Vendor: F5

Exam Code: F5CAB5

Exam Name: BIG-IP Administration Support and Troubleshooting

Version: DEMO

QUESTION 1
A Virtual Server uses an iRule to send traffic to pool members depending on the URI. The BIG-IP Administrator needs to modify the pool member in the iRule. Which event declaration does the BIG- IP Administrator need to change to accomplish this?

A. CLIENT_ACCEPTED
B. HTTP_RESPONSE
C. HTTP_REQUEST
D. SERVER_CONNECTED

Answer: C
Explanation:
In F5 TMOS administration, the traffic flow is processed through specific event huddles within iRules. To troubleshoot or modify traffic based on a URI (Uniform Resource Identifier), the BIG-IP system must first parse the application-layer data. The HTTP_REQUEST event is triggered when the system has fully received and parsed the HTTP request headers from the client. This is the correct point to implement logic that selects a pool or pool member based on the path or file requested (e.g., /images or /api). Using CLIENT_ACCEPTED would be too early in the troubleshooting process because that event triggers at the L4 (TCP) connection establishment phase, before any URI information is available. Conversely, HTTP_RESPONSE occurs during the return traffic from the server, which is too late to make a load balancing decision. For troubleshooting virtual server behavior where URIs are involved, ensuring the iRule is attached to a Virtual Server with an HTTP profile and using the HTTP_REQUEST event is essential for proper traffic steering and inspection.

QUESTION 2
Refer to the exhibit. A BIG-IP Administrator creates a new Virtual Server to load balance SSH traffic. Users are unable to log on to the servers. What should the BIG-IP Administrator do to resolve the issue? (Exhibit shows a Standard Virtual Server with an HTTP profile applied).

A. Set Protocol to UDP8
B. Set HTTP Profile to None9
C. Set Source Address to 10.1.1.210
D. Set Destination Addresses/Mask to 0.0.0.0/011

Answer: B
Explanation:
When troubleshooting a Virtual Server that is not working as expected, it is critical to ensure that the applied profiles match the type of traffic being processed. SSH (Secure Shell) is a non-HTTP protocol that operates over TCP. The exhibit indicates that an HTTP profile is applied to the Virtual Server. An HTTP profile instructs the BIG-IP system to parse traffic as HTTP; however, since SSH traffic does not follow HTTP specifications, the BIG-IP's parser will fail to understand the data stream, typically resulting in dropped packets or reset connections. To fix this, the administrator must set the HTTP profile to "None". This allows the Virtual Server to act as a "Standard" or "FastL4" listener that passes the encrypted SSH data transparently to the backend pool members without attempting application-layer inspection. This highlights a common troubleshooting step: verifying that L7 profiles are not inadvertently applied to L4 traffic, which disrupts the expected traffic flow between the client and the server.

QUESTION 3
A BIG-IP Administrator uses backend servers to host multiple services per server. There are multiple virtual servers and pools defined, referencing the same backend servers. Which load balancing algorithm is most appropriate to have an equal number of connections on each

backend server?

A. Least Connections (member)
B. Least Connections (node)
C. Predictive (member)
D. Predictive (node)

Answer: B
Explanation:
When load balancing is not working as expected and connections appear skewed across physical hardware, the administrator must distinguish between "member" and "node" level balancing. A "member" refers to a specific IP and Port combination (e.g., 10.1.1.1:80), whereas a "node" refers to the underlying IP address (10.1.1.1) regardless of the port. If a single server hosts multiple services (Web, FTP, API) across different pools, using "Least Connections (member)" would only balance connections within each individual pool. This could lead to a scenario where one server is overwhelmed because it is winning the "least connections" count in three different pools simultaneously. By selecting "Least Connections (node)," the BIG-IP tracks the total number of concurrent connections to the physical IP address across all pools it belongs to. This ensures that the administrator can maintain an equal distribution of work across the hardware, preventing performance degradation on backend servers that host multiple application services.

QUESTION 4
In the BIG-IP Configuration Utility, a user requests a single screen view to determine the status of all Virtual Servers and associated pool members, as well as any iRules in use. Where should the BIG-IP Administrator instruct the user to find this view?

A. Local Traffic > Monitors
B. Local Traffic > Virