual server has no monitors but is disabled the icon would be a black square.

Objective - 1.03 - Identify the reason for an unresponsive pool member

Pool Intro:

LTM Pools Concepts

In a typical client-server scenario, a client request goes to the destination IP address specified in the header of the request. For sites with a large amount of incoming traffic, the destination server can quickly become overloaded as it tries to service a large number of requests. To solve this problem, BIG-IP Local Traffic Manager distributes client requests to multiple servers instead of to the specified destination IP address only. You configure Local Traffic Manager to do this when you create a load balancing pool.

You can enable or disable individual pool members. When you enable or disable a pool member, you indirectly set the value of the pool members State property, in the following way:

- Enable - Sets the State property of the pool member to Enabled.
- Disable - Sets the State property of the pool member to Disabled.

Note that the difference between a disabled pool member, and a pool member that a monitor reports as down, is that a disabled pool member continues to process persistent and active connections. Conversely, a pool member reported as down processes no connections whatsoever.

The status icons on the pool-member list screen and properties screen indicate whether a pool member is currently enabled or disabled.

Pool status

An important part of managing pools and pool members is viewing and understanding the status of a pool or pool member at any given time. The Configuration utility indicates status by displaying one of several icons, distinguished by shape and color, for each pool or pool member:

The shape of the icon indicates the status that the monitor has reported for that pool or pool member. For example, a circle-shaped icon indicates that the monitor has reported the pool member as being up, whereas a diamond-shaped icon indicates that the monitor has reported the pool member as being down.

The color of the icon indicates the actual status of the node itself. For example, a green shape indicates that the node is up, whereas a red shape indicates that the node is down. A black shape indicates that user-intervention is required.

At any time, you can determine the status of a pool. The status of a pool is based solely on the status of its members. Using the Configuration utility, you can find this information by viewing the Availability property of the pool. You can also find this information by displaying the list of pools and checking the Status column.

The Configuration utility indicates pool status by displaying one of several icons, distinguished by shape and color. To understand these icons, see table below.

Table 4.4 Explanation of status indicators for pools

Status indicator	Explanation
	At least one pool member is available for processing traffic.
	No pool members are currently available but any one of them could become available later, with no user action required. An example of an unavailable pool member becoming available automatically is when the number of concurrent connections to the pool member no longer exceeds the value defined in the pool members Connection Limit setting.
	All pool members are unavailable and therefore cannot accept traffic. A reason for a pool member being unavailable is that an associated EAV monitor has detected that the pool member is unavailable. When pool status is red, user action is usually required.
	The status of at least one pool member is unknown, and no other pool members are available. Sample reasons for unknown pool-member status are: One or more pool members has no associated monitor. Monitor results are not available yet. The pool members IP address is misconfigured. The parent node has been disconnected from the network.

1.03 - Discuss the effects of health monitors on the status of pool members/nodes

LTM Pools Concepts

Health monitors are a key feature of Local Traffic Manager. Health monitors help to ensure that a server is in an up state and able to receive traffic. When you want to associate a monitor with an entire pool of servers, you do not need to explicitly associate that monitor with each individual server. Instead, you can simply assign the monitor to the pool itself. Local Traffic Manager then automatically monitors each member of the pool.

Local Traffic Manager contains many different pre-configured monitors that you can associate with pools, depending on the type of traffic you want to monitor. You can also create your own custom monitors and associate them with pools. The only monitor types that are not available for associating with pools are monitors that are specifically designed to monitor nodes and not pools or pool members. That is, the destination address in the monitor specifies an IP address only, rather than an IP address and a service port. These monitor types are:

- ICMP
- TCP Echo
- Real Server
- SNMP DCA
- SNMP DCA Base
- WMI

With Local Traffic Manager, you can configure your monitor associations in many useful ways:

You can associate a health monitor with an entire pool instead of an individual server. In this case, Local Traffic Manager automatically associates that monitor with all pool members, including those that you add later. Similarly, when you remove a member from a pool, Local Traffic Manager no longer monitors that server.

When a server that is designated as a pool member allows multiple processes to exist on the same IP address and port, you can check the health or status of each process. To do this, you can add the server to multiple pools, and then within each pool, associate a monitor with that server. The monitor you associate with each server checks the health of the process running on that server.

When associating a monitor with an entire pool, you can exclude an individual pool member from being associated with that monitor. In this case, you can associate a different monitor for that particular pool member, or you can exclude that pool member from health monitoring altogether. For example, you can associate pool members A, B, and D with the http monitor, while you associate pool member C with the https monitor.

You can associate multiple monitors with the same pool. For instance, you can associate both the http and https monitors with the same pool.

1.03 - Determine the state and availability of the pool member/node in question

LTM Pools Concepts

Table 4.5 Explanation of status icons for pool members

Status indicator	Explanation	State property is set to...
	The pool member is set to Enabled, the parent node is up, and a monitor has marked the pool member as up.	Enabled (All Traffic Allowed)
	The pool member is unavailable, but could become available later with no user interaction required. This status occurs when the number of concurrent connections has exceeded the limit defined in the pool members Connection Limit setting.	Enabled (All Traffic Allowed)
	The pool member is unavailable because either the parent node is down, a monitor has marked the pool member as down, or a user has disabled the pool member.	Enabled (All Traffic Allowed)
	The pool member is set to Disabled, although a monitor has marked the pool member as up. To resume normal operation, you must manually enable the pool member.	Disabled (Only persistent or active connections allowed)
	The pool member is set to Disabled and is offline because the parent node is down. To resume normal operation, you must manually enable the pool member.	Forced Offline (Only active connections allowed)
	The pool member is set to Disabled and is offline because a user disabled it. To resume normal operation, you must manually enable the pool member.	Disabled (Only persistent or active connections allowed)
	The pool member is set to Disabled and is offline because either the parent node is down, or a monitor has marked the pool member as down. To resume normal operation, you must manually enable the pool member.	Forced Offline (Only active connections allowed)
	The pool member or node has no monitor associated with it, or no monitor results are available yet	Enabled (All Traffic Allowed)

1.03 - Verify the pool member/node Ratio configuration

Ratio weights for pool members

When using a ratio-based load balancing method for distributing traffic to servers within a pool, you can assign a ratio weight to the corresponding pool members. The ratio weight is used by the Local Traffic Manager to distribute connections among pool members or nodes in a static rotation. The number of connections that each system receives over time is proportionate to the ratio weight you defined for each pool member or node.

The ratio-based load balancing methods are: Ratio (node, member, and sessions), Dynamic Ratio (node and member), and Ratio Least Connections (node and member).

1.03 - Verify the pool member/node connection configuration and count

You can configure a virtual server, pool member, or node to prevent an excessive number of connection requests during events such as a Denial of Service (DoS) attack or a planned, high-demand traffic event. To ensure the availability of a virtual server, pool member, or node, you can use the BIG-IP Local Traffic Manager to manage the total number of connections and the rate at which connections are made.

When you specify a connection limit, the system prevents the total number of concurrent connections to the virtual server, pool member, or node from exceeding the specified number.

When you specify a connection rate limit, the system controls the number of allowed new connections per second, thus providing a manageable increase in connections without compromising availability.

After configuring connection limits and connection rate limits on a virtual server, or after configuring these limits on a pool member or node associated with a virtual server, the system controls the total number of concurrent connections and the rate of new connections to the virtual server, pool member, or node.

Objective - 1.04 - Identify a persistence issue

1.04 - Explain the concept of “persistence”

Session Persistence Profiles

Using BIG-IP Local Traffic Manager, you can configure session persistence. When you configure session persistence Local Traffic Manager tracks and stores session data, such as the specific pool member that serviced a client request. The primary reason for tracking and storing session data is to ensure that client

requests are directed to the same pool member throughout the life of a session or during subsequent sessions when an application requires it to be so.

In addition, session persistence can track and store other types of information, such as user preferences or a user name and password.

Local Traffic Manager offers several types of session persistence, each one designed to accommodate a specific type of storage requirement for session data. The type of persistence that you implement depends on where and how you want to store client-specific information, such as items in a shopping cart or airline ticket reservations.

For example, you might store airline ticket reservation information in a back-end database that all servers can access, or on the specific server to which the client originally connected, or in a cookie on the client's machine. When you enable persistence, returning connections will not be load balancing and instead will be sent to the server to which they last connected in order to access application again.

Local Traffic Manager keeps session data for a period of time that you specify.

The primary tool for configuring session persistence is to configure a persistence profile and assign it to a virtual server. If you want to enable persistence for specific types of traffic only, as opposed to all traffic passing through the virtual server, you can write an iRule.

To configure and manage persistence profiles, log in to the BIG-IP Configuration utility, and on the Main tab, expand Local Traffic, and click Persistence.

1.04 - Verify the type of persistence profile assigned to the virtual server in question

Session Persistence Profiles

A persistence profile is a pre-configured object that automatically enables persistence when you assign the profile to a virtual server. By using a persistence profile, you avoid having to write a program to implement a type of persistence.

Each type of persistence that Local Traffic Manager offers includes a corresponding default persistence profile. These persistence profiles each contain settings and setting values that define the behavior of the BIG-IP system for that type of persistence. You can either use the default profile or create a custom profile based on the default.

Persistence profile types:

You can configure persistence profile settings to set up session persistence on the BIG-IP system. You can configure these settings when you create a profile or after profile creation by modifying the profiles settings.

The persistence types that you can enable using a persistence profile are:

Cookie persistence

Cookie persistence uses an HTTP cookie stored on a clients computer to allow the client to reconnect to the same server previously visited at a web site.

Destination address affinity persistence

Also known as sticky persistence, destination address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the destination IP address of a packet.

Hash persistence

Hash persistence allows you to create a persistence hash based on an existing iRule.

Microsoft Remote Desktop Protocol persistence

Microsoft Remote Desktop Protocol (MSRDP) persistence tracks sessions between clients and servers running the Microsoft Remote Desktop Protocol (RDP) service.

SIP persistence

SIP persistence is a type of persistence used for servers that receive Session Initiation Protocol (SIP) messages sent through UDP, SCTP, or TCP.

Source address affinity persistence

Also known as simple persistence, source address affinity persistence supports TCP and UDP protocols, and directs session requests to the same server based solely on the source IP address of a packet.

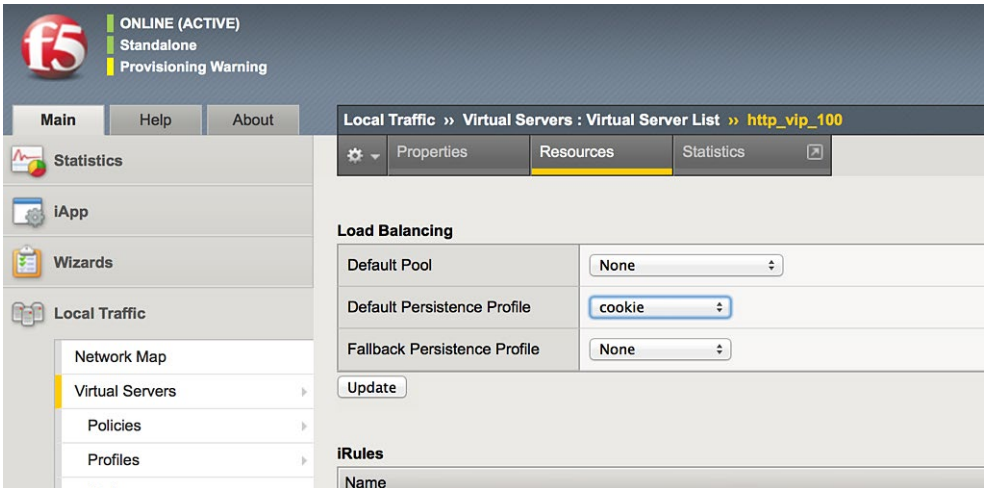
SSL persistence

SSL persistence is a type of persistence that tracks non-terminated SSL sessions, using the SSL session ID. Even when the clients IP address changes, Local Traffic Manager still recognizes the connection as being persistent based on the session ID. Note that the term non-terminated SSL sessions refer to sessions in which Local Traffic Manager does not perform the tasks of SSL certificate authentication and encryption/re-encryption.

Universal persistence

Universal persistence allows you to write an expression that defines what to persist on in a packet. The expression, written using the same expression syntax that you use in iRules®, defines some sequence of bytes to use as a session identifier.

You can see the type of persistence assigned to a virtual server by going to Local Traffic > Virtual Servers in the GUI and selecting the virtual server from the list you wish to inspect. Click on the Resources tab and look at the settings for the Default Persistence Profile setting and the Fallback Persistence Profile setting. To change the setting you can select the name of the profile you created or wish to use, such as cookie. This implements cookie persistence, using the default cookie persistence profile.



1.04 - Differentiate between fallback and primary persistence

GUI Study in the vLabs

The administrator of a BIG-IP can set a primary persistence type for a virtual server as shown in the previous section. A fallback persistence type can also be set. Only IP address based persistence types are allowed as fallback. This means that along with honoring the primary persistence method there is a second record being kept that can be used to persist the client's transaction to the resource of the virtual server as well. For example if cookie persistence is set with a fallback of sourceaddr, as a client makes their second connection to the virtual server the cookie from the first connection will be used to determine the server in the pool to send the connection to. But at the same time as the first connection was made to the virtual server a source address persistence record was also created. And if the client did not have the cookie any longer the record matching their IP address would still exist (if it had not timed out) and could be used to get them back to their original pool member.

However this also means that if a source address persistence profile is used as a fallback that has a wider subnet in the configuration such as a `255.255.255.0`, and a second client from the same class C network as the first client made their first connection to the virtual server. They would be persisted to the same pool member as the first client since they would match the source IP record of the first client even though they did not have a cookie when they connected.

1.04 - Validate the expected persistence behavior

GUI Study in the vLabs- Module 8 Exercises

As you connect to an application through the virtual server of the BIG-IP platform the first connection is load balanced to the best available resource according to the load-balancing algorithm. With persistence enabled the following connections from the same client will be sent to the same resource as their first initial load balanced connection.

Checking to see if the client is being persisted is simple in a test scenario where a single client connects to the virtual server and the statistics on the system show the connections only going to the same resource in the pool.

However in regular production volume it will be hard to see the individual client connections hitting the same resource when there are hundreds or thousands of connections coming in all the time. An easy way to see that the client is connecting to the same server resource is to have watermarks on the application webpages. These watermarks will show a unique mark on the web page identifying it to the individual server, much like we use in the vLabs on the load-balanced sites. Not all developers will take the time or effort to do this water marking. If you do not have the ability to add a watermark to your page then there needs to be another method.

In the BIG-IP platform you have the ability to show the active connection table and use filters to show the data you want to see. So to show a client's current connection in the connection table you can type the following command:

In version 9.X and 10.X:

```
bigpipe conn show | grep "client IP"
```

In version 11.x:

```
tmsh show sys conn cs-client-addr "client IP"
```

1.04 - Use the appropriate tool to troubleshoot persistence

GUI Study in the vLabs

If the persistence method you are using is not tracked locally by the BIG-IP system, such as Cookie persistence; then there are no local records on the BIG-IP to review. This is due to the fact that the cookie containing the pool member info is passed to the client system from the BIG-IP, and when the client makes the next connection it will include the cookie from the previous in the request for the BIG-IP system to use for the persistence info. Allowing the BIG-IP to simply read the cookie and not have to locally store the info. An administrator can find the cookie on the client's workstation. It is stored where the client's local browser would normally store cookies. This location will vary by browser type and OS type.

If the persistence method you are using is tracked by the BIG-IP system locally, such as Source Address Affinity persistence, then you can look at the records that are stored on the local system using the following methods:

- Source Address persistence records can be found in the Configuration Utility, open the Statistics > Module Statistics > Local Traffic page and select Persistence Records from the Statistics Type list.
- In version 11.X command line do: tmsh show /ltm persistence persist-records
- In version 9.X and 10.X command line do: B persist show all

SECTION 2 - TROUBLESHOOT BASIC HARDWARE ISSUES

Objective - 2.01 Perform an End User Diagnostic and interpret the output

2.01 - Reboot an F5 platform into the EUD

Field Testing BIG-IP Hardware

You can run the EUD only from a console connected to the BIG-IP system. You can start the EUD using the following methods:

- Attach a USB CDROM drive containing the bootable system CD. As the system boots up, the EUD starts.
- Attach a USB mass storage device drive with the EUD boot image loaded. As the system boots up, the EUD starts.
- While the system is booting, select the End User Diagnostics option from the boot menu.

You can then run the tests that are necessary.

After you have completed the tests you want to run, use option 21 to exit the EUD and reboot the system. You must use this option to exit the EUD. Using other methods, such as rebooting or using the command menu, can destabilize the system.

2.01 - Download output from the unit an EUD was run on

Field Testing BIG-IP Hardware

An End User Diagnostic or EUD report log is stored as a text file named eud.log in the /shared/log/ directory on the host file system.

If you have run an EUD Test on the system it will be available in this location. You can connect to the console IP address of the BIG-IP system and use and SCP tool to get the file off of the system, to upload to the F5 Support case.

2.01 - Interpret the output from an EUD and determine if the test passed or failed

Field Testing BIG-IP Hardware

When all tests complete correctly, the following message displays:

```
Completed test with 0 errors.
```

Objective - 2.02 Interpret the LCD Warning Messages

2.02 - Locate the LCD on an F5 Platform

Operating the LCD Panel

The liquid crystal display, or LCD panel, provides the ability to control the unit without attaching a serial or network cable. The following menus are available on the LCD panel.

Information menu

Use the Information menu to find information about using the LCD and its functionality.

System menu

Use the System menu to reboot, netboot, or halt the unit. This menu also has options for setting the properties of the management interface (MGMT) and the serial port

Screens menu

Use the Screens menu to set up the informational screens you would like the LCD to cycle through. The information screens include system status, statistics, and system alerts.

Options menu

Use the Options menu to configure the properties of the LCD panel.

The LCD panel is located on the front of all F5 hardware except for the Viprion 2400 Series Chassis. A separate USB attachable LCD panel is available for the Viprion 2400 Series Chassis.

2.02 - Correlate the LCD message to message in the corresponding log file

Front panel LED indicator behavior for legacy platforms

Alert conditions

Alerts that affect the behavior of the Alarm LED indicator are defined in the /etc/alertd/alert.conf file. The lcdwarn function of an alert definition defines which alerts will modify the Alarm LED indicator.

As an example, the default alertd process conditions in BIG-IP version 9.2 are defined in the following table:

Description	Alert Level	LED behavior
CPU Temp too high	3 - Critical	Solid Red
CPU fan too slow	3 - Critical	Solid Red
CPU fan bad	3 - Critical	Solid Red
Chassis Temp too high	3 - Critical	Solid Red
Chassis Fan bad	3 - Critical	Solid Red
Power Supply bad	4 - Emergency	Blink Red
Unit going standby	0 - Warning	Solid Yellow
Unit going Active	0 - Warning	Solid Yellow
The license validation failed	2 - Alert	Solid Red
The license has expired	2 - Alert	Solid Red
Blocking DoS attack	2 - Alert	Solid Red
Hard disk is failing	4 - Emergency	Blink Red

The events that trigger LCD screen events and lights are written to log files. You may want to look up more information on the logged events. For example, the BIG-IP system may generate an error messages to the /var/log/ltm file that contains the following event:

```
emerg system_check[11277]: 010d0010:0: Power supply #2 fan-1: fan speed (0) is too low.
```

2.02 - Identify which tasks the buttons on the LCD perform

Pressing the X button puts the LCD panel in Menu. The buttons Left Arrow, Right Arrow, Up Arrow, and Down Arrow are only functional when the LCD is in Menu mode for navigation. The ✔ check button is used to select and confirm selections.

Objective - 2.03 Identify a possible hardware issue within the log files

2.03 - Indicate which logs would contain debugging information

Logging

If you are using the Syslog utility for local logging, whether or not you are using the high-speed logging mechanism you can view and manage the log messages, using the BIG-IP® Configuration utility.

The local Syslog logs that the BIG-IP system can generate include several types of information. For example, some logs show a timestamp, host name, and service for each event. Moreover, logs sometimes include a status code, while the audit log shows a user name and a transaction ID corresponding to each configuration change. All logs contain a one-line description of each event.

For local log messages that the BIG-IP system stores in the local Syslog data base, the BIG-IP system automatically stores and displays log messages in these categories:

- System messages
- Packet filter messages
- Local Traffic messages
- Global Traffic messages
- BIG-IP system configuration (audit) messages

Each type of event is stored locally in a separate log file, and the information stored in each log file varies depending on the event type. All log files for these event types are in the directory /var/log.

The product specific logs like /var/log/ltm, var/log/gtm, etc will contain debug info relative to that product. If you are logging from an irule you can define what log file you want to write your debug info into by specifying the local facility you chose.

2.03 - Given a log file, determine the nature of a hardware issue

Event Logging

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

You may look in the logs and see there are many events. Perhaps you notice an event like this:

```
Mon Feb 14 o4:36:06 PST 2005   bigip2   bcm56xxd(785)   00010012   Link 2.5 is up
```

This could have been caused by the administrator turning up a new interface or because the interface lost connectivity to the upstream switch. Some events can be self-explanatory while others may be more cryptic and need some deciphering.

Understanding log content

The logs that the BIG-IP system generates include several types of information. For example, some logs show a timestamp, host name, and service for each event. Moreover, logs sometimes include a status code, while the audit log shows a user name and a transaction ID corresponding to each configuration change. All logs contain a 1-line description of each event.

The table below lists the categories of information contained in the logs and the specific logs in which the information is displayed.

Log information categories and their descriptions

Information Type	Explanation	Log Type
Timestamp	The time and date that the system logged the event message.	System Packet Filter Local Traffic Audit
Host name	The host name of the system that logged the event message. Because this is typically the host name of the local machine, the appearance of a remote host name could be of interest.	System Packet Filter Local Traffic
Service	The service that generated the event.	System Packet Filter Local Traffic
Status code	The status code associated with the event. Note that only events logged by BIG-IP system components, and not Linux system services, have status codes.	Packet Filter Local Traffic
Description	The description of the event that caused the system to log the message.	System Packet Filter Local Traffic
User Name	The name of the user who made the configuration change.	Audit
Transaction ID	The identification number of the configuration change.	Audit
Event	A description of the configuration change that caused the system to log the message.	Audit

2.03 - Given a possible issue, determine which log file entries to review

Viewing and managing log messages are an important part of maintaining a BIG-IP system. Log messages inform you on a regular basis of the events that are happening on the system. Some of these events pertain to general events happening within the operating system, while other events are specific to the BIG-IP system, such as the stopping and starting of BIG-IP system services.

The mechanism that the BIG-IP system uses to log events is the Linux utility syslog-ng. The syslog-ng utility is an enhanced version of the standard UNIX and Linux logging utility syslog.

The types of events that the BIG-IP system logs are:

System events

System event messages are based on Linux events, and are not specific to the BIG-IP system.

Packet filter events

Packet filter messages are those that result from the implementation of packet filters and packet-filter rules.

Local traffic events

Local-traffic event messages pertain specifically to the local traffic management system.

Audit events

Audit event messages are those that the BIG-IP system logs as a result of changes to the BIG-IP system configuration. Logging audit events is optional.

To configure and manage event logging, log in to the BIG-IP Configuration utility, and on the Main tab, expand System, and click Logs.

As described in Introducing BIG-IP system logging, the BIG-IP system automatically logs four main event types: system, packet filter, local traffic, and configuration changes (audit). Each type of event is stored in a separate log file, and the information stored in each log file varies depending on the event type. All log files for these event types are in the directory /var/log.

Logging system events

Many events that occur on the BIG-IP system are Linux-related events, and do not specifically apply to the BIG-IP system.

Using the Configuration utility, you can display these system messages. The table below shows some sample system log entries.

Sample system log entries

Timestamp	Host	Service	Event
Mon Feb 14 03:34:45 PST 2005	bigip3	syslog-ng[5494]	new configuration initialized
Mon Feb 14 03:35:06 PST 2005	bigip3	syslog-ng[5494]	kjournald starting. Commit interval 5 seconds.
Mon Feb 14 04:38:06 PST 2005	bigip3	EXT3-fs	mounted filesystem with ordered data mode.

Logging packet filter events

Some of the events that the BIG-IP system logs are related to packet filtering. The system logs the messages for these events in the file /var/log/pktfilter.

Using the Configuration utility, you can display these packet filter messages.

Logging local traffic events

Many of the events that the BIG-IP system logs are related to local area traffic passing through the BIG-IP system. The BIG-IP system logs the messages for these events in the file /var/log/ltm.

Using the Configuration utility, you can display these local-traffic messages. The table below shows some sample local-traffic log entries.

Sample local-traffic log entries

Timestamp	Host	Service	Status Code	Event
Mon Feb 14 03:34:45 PST 2005	bigip2	bcm56xxd(785)	00010013	Starting packet registry event timer
Mon Feb 14 03:35:06 PST 2005	bigip2	bcm56xxd(785)	00010013	Starting HA heartbeat timer tick
Mon Feb 14 04:38:06 PST 2005	bigip2	bcm56xxd(785)	00010013	Successful start. Entering main message loop
Mon Feb 14 o4:36:06 PST 2005	bigip2	bcm56xxd(785)	00010012	Link 2.5 is up

Some of the specific types of events that the BIG-IP system displays on the Local Traffic logging screen are:

- Address Resolution Protocol (ARP) packet and ARP cache events
- bigdb database events (such as populating and persisting bigdb variables)
- HTTP protocol events
- HTTP compression events
- IP packet discard events due to exceptional circumstances or invalid parameters (such as a bad checksum)
- Layer 4 events (events related to TCP, UDP, and Fast L4 processing)
- MCP/TMM configuration events

- Monitor configuration events
- Network events (Layers 1 and 2)
- Packet Velocity® ASIC (PVA) configuration events
- iRule events related to run-time iRule processing
- SSL traffic processing events
- General TMM events such as TMM startup and shutdown

Objective - 2.04 Perform a failover to a standby box under the appropriate circumstances

2.04 - Explain, under which circumstances, a failover would be used to determine if an issue is software or hardware related

General Network Study and vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

For example:

If the BIG-IP HA pair is synchronized then the configurations are the same on both systems. If the active system is having an issue and you can't find an issue with the other systems in the environment (Client or Server). The issue may have something to do with the LTM. You could try a fail over of the Active system to the standby system. If the problem resolves then you are likely faced with an issue in the first system and since they were in sync it may be hardware. That hardware issue may be in the LTM or in the network systems that it is connected to. If the fail over did not solve the issue the problem is like a configuration issue and hardware has been eliminated.

2.04 - Use failover as a troubleshooting step in an appropriate situation

General Network Study and vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Since a failover of an HA pair can interrupt current connections of clients and depending on the type of connection they may have made their connection may not recover from the termination of the connection (if connection mirroring is not properly configured for long lived connections), using failover as a troubleshooting step should be done as a last measure. However it can help to narrow down if there is an issue with hardware.

2.04 - Describe the consequences of performing a failover (mirrored connections, persistent connections)

General Network Study and vLabs

For a failover between systems in an HA pair, to be transparent to the clients currently connected to the active unit, the state of the active connections need to be known by the standby system. If the connection states are not know by the standby system when the failover occurs, connections that were being persisted, connections that were being SNAT'd or any active connection state know by the active unit will not survive the failover. To create a stateful failover environment the systems must be configured to mirror the current connection table, persistence records and SNAT table to the standby unit.

SECTION 3 – TROUBLESHOOT BASIC PERFORMANCE ISSUES

Objective - 3.01 Perform a packet capture within the context of a performance issue

A packet capture can be one of the most powerful tools that an administrator has at there command. If you are not use to doing packet captures or have never done one, you should do them in your vLabs as soon as possible to start becoming proficient.

Running tcpdump on a busy system

> **Important:** The BIG-IP system is designed as an application delivery network platform and not as a packet capture device. If you intend to capture traffic under high load conditions, F5 recommends mirroring traffic to a dedicated sniffing device.

Running tcpdump on a BIG-IP system is considered best effort, as it will place more load on the CPU and may result in inaccuracies in the tcpdump output, such as missed packets or packet timestamp irregularities. If you run tcpdump on a heavily loaded BIG-IP system, the packet capture process may not capture all matching traffic, and the statistical values reported by tcpdump may be inaccurate.

If you run tcpdump on a heavily loaded system, F5 recommends using tcpdump filter expressions to mitigate the potential for missed packets.

3.01 - Determine an appropriate location to take the capture

Recommended methods and limitations for running tcpdump on a BIG-IP system

An administrator can also do a capture from their workstation. The will gather traffic between the destination and their workstation, which in most cases is between the virtual server on the LTM and their workstation. Captures can also be done locally on the F5 BIG-IP platform. Doing a capture on the BIG-IP LTM is very strategic since you have the ability to capture both sides of the proxied conversation between the workstation and the back end server resources. Understanding which networks the resources are on for both sides of the conversation will also allow you to narrow the capture using filters in the tcpdump.

F5 recommends that you run tcpdump on a VLAN when you intend to capture traffic for in-depth troubleshooting on the BIG-IP system. When the VLAN is specified in the tcpdump syntax, tcpdump can read packets processed by TMM.

3.01 - Determine the appropriate time to take capture

Command Line Study in the vLabs

The right time to do a capture can be a catch 22. You need to capture the issue; so a capture needs to be done while the problem is occurring. Of course sometimes the problem may only be occurring under peak load. So doing a capture during peak load may be ineffective due to issues mentioned in the opening of this section. However most of the time you can do the capture when the problem is occurring and tightening up the amount of data you capture by using filters will help with overhead.

3.01 - Determine an appropriate tool to use

Overview of packet tracing with the tcpdump utility

The tcpdump utility is a command line packet sniffer with many features and options. For a full description, refer to the tcpdump man pages by typing the following command: man tcpdump

You can read the binary output of a tcpdump using a packet analyzer. Some analyzer software can also be used to capture traffic as well like Wireshark.

Running the tcpdump utility

Following are examples of commands used to run the tcpdump utility:

Selecting an Interface or VLAN

The tcpdump utility is able to sniff for packets on only one interface or VLAN. By default, it selects the lowest numbered interface.

To select an interface, use the -i flag, as follows:

```
tcpdump –i <interface>
```

For example:

To tcpdump a specific interface:

```
tcpdump –i 2.1
tcpdump –i 1.10
```

To tcpdump a specific vlan:

```
tcpdump –i internal
tcpdump –i external
```

To tcpdump the management interface:

```
tcpdump –i eth0
```

Note: Do not attempt to run tcpdump on an interface that contains a colon.

For example:

```
eth0:mgmt
```

Disabling name resolution

By default, tcpdump attempts to look up IP addresses and use names, rather than numbers, in the output. The BIG-IP system must wait for a response from the DNS server, so the lookups can be time consuming and the output may be confusing.

To disable name resolution, use the -n flag as in the following examples:

```
tcpdump -n
tcpdump -ni internal
```

Saving tcpdump output to a file

You can save the tcpdump data to one of the following file formats:
A binary file that contains all the information collected by the tcpdump and is readable by the tcpdump utility as well as many other traffic analysis packages.

A text file that contains a subset of the full tcpdump data, but is readable only as plain text.

When working with F5 Technical Support, you must provide the tcpdump output in the binary file format.

Binary file

To save the tcpdump output to a binary file, type the following command:

```
tcpdump -w <filename>
```

For example:

```
tcpdump -w dump1.bin
```

Note: The tcpdump utility does not print data to the screen while it is capturing to a file. To stop the capture, press CTRL-C.

Text file

To save the tcpdump output to a text file, type the following command:

```
tcpdump ><filename>
```

For example:

```
tcpdump >dump1.txt
```

Reading tcpdump binary file output

To read data from a binary tcpdump file (that you saved by using the tcpdump -w command), type the following command:

```
tcpdump –r <filename>
```

For example:

```
tcpdump –r dump1.bin
```

In this mode, the tcpdump utility reads stored packets from the file, but otherwise operates just as it would if it were reading from the network interface. As a result, you can use formatting commands and filters.

Beginning in BIG-IP 11.2.0-HF3, 11.2.1-HF3, and 11.3.0, a pseudo header which includes the following parameters is added to the start of each binary tcpdump capture:
The tcpdump command syntax used, including all options
Version of software
Hostname of the system
Platform ID
Product

Filters

The tcpdump utility allows you to use filters to, among other things, restrict the output to specified addresses, ports, and tcp flags.

Filtering on a host address

To view all packets that are traveling to or from a specific IP address, type the following command:

```
tcpdump host <IP address>
```

For example:

```
tcpdump host 10.90.100.1
```

To view all packets that are traveling from a specific IP address, type the following command:

```
tcpdump src host <IP address>
```

For example:

```
tcpdump src host 10.90.100.1
```

To view all packets that are traveling to a particular IP address, type the following command:

```
tcpdump dst host <IP address>
```

For example:

```
tcpdump dst host 10.90.100.1
```

Filtering on a port

To view all packets that are traveling through the BIG-IP system and are either sourced from or destined to a specific port, type the following command:

```
tcpdump port <port number>
```

For example:

```
tcpdump port 80
```

To view all packets that are traveling through the BIG-IP system and sourced from a specific port, type the following command:

```
tcpdump src port<port number>
```

For example:

```
tcpdump src port 80
```

To view all packets that are traveling through the BIG-IP system and destined to a specific port, type the following command:

```
tcpdump dst port <port number>
```

For example:

```
tcpdump dst port 80
```

Filtering on a tcp flag

To view all packets that are traveling through the BIG-IP system that contain the SYN flag, type the following command:

```
tcpdump 'tcp[tcpflags] & (tcp-syn) != 0'
```

To view all packets that are traveling through the BIG-IP system that contain the RST flag, type the following command:

```
tcpdump 'tcp[tcpflags] & (tcp-rst) != 0'
```

Combining filters with the 'and' operator

You can use the and operator to filter for a mixture of output.

Following are some examples of useful combinations:

```
tcpdump host 10.90.100.1 and port 80
tcpdump src host 172.16.101.20 and dst port 80
tcpdump src host 172.16.101.20 and dst host 10.90.100.1
```

Capturing packet data

The tcpdump utility provides an option that allows you to specify the amount of each packet to capture.

You can use the -s (snarf/snaplen) option to specify the amount of each packet to capture. To capture the entire packet, use a value of 0 (zero).

For example:

```
tcpdump -s0 src host 172.16.101.20 and dst port 80
```

Alternatively, you can specify a length large enough to capture the packet data you need to examine.

For example:

```
tcpdump -s200 src host 172.16.101.20 and dst port 80
```

If you are using the tcpdump utility to examine the output on the console during capture or by reading from an input file with the -r option, you should also use the -X flag to display ASCII encoded output along with the default HEX encoded output.

For example:

```
tcpdump -r dump1.bin -X -s200 src host 172.16.101.20 and dst port 80
```

Suppressing hostname and port resolution

The tcpdump utility provides an option that allows you to specify whether IP addresses and service ports are translated to their corresponding hostnames and service names.

Since performing multiple name lookups during a packet capture may be resource intensive, you should disable name resolution while capturing on a busy system using the -n option.

For example:

```
tcpdump -n src host 172.16.101.20 and dst port 80
```

Service port lookups incur less overhead than DNS-based name resolutions, but still are usually unnecessary while performing a capture. You can disable both name and service port resolution while performing a capture, by using the -nn option.

For example:

```
tcpdump -nn src host 172.16.101.20 and dst port 80
```

Combining tcpdump options

This article contains the most essential tcpdump options. You will generally need to use most of the options in combination.

Following are examples of how to combine the tcpdump options to provide the most meaningful output:

```
tcpdump -ni internal -w dump1.bin
tcpdump -ni internal -r dump1.bin host 10.90.100.1
tcpdump -ni 2.1 host 10.90.100.1 and port 80
tcpdump -ni 1.10 src host 172.16.101.20 and dst port 80 >dump1.txt
tcpdump -Xs200 -nni eth0 -w /var/tmp/mgmt.cap dst host 172.16.101.20 and dst port 162
```

3.01 - Ensure the packet capture tool has the capacity to capture (driver/tap)

Command Line Study in the vLabs

If you are using a packet capture tool other than tcpdump on the BIG-IP platform you will need to make sure that the system you are running the capture tool on has access to the local network, which you need to capture. This may mean that you need to be inline between devices or you may need a network tap or a span port. If you are capturing the traffic on your workstation you will need to make sure the network card can support promiscuous mode and has the right drivers to support the capture software.

3.01 - Narrow the scope/context of information being gathered

Command Line Study in the vLabs

Narrowing the capture data by using filters in tcpdump to only capture the needed traffic from nodes in question can greatly reduce the size of the capture as well as the overhead on the system. You can narrow the scope of a capture in many ways. Restricting the capture as narrow as possible to gather only the necessary traffic can sometimes cause you to miss the problem. You may want to start with a full capture of all traffic (as long as the system can handle it) to pinpoint where the basic problem lies and then narrow the capture data with filters in Wireshark or other packet analyzer software. And if you have to gather additional captures you will then know how to narrow based on what you already know about the issue.

3.01 - Given a scenario, determine whether a packet capture is appropriate

Command Line Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

There may be times that determining the source of an issue will not require the administrator to do a capture. When a problem arises look first to the status of the BIG-IP and the configuration. If all of the settings and statistics look fine, you can then check the client settings and client access restrictions before moving on to a capture of the network traffic.

Objective - 3.02 Use BIG-IP tools in order to identify potential performance issues

3.02 - Differentiate between performance issue types (i.e. Latency, Congestion, broken content)

General Network Study

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Latency

Latency is the largest cause of slow Web applications over the WAN or Internet. Latency describes the time delay experienced while a data packet moves from one point to another, usually caused by physical distance and high round-trip times. Latency can also be introduced by compute-intensive processing such as SSL handshaking, bulk encryption/decryption, and TCP session management. Latency can have a profound effect on application performance, even over networks with abundant bandwidth.

Congestion

Network congestion occurs a node or network is processing so much data that its level of service deteriorates. The BIG-IP platform has some built in optimizations to help with network congestion. The TCP profile has a setting to enable Nagles algorithm. Nagles algorithm attempts to reduce network congestion by aggregating smaller TCP packets into larger ones.

3.02 - Establish the frequency of a given issue (random, continuous, isolated, intermittent, repetitive intervals)

General Network Study

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Tracking how often issues occur or for how long an issue is impacting a function can be a telltale sign to what may be happening. This can be done through the use of logs, statistics, network captures and observation.

For instance an administrator wants to load balance a server that is already functioning in their DMZ. They spin up a second instance of the server and place both the new and old server behind an LTM pair off of the DMZ. They use the server's address on the DMZ network for the virtual server address on the LTM and place the servers on a new network behind the LTM, with the LTM acting as the servers default gateway. The firewall administrators add the new server IP addresses to the rule sets allowing all the same server traffic to get to the servers on the new network.

When the servers are brought on-line the users immediately notice a delay in the transactions to the server. It seems to be taking about 30 seconds longer than before and is consistent on every transaction. In thinking through the change in architecture, you would not expect that the F5 platform introduced a 30 delay with each connection. The time it takes for a DNS query to timeout in many systems is around 30 seconds. On a deeper look into the logs on the server, it was doing a DNS reverse lookup and it was timing out. The firewall admin had not added the new network to the DNS rule on the firewall rule set to allow the network nodes to query their DNS servers.

3.02 - Explain how to get performance statistics in addition to the those shown in the dashboard (Overview - Performance)

GUI Study in the vLabs

To see additional platform performance information, use the following steps:

In version 11.x of the BIG-IP Configuration Utility:

1. Click Statistics.
2. Click Performance.

In version 10.x of the BIG-IP Configuration Utility:

1. Click Overview.
2. Click Performance.

All categories are shown under the **All** tab or you can see the break outs of **System**, Connections, **Throughput** and **Cache**.

SECTION 4 – TROUBLESHOOT BASIC DEVICE MANAGEMENT CONNECTIVITY ISSUES

Objective - 4.01 Verify remote connectivity to the box in order to determine the cause of a management connectivity issue

4.01 - Isolate potential causes of basic network connectivity issues, given scenarios related to: client configuration, client network access, device network access, and network topologies

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

A general knowledge of how devices communicate on IP based networks and basic configuration settings that are necessary on the client as well as the server environments are critical to being able to support an ADN environment. An understanding of how networks are designed and where devices are connected in a network topology are also critical to supporting an ADN environment.

4.01 - Apply connectivity troubleshooting tools (i.e. ping, traceroute, http/https availability, remote shell access, network based console access) in the appropriate situation

General Network Study and vLabs Practice

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Understanding of each of these tools functions and when you should use them to do troubleshooting of issues is key to administration of any network. An understanding of ways to connect to systems via console to test connectivity from the remote device on the network is critical as well.

Ping

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response.

Traceroute

Traceroute is a computer network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an Internet Protocol (IP) network. The history of the route is recorded as the round-trip times of the packets received from each successive host (remote node) in the route (path); the sum of the mean times in each hop indicates the total time spent to establish the connection. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Traceroute sends a sequence of three Internet Control Message Protocol (ICMP) Echo Request packets addressed to a destination host.

Objective - 4.02 Check and interpret port lockdown settings in order to determine the cause of a management connectivity issue

4.02 - Given a scenario, review port lockdown settings on the Self-IP to determine the cause of the issue

Overview of port lockdown behavior

Port lockdown is a BIG-IP security feature that allows you to specify particular protocols and services from which the self-IP address defined on the BIG-IP system can accept traffic.

The port lockdown feature allows you to secure the BIG-IP system from unwanted connection attempts by controlling the level of access to each self-IP address defined on the system. Each port lockdown list setting specifies the protocols and services from which a self-IP can accept connections. The system refuses traffic and connections made to a service or protocol port that is not on the list.

Port lockdown setting definitions:

Allow Default

This option allows access for a pre-defined set of network protocols and services that are typically required in a BIG-IP deployment.

The Allow Default setting specifies that connections to the self-IP addresses are allowed from the following protocols and services:

Allowed protocol	Service	Service definition
OSPF	N/A	N/A
TCP	4353	iQuery
UDP	4353	iQuery
TCP	443	HTTPS
TCP	161	SNMP
UDP	161	SNMP
TCP	22	SSH
TCP	53	DNS
UDP	53	DNS
UDP	520	RIP
UDP	1026	network failover

You can also determine the default supported protocols and services using the following command:

```
tmsh list net self-allow
```

The output will appear similar to the following example:

```
net self-allow {
        defaults {
                ospf:any
                tcp:domain
                tcp:f5query
                tcp:https
                tcp:snmp
                tcp:ssh
                udp:520
                udp:cap
                udp:domain
                udp:f5-iquery
                udp:snmp
        }
}
```

Allow All

This option specifies that all connections to the self-IP address are allowed, regardless of protocol or service.

Allow None

This option specifies that no connections are allowed on the self IP address, regardless of protocol or service. However, ICMP traffic is always allowed, and if the BIG-IP systems are configured in a redundant pair, ports that are listed as exceptions are always allowed from the peer system.

Allow Custom

This option allows you to specify the protocols and services for which connections are allowed on the self-IP address. However, ICMP traffic is always allowed, and if the BIG-IP systems are configured in a redundant pair, ports that are listed as exceptions are always allowed from the peer system.

Important: A known issue prevents connections to the state mirroring address when port tcp:1028 is explicitly allowed in the custom port lockdown list. For more information, refer to SOL12932: The BIG-IP system resets statemirror connections when port 1028 is configured in the Self IP Port Lockdown list.

Default port lockdown setting

When creating a self-IP address, the default port lockdown setting in BIG-IP 10.x is Allow Default. In BIG-IP 11.x, the default port lockdown setting is None.

Modifying port lockdown settings for a specific self IP using the Configuration utility

1. Log in to the Configuration utility.
2. Click Network.
3. Click Self-IPs.
4. Click the relevant self-IP address.
5. Select the desired setting from the Port Lockdown box.
6. Click Update.

Modifying port lockdown settings using the tmsh utility

1. Log in to the Traffic Management Shell (tmsh) by entering the following command:
   `tmsh`

   Note: If you are currently logged in to the tmsh shell, you can skip this step.

2. To modify the port lockdown settings for a self IP address, use the following command:
   `syntax:modify /net self <self_ip> allow-service <option>`

   For example, to change the port lockdown setting for self IP address 10.10.10.1 to default, you would type the following command:
   `modify /net self 10.10.10.1 allow-service default`

3. Save the change by typing the following command:

   - BIG-IP 10.1.0 and later:save sys config
   - BIG-IP 10.0.x:save config

4.02 - Describe appropriate use cases for the use of port lockdown

Overview of port lockdown behavior

For optimal security, F5 recommends using the port lockdown feature to allow only the protocols or services required for a self-IP address.

If you are managing the BIG-IP platform from one of the Self-IP addresses rather than using the out of band management interface, you run the risk of users having access to the Self-IP address on a port that will allow administration of the BIG-IP platform. All external facing Self-IP addresses should be restricted to only necessary ports for the BIG-IP platform to communicate to other necessary BIG-IP platforms or other necessary network functions such as DNS servers, etc.

Objective - 4.03 Check and interpret packet filters in order to determine the cause of a management connectivity issue

4.03 - Determine whether a filter is enabled

Packet filters enhance network security by specifying whether a BIG-IP system interface should accept or reject certain packets based on criteria that you specify. Packet filters enforce an access policy on incoming traffic. They apply to incoming traffic only.

You implement packet filtering by creating packet filter rules, using the BIG-IP Configuration utility. The primary purpose of a packet filter rule is to define the criteria that you want the BIG-IP system to use when filtering packets.

Examples of criteria that you can specify in a packet filter rule are:

- The source IP address of a packet
- The destination IP address of a packet
- The destination port of a packet

You specify the criteria for applying packet filter rules within an expression. When creating a packet filter rule, you can instruct the BIG-IP system to build an expression for you, in which case you need only choose the criteria from predefined lists, or you can write your own expression text, using the syntax of the tcpdump utility. For more information on the tcpdump utility, see the online man page for the tcpdump command.

Note: Packet filter rules are unrelated to iRules.

You can also configure global packet filtering that applies to all packet filter rules that you create. The following sections describe how to use the Configuration utility to set global packet filtering options, as well as create and manage individual packet filters rules.

To configure and manage packet filtering, log in to the BIG-IP Configuration utility, and on the Main tab, expand Network, and click Packet Filters.

Packet filter enabling

Before you can implement packet filtering on the BIG-IP system, you must enable the packet filter feature. You do this by changing the Packet Filtering setting to Enabled. The default setting for packet filtering is disabled.

4.03 - Interpret a packet filter rule list in a given situation

GUI Study in the vLabs

Packet filter rules

Packet filter rules are criteria statements that the BIG-IP system uses for filtering packets. The BIG-IP system attempts to match packet filter rules with an incoming packet, and if a match exists, determines whether or not to accept or reject the packet.

When you create a packet filter rule, you configure several settings, and then define the criteria that you want the BIG-IP system to use to filter the traffic.

Configuring settings for packet filter rules

You can configure a number of different settings when you create a packet filter rule. Specifying a name.

Order of packet filter rules

You use the Order setting to specify the order in which you want the BIG-IP system to apply existing packet filter rules. This setting is required.

Possible values for this setting are:

First

Select this value if you want this packet filter rule to be the first rule that the BIG-IP system applies.

Last

Select this value if you want this packet filter rule to be the last rule that the BIG-IP system applies.

After

Select this value, and then select a packet filter rule from the list, if you want the system to apply this packet filter after the packet filter that you select from the list. Note that this setting is most useful when you have more than three packet filter rules configured.

Action

When a packet matches the criteria that you have specified in a packet filter rule, the BIG-IP system can take a specific action. You define this action using the Action setting.

You can choose one of these actions:

Accept

Select Accept if you want the system to accept the packet, and stop processing additional packet filter rules, if any exist. This is the default setting.

Discard

Select Discard if you want the system to drop the packet, and stop processing additional packet filter rules, if any exist.

Reject

Select Reject if you want the system to drop the packet, and also send a rejection packet to the sender, indicating that the packet was refused. Note that the behavior of the system when you select the Reject action depends on how you configured the general packet filter Options property Send ICMP Error on Packet Reject.

Continue

Select Continue if you simply want the system to acknowledge the packet for logging or statistical purposes. Setting the Action value to Continue does not affect the way that the BIG-IP system handles the packet; the system continues to evaluate traffic matching a rule, starting with the next packet filter rule in the list.

Rate class assignment

Using the Rate Class setting, you can assign a rate class to traffic that matches the criteria defined in a packet filter rule. Note that this setting applies only when you have the rate-shaping feature enabled.

The default value for this setting is None. If you previously created rate classes using the rate-shaping feature, you can choose one of those rate classes from the Rate Class list.

One or more VLANs

You use the Apply to VLAN setting to display a list of VLANs and then select a VLAN or VLAN group name. Selecting a VLAN from the list means that the packet filter rule filters ingress traffic from that VLAN only. For example, if you select the value *All VLANS, the BIG-IP system applies the packet filter rule to all traffic coming into the BIG-IP system.

Similarly, if you select the VLAN internal, the BIG-IP system applies the packet filter rule to traffic from VLAN internal only. The default value is *All VLANS.

If you select the name of a VLAN group instead of an individual VLAN, the packet filter rule applies to all VLANs in that VLAN group.

Logging

If you want to generate a log message each time a packet matches a rule, you can enable logging for the packet filter rule. With this configuration, you can then display the Logging screen in the Configuration utility and view events related to packet filtering.

Creating a filter expression

To match incoming packets, the BIG-IP system must use a filter expression. A filter expression specifies the criteria that you want the BIG-IP system to use when filtering packets. For example, the BIG-IP system can filter packets based on the source or destination IP address in the header of a packet.

Using the Configuration utility, you can create a filter expression in either of two ways:

You can write your own expression, using a Filter Expression box.

You can specify a set of criteria (such as source or destination IP addresses) that you want the BIG-IP system to use when filtering packets. When you use this method, the BIG-IP system builds a filter expression for you.

You can have as many rules as you want, limited only by the available memory. Of course, the more statements you have, the more challenging it is to understand and maintain your packet filters.

Objective - 4.04 Given the use of a remote authentication server, verify proper DNS settings in order to diagnose a connectivity issue

Remote Server Authentication

Remote Authentication Intro:

A significant feature of BIG-IP Local Traffic Manager is its ability to support Pluggable Authentication Module (PAM) technology. PAM technology allows you to choose from a number of different authentication and authorization schemes to use to authenticate or authorize network traffic.

The goal of PAM technology is to separate an application, such as the BIG-IP system, from its underlying authentication technology. This means that you can dictate the particular authentication/authorization technology that you want the BIG-IP system to use to authenticate application traffic coming into the BIG-IP system.

To this end, Local Traffic Manager offers several authentication schemes, known as authentication modules. These authentication modules allow you to use a remote system to authenticate or authorize application requests that pass through the BIG-IP system.

> **Note:** The BIG-IP system normally routes remote authentication traffic through a Traffic Management Microkernel (TMM) switch interface (that is, an interface associated with a VLAN and a self-IP address), rather than through the management interface. Therefore, if the TMM service has been stopped for any reason, remote authentication is not available until the service is running again.

To configure and manage authentication profiles, log in to the BIG-IP Configuration utility, and on the Main tab, expand Local Traffic, and click Authentication.

BIG-IP system authentication modules

Local Traffic Manager authentication modules that you can implement for remote authentication are:

Lightweight Directory Access Protocol (LDAP)

Local Traffic Manager can authenticate or authorize network traffic using data stored on a remote LDAP server or a Microsoft® Windows® Active Directory® server. Client credentials are based on basic HTTP authentication (user name and password).

Remote Authentication Dial-In User Service (RADIUS)

Local Traffic Manager can authenticate network traffic using data stored on a remote RADIUS server. Client credentials are based on basic HTTP authentication (user name and password).

TACACS+

Local Traffic Manager can authenticate network traffic using data stored on a remote TACACS+ server. Client credentials are based on basic HTTP authentication (user name and password).

SSL client certificate LDAP

Local Traffic Manager can authorize network traffic using data stored on a remote LDAP server. Client credentials are based on SSL certificates, as well as defined user groups and roles.

Online Certificate Status Protocol (OCSP)

Local Traffic Manager can check on the revocation status of a client certificate using data stored on a remote OCSP server. Client credentials are based on SSL certificates.

Certificate Revocation List Distribution Point (CRLDP)

Local Traffic Manager can use CRL distribution points to determine revocation status.

Kerberos Delegation

Local Traffic Manager can authenticate application traffic when you are using Microsoft® Windows® Integrated Authentication.

4.04 - Given a suspected DNS issue, use appropriate tools to verify proper settings

GUI Study in the vLabs

Configuring the BIG-IP system to resolve DNS hostnames (11.x)

For the BIG-IP platform to connect to a node by name or to get to any system for any reason by the server's DNS name, a DNS server must be configured on BIG-IP's settings. The BIG-IP system uses two sources of information to resolve host names: the hosts file and DNS. The BIG-IP system first refers to the local /etc/hosts file. If the host name is not found in the /etc/hosts file, the BIG-IP system uses DNS if configured to do so. The following procedures help you configure the BIG-IP system to use DNS.

Using the BIG-IP Configuration utility is the preferred method of configuring a DNS remote lookup server.

Impact of procedure: Performing the following procedure should not have a negative impact on your system.

3. Log in to the BIG-IP Configuration utility.
4. Click System.
5. Click Configuration.
6. Click Device.
7. Click DNS.
8. In the DNS Lookup Server List section, type the IP address of your remote DNS lookup server.
9. Click Add.
10. Complete the change by clicking Update.

This same procedure can be used to modify the BIND Forwarder Server List or DNS Search Domain List. If this setting is not configured then resolving a DNS name from the BIG-IP platform will fail, including resolving the name of the remote authentication server for remote authentication.

4.04 - Given a suspected DNS issue, use appropriate tools to verify DNS response

GUI Study in the vLabs

If the DNS issue is related to the BIG-IP platform connecting to a DNS name you can check to make sure that the system is able to resolve names. From the command prompt you can do a NSLOOKUP of a server name, or you can DIG the server name. Both of these tools are found on the BIG-IP platform.

nslookup example:

```
nslookup www.stonegreyband.com
```

Server: `192.168.69.1`

Address: `192.168.69.1#53`

Non-authoritative answer:

```
www.stonegreyband.com  canonical name = stonegreyband.com.
```

Name: `stonegreyband.com`

Address: `71.251.96.82`

Dig Example:

```
dig www.stonegreyband.com

; <<>> DiG 9.8.3-P1 <<>> www.stonegreyband.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24965

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:

;www.stonegreyband.com.    IN   A

;; ANSWER SECTION:

www.stonegreyband.com.    3495   IN   CNAME stonegreyband.com.

stonegreyband.com.    495   IN   A   71.251.96.82

;; Query time: 4 msec

;; SERVER: 192.168.69.1#53(192.168.69.1)

;; WHEN: Thu Jan 9 22:41:06 2014

;; MSG SIZE rcvd: 69
```

SECTION 5 – OPEN A SUPPORT TICKET WITH F5

Objective - 5.01 Identify the appropriate supporting components and severity levels for an F5 support ticket

5.01 - Identify the necessary components for all support cases (Qkview uploaded to iHealth/ or attached to case, serial number of device, problem description, other supporting data)

Information required when opening a support case for BIG-IP LTM, AFM, GTM, Link Controller, and PEM

F5 Technical Support can help resolve issues more quickly when you provide a full description of the issue and the details of your configuration. To help you gather all the required information, use the following guidelines to prepare for opening a case:

General Information

Provide the following information when you open a case with F5 Technical Support:

1. A full description of the issue, including the following details:
    - The symptoms of the issue
    - The approximate time the issue first occurred
    - The number of times the issue has recurred
    - Any error output provided by the system
    - Steps to reproduce the issue
    - Any changes you made to the system before the issue first occurred
    - Any steps you have attempted to resolve the issue
2. A description of the impact the issue is having on your site, using the following definitions:
    - Site Down - All network traffic has ceased, causing a critical impact to your business.
    - Site at Risk - Primary unit has failed resulting in no redundancy. Site is at risk of going down.

- Performance Degraded - Network traffic is partially functional causing some applications to be unreachable.

3. The hours that you are available to work on the issue and any alternative contacts that can work on the issue if you are not available.
4. Remote access information, if possible.

    - Remote access to your network environment is important, because it is the most effective method for collecting information and troubleshooting technical issues. If you cannot provide remote access, F5 Technical Support will work directly with you to resolve the issue over the phone; however, this method can often be more time consuming and may require file transfers, replication, and additional testing.

Collect the following information from the affected systems and provide the information when you open the case.

qkview or "tech.out" file

The qkview utility is a BIG-IP program that an administrator can use to automatically collect configuration and diagnostic information from BIG-IP and Enterprise Manager systems.

Starting in BIG-IP 10.0.0, the qkview utility is an executable program that generates machine-readable (XML) diagnostic data from the BIG-IP or Enterprise Manager system and combines the data into a single compressed tar file. The diagnostic file can then be uploaded to BIG-IP iHealth, or given to F5 Technical Support to aid in troubleshooting.

Note: If you are running BIG-IP version 10.x or later, you can use BIG-IP iHealth to diagnose a qkview file. BIG-IP iHealth diagnoses the health and proper operation of your BIG-IP system when you upload the qkview file to the BIG-IP iHealth website. For more information, refer to the BIG-IP iHealth website.

Log files

Note: The qkview utility automatically gathers 5MB of log files and includes them with qkview in a .tar output.

If the systems logs are heavy and more of the logs are needed, provide all the log files on the system by performing the following procedure:

Log in to the command line.

Create a tar archive named `logfiles.tar.gz` in the `/var/tmp` directory which contains all the files in the `/var/log` directory, by typing the following command:

```
tar -czpf /var/tmp/logfiles.tar.gz /var/log/*
```

Packet traces

If the issue involves the network, perform a packet trace while the issue is occurring and provide the packet trace when you open the case.

Note: For more information about performing packet traces with tcpdump, refer to SOL4714: Performing a packet trace and providing the results to F5 Technical Support.

UCS archive

If you cannot give F5 Technical Support remote access to your system, you may need to provide a UCS archive of the current configuration. For more information, refer to SOL4423: Overview of UCS archives.

Core files

Core files contain the contents of the system memory at the time a crash occurred. If the system has been configured to save core files, they will be located in the /var/savecore directory (BIG-IP versions 9.0 through 9.2.5) or `/var/core` directory (BIG-IP versions 9.3 and later). Provide any existing core files when you open the case.

Note: For information about requirements when submitting core files to F5, refer to SOL10062: Submitting core files for analysis to F5 Technical Support.

5.01 - Identify severity levels and the associated response times

Guidelines and Policies

All F5 Network Support Centers uphold the following case severity definitions and target response times to ensure that the appropriate resources are used to resolve all technical issues as efficiently as possible. F5 will endeavor to respond to Severity 1 and Severity 2 issues within one hour. Understanding that unforeseen events could delay attempts, F5 expects that the majority of Severity 1 and Severity 2 issues will be responded to within this service level. Initial response is defined as the time from when the F5 case was created to when a Network Support Engineer first attempts to contact the case contact for troubleshooting and updates the case log reflecting this action.

Severity 1

1-hour response - Software or hardware conditions on your F5 device are preventing the execution of critical business activities. The device will not power up or is not passing traffic.

Severity 2

1-hour response - Software or hardware conditions on your F5 device are preventing or significantly impairing high-level commerce or business activities.

Severity 3

4-business hour response - Software or hardware conditions on your F5 device are creating degradation of service or functionality in normal business or commerce activities.

Severity 4

24-hour response - Questions regarding configurations (“how to”), troubleshooting non-critical issues, or requests for product functionality that is not part of the current product feature set.

When a case is logged as Severity 1, F5 Network Support Managers are immediately notified to ensure the case is assigned within the appropriate timeframe to an appropriately skilled Network Support Engineer.

Objective - 5.02 Given an issue, determine the appropriate severity

Guidelines and Policies

Severity 1

Software or hardware conditions on your F5 device are preventing the execution of critical business activities. The device will not power up or is not passing traffic.

Severity 2

Software or hardware conditions on your F5 device are preventing or significantly impairing high-level commerce or business activities.

Severity 3

Software or hardware conditions on your F5 device are creating degradation of service or functionality in normal business or commerce activities.

Severity 4

Questions regarding configurations (“how to”), troubleshooting non-critical issues, or requests for product functionality that is not part of the current product feature set.

Objective - 5.03 Provide quantitative and relevant information appropriate for a given issue

5.03 - Distinguish between qualitative/quantitative statements in order to assemble an accurate problem description

General Network Study

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Quantitative observations are observations that can be precisely measured. (i.e. There is taking an additional 20 seconds per connection over the connection times this morning.)

Qualitative observations have more to do with characteristics of what is being observed. (i.e. It seems to be taking longer to connect than it did this morning.)

5.03 - Distinguish between relevant/irrelevant information in order to assemble an accurate problem description

General Network Study

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Is the information that you are gathering relative to the issue you are experiencing? Troubleshooting can lead to many rat holes where you can get lost from the real issues.

Objective - 5.04 Given a scenario, determine the proper F5 escalation method

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Evaluate your current network state and understand the Severity levels in section 5.02 to understand at what level your issue should be categorized. Realize that even though you have an issue with your environment not all issues are a Severity 1 issue. Be realistic with your assessment and be ready to categorize issues on the exam.

SECTION 6 – IDENTIFY AND REPORT CURRENT DEVICE STATUS

Objective - 6.01 Review the network map in order to determine the status of objects on the box

6.01 - Explain the status icons of objects on the map

Introducing BIG-IP Local Traffic Manager

The Configuration utility includes a feature known as the network map. The network map shows a summary of local traffic objects, as well as a visual map of the virtual servers, pools, and pool members on the BIG-IP system. For both the local traffic summary and the network map, you can customize the display using a search mechanism that filters the information that you want to display, according to criteria that you specify. The system highlights in blue all matches from a search operation.

Object summary

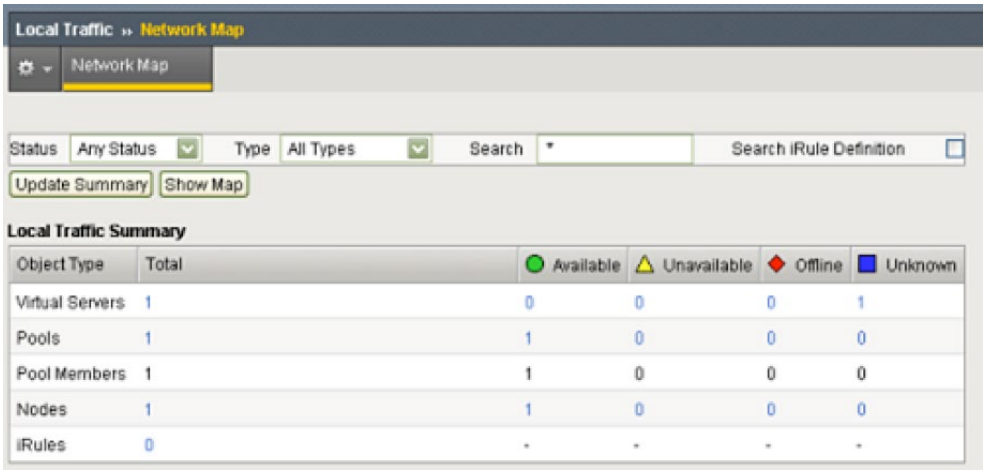
When you first open the Network Map screen, the screen displays a summary of local traffic objects. This summary includes the type of objects specified with the search mechanism, the number of each type of object, and, for each object type, the number of objects with a given status.

The summary displays data for these object types:

- Virtual servers
- Pools
- Pool members
- Nodes
- iRules

Note: A local traffic summary includes only those objects that are referenced by a virtual server. For example, if you have configured a pool on the system but there is no virtual server that references that pool, the local traffic summary does not include that pool, its members, or the associated nodes in the summary.

The diagram below shows an example of a network map screen that summarizes local traffic objects on the system.



For each object type listed in the summary, the system shows the number of objects with each type of status. Table 1.3 shows the various status indicators that the summary screen can display for a local traffic object.

Table 1.3 Explanation of status icons in a local traffic summary

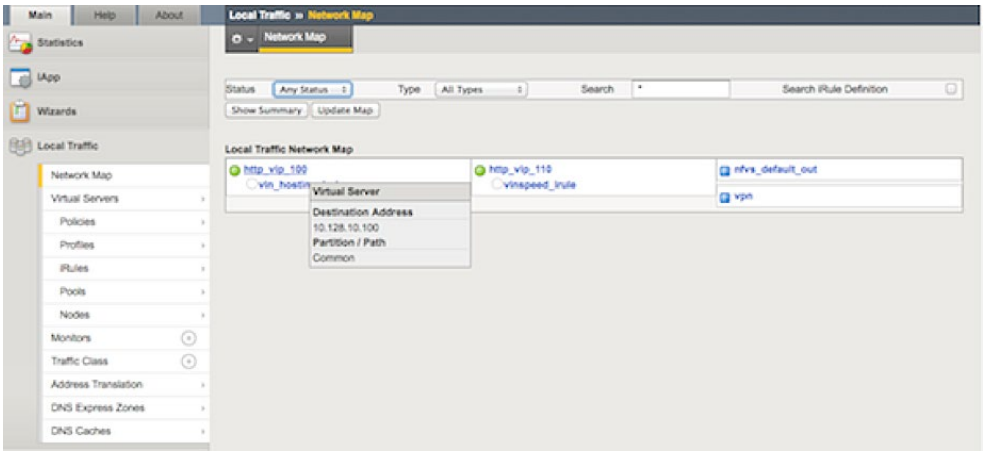
Status indicator	Explanation
	The objects are enabled and available (able to receive traffic).
	The objects are enabled but are currently unavailable. However, the objects might become available later, with no user action required. An example of an object showing this status is a virtual server whose connection limit has been exceeded. When the number of connections falls below the configured limit, the virtual server becomes available again.
	The objects are enabled but offline because an associated object has marked the object as unavailable. To change the status so that the object can receive traffic, you must actively enable the object.
	The status of the objects is unknown.

The network map display

The network map presents a visual hierarchy of the names and status of virtual servers, pools, pool members, nodes, and iRules defined on the system. The map shows all objects in context, starting with the virtual servers at the top. The Status, Type, and Search settings at the top of the screen determine the objects that the map includes.

When you position the cursor over an object on the map, the system presents hover text containing information about the object. When you position the cursor over the status icon accompanying an object, the system presents hover text containing information about the object's status, text which also appears on the pool's Properties screen. The system arranges objects in alphabetic order, and organizes the dependent objects in a hierarchy. Due to the way that a network map presents objects in context, the updated screen also shows objects of other statuses, types, and names that relate to those objects. This is because a network map always shows objects in context with the objects that depend on them, and the objects they depend on.

For example, if you have an available virtual server with an available pool and two pool members, one available and one offline, then selecting Offline from the Status list causes the system to show the offline pool member in context with the available virtual server and the available pool. This is because the available virtual server and the available pool depend on the offline pool member.



6.01 - Explain what virtual servers, pools, nodes and pool members are

Virtual Servers

Virtual Server

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. For example, a virtual server can enable compression on HTTP request data as it passes through the BIG-IP system, or decrypt and re-encrypt SSL connections and verify SSL certificates. For each type of traffic, such as TCP, UDP, HTTP, SSL, SIP, and FTP, a virtual server can apply an entire group of settings, to affect the way that Local Traffic Manager manages that traffic type.

A virtual server can also enable session persistence for a specific traffic type. Through a virtual server, you can set up session persistence for HTTP, SSL, SIP, and MSRDP sessions, to name a few.

Finally, a virtual server can apply an iRule, which is a user-written script designed to inspect and direct individual connections in specific ways. For example, you can create an iRule that searches the content of a TCP connection for a specific string and, if found, directs the virtual server to send the connection to a specific pool or pool member.

To summarize, a virtual server can do 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

Pools

Pool and Pool Members

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.

When you create a pool, you assign pool members to the pool. A pool member is a logical object that represents a physical node (server), on the network. You then associate the pool with a virtual server on the BIG-IP system. Once you have assigned a pool to a virtual server, Local Traffic Manager directs traffic coming into the virtual server to a member of that pool. An individual pool member can belong to one or multiple pools, depending on how you want to manage your network traffic.

The specific pool member that the Local Traffic Manager chooses to send the request to is determined by the load balancing method that you have assigned to the pool. A load balancing method is an algorithm that Local Traffic Manager uses to select a pool member for processing a request. For example, the default load balancing method is Round Robin, which causes Local Traffic Manager to send each incoming request to the next available member of the pool, thereby distributing requests evenly across the servers in the pool.

To configure and manage pools, log in to the BIG-IP Configuration utility, and on the Main tab, expand Local Traffic, and click Pools.

Nodes

Nodes

A node is a logical object on the BIG-IP Local Traffic Manager system that identifies the IP address of a physical resource on the network. You can explicitly create a node, or you can instruct Local Traffic Manager to automatically create one when you add a pool member to a load balancing pool.

The difference between a node and a pool member is that a node is designated by the devices IP address only (`10.10.10.10`), while designation of a pool member includes an IP address and a service (such as `10.10.10:80`).

A primary feature of nodes is their association with health monitors. Like pool members, nodes can be associated with health monitors as a way to determine server status. However, a health monitor for a pool member reports the status of a service running on the device, whereas a health monitor associated with a node reports status of the device itself.

For example, if an ICMP health monitor is associated with node `10.10.10.10`, which corresponds to pool member `10.10.10.10:80`, and the monitor reports the node as being in a down state, then the monitor also reports the pool member as being down. Conversely, if the monitor reports the node as being in an up state, then the monitor reports the pool member as being either up or down, depending on the status of the service running on it.

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, that is, designate that server as a node. After designating the server as node, you can add the node to a pool as a pool member. You can also associate a health monitor with the node, to report the status of that server.

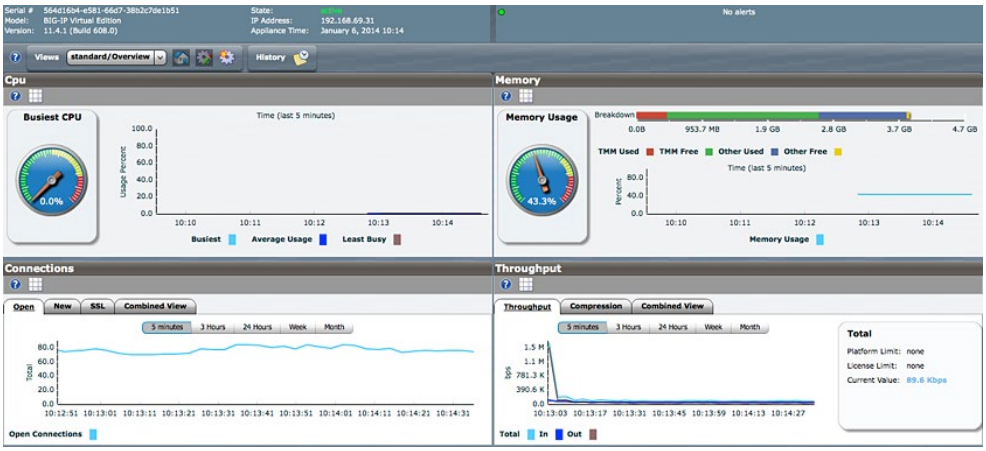
To configure and manage nodes, log in to the BIG-IP Configuration utility, and on the Main tab, expand Local Traffic, and click Nodes.

Objective - 6.02 Use the dashboard to gauge the current running status of the system

6.02 - Interpret each of the statistic types displayed by the dashboard

GUI Study in the vLabs

The main Dashboard screen is of the system overview. This screen displays a graphical representation of CPU utilization, Memory utilization, Connections and Throughput of the system.



6.02 - Given a situation, predict the appropriate dashboard statistics

GUI Study in the vLabs

Understand what situations and which configurations will affect the different areas of the Dashboard statistics. For example, the more features that are provisioned on the BIG-IP platform the higher the base Memory utilization will be. Also, if ASM is running on the BIG-IP the CPU utilization my get higher as additional policies are added to the configuration under load.

Objective - 6.03 Review log files in order to gauge the current operational status of the device

6.03 - Given log file snippets, describe an event sequence

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Get familiar with looking at the event logs on the BIG-IP and learn to reconstruct what has happened recently based on the events in the logs.

6.03 - Given log file snippets, identify critical events

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Get familiar with looking at the event logs on the BIG-IP and be able to identify critical events. This may be hard to do in the lab unless you are cresting your own system errors. Possible do the opposite and get used to seeing what is there when all is good and then the errors will stand out.

Objective - 6.04 Use iApps Analytics to gauge the current running status of application services

6.04 - Explain the purpose of iApps Analytics

What is Analytics?

Analytics (also called Application Visibility and Reporting) is a module on the BIG-IP® system that lets you analyze performance of web applications. It provides detailed metrics such as transactions per second, server and client latency, request and response throughput, and sessions. You can view metrics for applications, virtual servers, pool members, URLs, specific countries, and additional detailed statistics about application traffic running through the BIG-IP system.

Transaction counters for response codes, user agents, HTTP methods, countries, and IP addresses provide statistical analysis of the traffic that is going through the system. You can capture traffic for examination and have the system send alerts so you can troubleshoot problems and immediately react to sudden changes.

The Analytics module also provides remote logging capabilities so that your company can consolidate statistics gathered from multiple BIG-IP appliances onto syslog servers or SIEM devices, such as Splunk.

About Analytics profiles

An Analytics profile is a set of definitions that determines the circumstances under which the system gathers, logs, notifies, and graphically displays information regarding traffic to an application. The Analytics module requires that you select an Analytics profile for each application you want to monitor. You associate the

Analytics profile with one or more virtual servers used by the application, or with an iApps™ application service. Each virtual server can have only one Analytics profile associated with it.

In the Analytics profile, you customize:

- What statistics to collect
- Where to collect data (locally, remotely, or both)
- Whether to capture the traffic itself
- Whether to send notifications

The BIG-IP® system includes a default Analytics profile called analytics. It is a minimal profile that internally logs application statistics for server latency, throughput, response codes, and methods. You can create custom Analytics profiles for each application if you want to track different data for each one.

Charts shown in the Overview > Statistics > Analytics screen display the application data saved for all Analytics profiles associated with iApps application services or virtual servers on the system. You can filter the information, for example, by application or URL. You can also drill down into the specifics on the charts, and click the tabs to further refine the information in the charts.

Overview: Setting up application statistics collection

This implementation describes how to set up the BIG-IP system to collect application performance statistics. The system can collect application statistics locally, remotely, or both. You use these statistics for troubleshooting and improving application performance.

You can collect application statistics for one or more virtual servers or for an iApps application service. If virtual servers are already configured, you can specify them when setting up statistics collection. If you want to collect statistics for an iApps application service, you should first set up statistics collection, creating an Analytics profile, and then create the application service.

The system can send alerts regarding the statistics when thresholds are exceeded, and when they cross back into the normal range. You can customize the threshold values for transactions per second, latency, page load time, and throughput.

6.04 - Describe how to capture application statistics

You can examine the statistics on the Analytics charts when Application Visibility and Reporting (AVR) is provisioned. The system recalculates the Analytics statistics and updates the charts every five minutes.

Before you can look at the application statistics, you need to have created an Analytics profile so that the system is capturing the application statistics internally on the BIG-IP® system. You must associate the Analytics profile with one or more virtual servers (in the Analytics profile or in the virtual server). If you created an iApp application service, the template provided allows you to associate the virtual server. To view Analytics statistics properly, Adobe Flash Player must be installed on the computer where you plan to view them.

6.04 - Given a current running status, recognize significant statistics

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

Get familiar with looking at the status information in Statistics – Module Statistics – Local Traffic under the different Statistics Types drop menu on the BIG-IP and be able to identify significant statistic levels. This may be hard to do in the lab unless you are pushing load through the unit. Get used to how the reports look and how to read them.

SECTION 7 – MAINTAIN SYSTEM CONFIGURATION

Objective - 7.01 Create and restore a UCS archive under the appropriate circumstances

7.01 - Discuss scenarios in which restoring a UCS archive is appropriate

Once you have created the configuration data for the BIG-IP system, you can replicate all of this set of data in a separate file. You can then use this replicated data later, for these reasons:

As an archive for disaster recovery

Using the Archives feature, you can back up the current configuration data, and if necessary, restore the data at a later time. We highly recommend that you use this feature to mitigate the potential loss of BIG-IP system configuration data. To create an archive, you can use the Configuration utility, which stores the configuration data in a special file known as a user configuration set, or UCS file. You can then use the UCS file to recover from any loss of data, in the unlikely event that you need to do so.

7.01 - Discuss the tasks involved in successfully restoring a UCS archive

Restoring configuration data by using the Configuration utility

There are a few different ways to do a UCS restore on a BIG-IP platform.

Restoring configuration data by using the Configuration utility

Impact of procedure: The BIG-IP system replaces any existing configuration with the UCS archive file configuration.

If you are restoring a UCS archive on a BIG-IP 6400, 6800, 8400, or 8800 hardware platform other than the system from which the backup was created, such as when replacing an RMA system, you must perform the procedure in the “Restoring configuration data from the command line by using the tmsh utility” section of this article to restore the configuration.

To restore a configuration in a UCS archive by using the Configuration utility, review the considerations described in the Considerations for restoring configuration data section of this article before performing the following procedure:

1. Log in to the Configuration utility.
2. Click System.
3. Click Archives.
4. Click the name of the UCS archive you want to restore.
5. If the UCS archive is encrypted, type the passphrase for the encrypted UCS archive file in the Restore Passphrase field. If the UCS archive is not encrypted, you can skip this step.
6. To initiate the UCS archive restore process, click Restore.
7. When the restore process is completed, examine the status page for any reported errors before proceeding to the next step.
8. To return to the Archive List page, click OK.

If you restored the UCS archive on a different device and received the errors noted in the “Considerations for restoring configuration data” section of this article, you must reactivate the BIG-IP system license.

After relicensing the system, restart the system to ensure that the configuration is fully loaded. To restart the system, navigate to System > Configuration, and then click Reboot.

If the system you restored contains the FIPS 140 HSM, you must configure the FIPS 140 HSM Security World after completing steps 1 through 9. For additional information about recovering FIPS information after a system recovery, refer to the Configuring and Maintaining a FIPS Security Domain chapter in the Platform Guide: 6900 and 8900.

Restoring configuration data from the command line by using the tmsh utility

Impact of procedure: The BIG-IP system replaces any existing configuration with the UCS archive file configuration.

1. Log in to tmsh by typing the following command:
   `tmsh`
2. Restore the UCS archive file by using the following command syntax. Replace <path/to/UCS> with the full path of the UCS archive file you want to restore:
   `load /sys ucs <path/to/UCS>`

   If you do not specify the path, the BIG-IP system performs as if the UCS archive file is located in the default /var/local/ucs directory.
3. If the UCS archive file was encrypted with a passphrase during the backup, you are prompted to enter the passphrase for the archive file.
4. If you are running BIG-IP on a 6400, 6800, 8400, or 8800 hardware platform, type the following command to switch to the bash shell:
   `run /util bash`
5. Type the following command to verify that the new or replaced secure shell (SSH) keys from the UCS file are synchronized between the BIG-IP system and the Switch Card Control Processor (SCCP):
   `keyswap.sh sccp`
6. Type the following command to switch back to tmsh:
   `exit`
7. Restart the system by typing the following command:
   `reboot`

   If you installed the UCS archive on the same device on which the backup was created, it loads the restored configuration after the system restarts. If you restored the backup on a different device and received the first error noted in the Considerations for restoring configuration data section of this article, you must reactivate the BIG-IP system license. Alternatively, you can replace the /config/bigip.license file with the original bigip.license file that you backed up from the target system.

8. If the system you restored contains the FIPS 140 HSM, you must configure the FIPS 140 HSM Security World after completing steps 1 through 5. For additional information about recovering FIPS information after a system recovery, refer to the Configuring and Maintaining a FIPS Security Domain chapter in the Platform Guide: 6900 and 8900.

Restoring configuration data on a replacement RMA unit

F5 recommends that you use the following procedure when you restore the archive on a different device than the system on which the backup was created, such as an RMA system. If you do not use this procedure when restoring the archive on a different device, the configuration load may fail and the mcpd process generates an error message that appears similar to the following example to both stdout and the /var/log/ltm file:

```
mcpd[2395]: 01070608:0: License is not operational(expired or digital signature
does not match contents)
```

F5 expects this message, and you can correct the issue by re-licensing the system, which is discussed later in the procedure.

Impact of procedure: The BIG-IP system replaces any existing configuration with the UCS archive file configuration.

1. Activate the license on the unit according to the steps detailed in SOL7752: Overview of licensing the BIG-IP system.
2. Log in to tmsh by typing the following command:
   `tmsh`
3. Restore the UCS archive file by using the following command syntax. Replace <path/to/UCS> with the full path of the UCS archive file you want to restore:
   `load /sys ucs <path/to/UCS> no-license`

   If you do not specify the path, the BIG-IP system performs as if the UCS archive file is located in the default /var/local/ucs directory.
4. If the UCS archive file was encrypted with a passphrase during the backup, you are prompted to enter the passphrase for the archive file.
5. If you are running the BIG-IP system on a 6400, 6800, 8400, or 8800 hardware platform, switch to the bash utility by entering the following command:
   `run /util bash`
6. To verify that the new or replaced SSH keys from the UCS file are synchronized between the BIG-IP and the SCCP, enter the following command:
   `keyswap.sh sccp`

7. To switch back to tmsh, type the following command:
   `exit`

8. Restart the system by typing the following command:
   reboot

9. If the system you restored contains the FIPS 140 HSM, you must configure the FIPS 140 HSM Security World after completing steps 1 through 5. For additional information about recovering FIPS information after a system recovery, refer to the Configuring and Maintaining a FIPS Security Domain chapter in the Platform Guide: 6900 and 8900.

Restoring UCS archives on BIG-IP systems running later software versions

Impact of procedure: The BIG-IP system replaces any existing configuration with the UCS archive file configuration.

F5 recommends that the BIG-IP system run the same version of the BIG-IP software from which it was backed up. However, in some cases, it is possible to restore a UCS archive that was obtained from an earlier software version on a target BIG-IP system running a later software version. For example, if you saved a UCS archive on a system running BIG-IP 10.2.3, it is possible to restore the version BIG-IP 10.2.3 archive file on a BIG-IP system running 11.x. To restore a UCS archive on a BIG-IP system running a later software version, perform the following procedure:

1. Verify that a supported upgrade path exists between the software version from which the UCS archive was obtained and the software version running on the target system.

   For example, there is a supported upgrade path between BIG-IP 10.x and BIG-IP 11.x. As a result, you can successfully restore a BIG-IP 10.x UCS archive file on a BIG-IP system running 11.x. However, there is no supported upgrade path between BIG-IP 9.x and BIG-IP 11.x. As a result, you cannot restore a BIG-IP 9.x UCS archive file on a BIG-IP system running 11.x.

   For information about supported upgrade paths, refer to the product release notes for your specific software version.

2. Review the previous section, Considerations for restoring configuration data.

3. Manually copy the UCS archive file to the /var/local/ucs/ directory on the target system.

4. Restore the UCS archive on the BIG-IP system:

   - If you are restoring the archive on a different device than the system on which the backup was created, follow the “Restoring configuration data on a replacement RMA unit” procedure.

- If you are restoring the archive on a different device than the system on which the backup was created, follow the “Restoring configuration data from the command line by using the tmsh utility” procedure.

7.01 - Given a scenario, discuss when it is appropriate to create a UCS archive

GUI Study in the vLabs

Any time the system administrator makes changes to the configuration of the system a UCS archive should be taken prior to the change and after the change. This will allow for a restore to the point prior to the change and also provides a backup of the new current state. This should be done on both the Active and stand by systems in an HA pair.

Objective - 7.02 Identify the components and methods associated with automating and scheduling tasks with Enterprise Manager

7.02 - Identify which tasks can be automated using EM

Enterprise Manager Overview

You can select, stage, and automate common operational tasks, including:

- Configuration
- Certificate management
- Software updates
- Node management
- Policy control

7.02 - Identify which sub-tasks exist (i.e. install a hotfix but not reboot into the newly upgraded volume, etc.)

Managing Software Images

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

In an Enterprise Manager task, such as one that installs new software to a BIG-IP platform, there may be follow on tasks or Task Options necessary for the installation to be complete. A “sub-task” to a software install may be to reboot the system, found in the task options section.

7.02 - Outline EM’s method of creating automated UCS archives

Enterprise Manager Administrator Guide, version 1.0

Enterprise Manager saves UCS files to a UCS archive. You can create a task to save UCS archives for devices at regularly scheduled intervals. Archives that are created and saved on a schedule are called, rotating archives. When the system creates rotating archives, it compares the most recently stored UCS archive file to the current configuration on the device at the specified interval. If there are any differences, Enterprise Manager stores a copy of the current configuration in a UCS archive. If there are no differences, Enterprise Manager does not store an additional copy of the current configuration, which leaves you room to store a higher number of unique historical UCS archives. When Enterprise Manager reaches the maximum number of archives specified to store, it deletes the oldest archive in the rotating archive list. By default, Enterprise Manager stores up to 10 rotating archives each, for itself and every managed device.

Another option for archive storage is to create an archive of a specific UCS for a device, referred to as a pinning an archive. Enterprise Manager also creates a pinned archive of a device’s current configuration before it installs new software. Pinned archives are stored until you delete them.

Creating a rotating UCS archive schedule

A device must be listed on the Device List screen before you can create a rotating archive schedule for it.

It is best practice to create a rotating archive schedule for each device in your network so that you always have a copy of a recent configuration. The UCS archive provides your network with added stability in the event that a configuration change results in a need for a system restore. You can create a customized schedule for a specific device, or create several schedules and assign any number of devices to each schedule.

- On the Main tab, click Enterprise Management > Tasks > Schedules > Archive Collection. The Archive Collection screen opens.
- Click the Create button. The New Scheduled Task screen opens.
- In the Archive File Name field, type a name for the rotating archive schedule.
- From the Check for Changes list, select the frequency that you want Enterprise Manager to check for configuration changes. Depending on your selection, the screen refreshes to display associated options.
- Click Finished to save the settings.

The Archive Collection list screen opens and the new rotating archive schedule appears in the list. If a device in the Assigned list changes its configuration during the interval you specified, Enterprise Manager creates an archive of the device's configuration and adds it to the rotating archives on the Archives Collection screen.

7.02 - Describe EM's behavior when encountering task failures on specific devices

Enterprise Manager Administrator Guide, version 1.0

You see the failure in the Task List if a task fails.

You can configure custom alerts to notify you or others if a device becomes unreachable by Enterprise Manager, the completion or failure of a software or hotfix installation, and if a device system clock differs from the Enterprise Manager clock. When you configure custom alerts, you can apply them to individual devices, or to a device group. You can also create alerts for the Enterprise Management device itself so that you can maintain the health of your management system.

Objective - 7.03 Automate and schedule tasks using Enterprise Manager

7.03 - Discuss the strategy for deploying a hotfix from EM to multiple high availability (HA) pairs

You can use Enterprise Manager's software repository to store both software, and hotfix images. Once you add these images to the repository, you can deploy a hotfix or software upgrade to one device, or configure multiple device upgrades. Alternately, you can check which upgrades are compatible on a per device basis and install only the upgrades that suit your needs. In any software upgrade, you can choose multiple upgrade options, including the installation location and reboot location on each device.

Installing software to high availability systems

To minimize the risk when performing a installation to a system in a high availability configuration, we recommend that you configure only one device in the pair per upgrade task. For example, for an active-standby pair, instead of adding both the active and standby devices to the installation list when configuring the task, upgrade only the software on the standby device. Then, when the upgrade completes, you can switch the device to active mode to test whether the upgrade works properly. Once you confirm that the upgrade works as expected, you can configure a task to upgrade the second device of the pair.

> **Important:** If you include both the active and standby systems in the same upgrade task and the upgrade does not work properly on the first device of a high availability pair, you cannot cancel the upgrade on the second device.

7.03 - Discuss how EM can be used to track a configuration change on a managed device

Enterprise Manager can create and store UCS archives for managed devices on demand, or at regularly scheduled intervals using rotating archives. Rotating archives are UCS archives created at a regular interval according to a schedule that you set in Enterprise Manager.

The advantage of scheduling rotating archives is that you can set Enterprise Manager to create archives on a regular interval so that after Enterprise Manager recognizes that a managed device's configuration has changed, it schedules the creation of a UCS archive during the current rotating archive schedule. This way, you can have a recent backup configuration for a managed device, which provides added stability in case a configuration change results in a need for a system restore. For example, if you set up a daily rotating archive schedule, Enterprise Manager creates a UCS archive on each day that the managed device configuration changes. This ensures that you do not unnecessarily save any duplicate configuration archives, and that you always have one or more archives of recent configurations with which to restore. In a rotating archive schedule, Enterprise Manager saves multiple archives and cycles out old archives as it creates new ones.

So each time you see a new archive created for a device you know that changes have been made.

7.03 - Discuss how to use EM to determine SSL certification expiration on managed devices

Working with device certificates

Because the BIG-IP Local Traffic Manager (LTM) can control your SSL traffic, you may have a large number of SSL and web certificates on many different LTM devices your network.

Enterprise Manager can provide a quick overview of all the server certificates and web certificates on each managed device in the network. You can use Enterprise Manager to monitor which certificates are nearing their expiration date, and which ones have expired. Using this overview can save you time over monitoring certificate expiration dates on individual LTM devices.

Monitoring device certificates

When Enterprise Manager adds a device to the device list, you have the option to monitor the expiration status of all the certificates on the managed device. You can view the status of both traffic certificates and system certificates. Traffic certificates are server certificates that a managed device uses in its traffic management tasks. System certificates are the web certificates that allow client systems to log into the BIG-IP system Configuration utility.

Enabling certificate monitoring

By default, certificate monitoring is enabled for all managed devices, however, you may specify which specific device or device groups you want to monitor. If you choose to monitor a device group, you automatically monitor all of the certificates on all of the devices that are members of the device group.

Working with the certificate list screens

You can view either traffic certificates or system certificates on their own certificate list screens. These screens provide a quick overview of vital certificate information such as the expiration status, name, the device the certificate is configured on, the common name, and expiration date and time.

Status flags offer the quickest view on the status of a certificate. The table below outlines the status flags.

Table - Certificate status flags

Status indicator	Expiration Status
	The Red Status Flag indicates that the certificate has expired. When client systems require this certificate for authentication, the client receives an expired certificate warning.
	The Yellow Status Flag indicates that a certificate will expire in 30 days or less. The certificate is still valid, but you should take action to prevent certificate expiration.
	The Green Status Flag indicates that a certificate is valid and will remain valid for at least 30 more days.

When working with the certificate list screens, you can sort the list by clicking the respective column headings, or you can filter the list to display only certificates with a particular status flag. When working with the

certificate list screens, you can sort the list by clicking the respective column headings, or you can filter the list to display only certificates with a particular status flag.

Creating alerts for certificate expiration

If you require more precise notification of certificate expiration dates, you can create a custom alert. When you create a custom alert on the New Alert screen, in the Alert Type box, select Certificate Expiration. Once you select this type of alert, you can configure an alert based on the number of days until the certificate expires.

Objective - 7.04 Manage software images

7.04 - Given an HA pair, describe the appropriate strategy for deploying a new software image

The upgrade process involves preparation of the two BIG-IP® devices (Device A and Device B) configured in an active-standby implementation, followed by the installation and verification of version 11.0 on each device. When you upgrade each device, you perform several tasks. Completing these tasks results in a successful upgrade to version 11.0 on both BIG-IP devices, with a traffic group configured properly for an active-standby implementation.

In a properly configured HA pair of BIG-IP devices, a software upgrade should always be done on the standby unit in the pair. This allows the upgrade to be hitless to the extent of nothing greater than a failover between functioning units in the HA pair.

7.04 - Describe the potential impact of booting a device into another volume

GUI Study in the vLabs

Booting the BIG-IP platform into another volume may put the system in an inaccessible state if the circumstances are right. Just because there is an OS loaded onto a volume does not mean there is any configuration other than the default configuration on the volume. The out of band management may still be set to the default IP address and you could lose your management connection the unit. Or if this was a volume that was used in the past it will likely be in the state it was in when the system was booted into another volume. This could mean that it is running some older configuration that is not the same as the current configuration in the current volume, or the system could even be licensed differently leaving some functions of the OS not even enabled.

The **cpcfg** command allows you to copy a configuration from a specified source boot location to a specified target boot location. If the specified target boot location is an earlier version than the source boot location, the command fails with an error message. If the specified target boot location is the active boot location, the command fails with an error message.

7.04 - Discuss common issues related to the migration of a device to a new software version

Managing BIG-IP product hotfixes (11.x)

If the device you are migrating, to a new version of software, is not an HA pair. The upgrade will cause an outage so plan accordingly.

When dealing with an HA pair of devices, upgrades should be done on the units in the standby state to minimize outages. A hotfix to an existing software version is normally non-impactful to the operation of the unit, however it is still a best practice to upgrade the standby unit first, confirm the upgrade, failover the pair and proceed with upgrading the now standby unit.

Always follow the F5 Solutions or SOLs for installing the software.

Some common issues that can be impactful to an environment when doing software upgrades are know issues with the release, iRule compatibility with the newer version and older version configurations migrating forward successfully.

Before upgrading to the next desired version of OS the administrator should read all the release notes to make sure that the known issues on that release will not impact with the configurations currently running.

iRules are compiled scripts running on the system's current version of code. Changes in the OS can change how the iRule functions (or functions at all) between versions. Testing the OS upgrade in a lab environment is the best way to make sure there are no failing iRules after an upgrade. Also reading through the DevCentral reference on Commands and Events by version is a good place to start.

DevCentral Commands and Events

When migrating from older releases to a newer major release of OS, there can be issues with configuration migration to the newer release. You should always read the release notes and follow the recommended migration path for the version on the Ask F5 site.

SECTION 8 – MANAGE EXISTING SYSTEM AND APPLICATION SERVICES

Objective - 8.01 Modify and manage virtual servers

8.01 - Given a proposed virtual server configuration change, outline the scope of the change and for which connections those changes will affect (active connections, new connections, persisted sessions)

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

This topic would be an example of an existing virtual server configuration that is being modified. If you were to add a profile or an iRule to a virtual server what would be the impact to the existing or new client connections.

Build out a basic virtual server on the LTM and see what different profile changes do to client connections.

8.01 - Given a description of an application, identify the correct virtual server configured for it (HTTP/HTTPS, TCP/UDP, VLANs enabled, route-domain)

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

With a description of an application can you tell how a virtual server will need to be configured? For example if you had an SSL protected virtual server and needed to do cookie insert persistence. How would this be configured at a high level? The virtual server would have to terminate the SSL traffic with a Clientside SSL profile, to be able to apply the http profile, so that you can process the http traffic to insert a cookie into the header.

8.01 - Given a situation where a virtual server configuration change did not appear to immediately take effect, determine why

GUI Study in the vLabs

This blueprint topic is related to choosing the correct answer for a scenario type of question. For most questions like these you must have exposure to supporting the BIG-IP platform in a production environment or understand many of the different issues that may arise around the topic and the best practice method of solving the issue. Hands-on study is the best way to master these types of topics.

This topic has to do with recognizing that changing settings on a virtual server may not immediately look as if anything changed. The scope of the change and behavior of the type of change will define who and how the clients will be affected.

Some changes do not affect existing connections only the new connections after the change is made will be affected.

Objective - 8.02 Modify and manage pools

8.02 - Distinguish between disabling a member and forcing it down

Disabling nodes or pool members for maintenance (9.x - 10.x)

You can set the node and pool members to a Disabled or Forced offline state. When you need to interrupt access to a network device (such as a server) for maintenance, you should change the state of the node to Disabled or Forced Offline.

When set to Disabled, a node or pool member continues to process persistent and active connections. It can accept new connections only if the connections belong to an existing persistence session.

When set to Forced Offline, a node or pool member allows existing connections to time out, but no new connections are allowed.

8.02 - Determine use cases for disabling a member

GUI Study in the vLabs

If the administrator needs to make changes, such as configuration maintenance, to a server, that is the resource of a pool, but wants to gracefully allow users to finish what they are doing, then they should set the pool resource to Disabled.

8.02 - Determine use cases for forcing down a member

GUI Study in the vLabs

If the administrator needs take a resource out of a pool immediately due to a critical misconfiguration or system error that is impacting business, they can set the resource to Forced Offline.

8.02 - Given a situation where a pool member has been disabled but still appears to be receiving traffic, determine the cause

GUI Study in the vLabs

Setting the pool resource to Disabled will allow the current users to finish their sessions but not start new connections to this resource unless the virtual server is using persistence. If the virtual server is using persistence then the persistence record will be honored until it expires. Thus the administrator could disable a pool member and that member can still receive new connections from the existing persisted clients.

8.02 - Articulate the characteristics of a pool member that has been disabled or forced offline (Such as for new connections, persisted connections, etc.)

GUI Study in the vLabs

Setting the pool resource to Disabled will allow the current users to finish their sessions but not start new connections to this resource unless the virtual server is using persistence. Setting the pool resource to Forced Offline will allow current connections to finish but will not allow any new connections to the even if persistence is configured on the virtual server. If the Administrator needs to stop all connections immediately from a pool resource with out any completion of the current connections. Then removing the pool member from the pool will kill all connections immediately. This is not recommended for day-to-day maintenance but is an option for emergencies.

Conclusion

This document is intended as a study guide for the F5 201 – TMOS Administration exam. This study guide is not an all-inclusive document that will guarantee a passing grade on the exam. It is intended to be a living doc and any feedback or material that you feel should be included, to help exam takers better prepare, can be sent to channeleng@f5.com.

Thank you for using this study guide to prepare the F5 201 – TMOS Administration exam and good luck with your certification goals.

Thanks,
Eric Mitchell
Channel FSE, East US and Federal

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Americas info@f5.com
Asia-Pacific apacinfo@f5.com
Europe/Middle-East/Africa emeainfo@f5.com
Japan f5j-info@f5.com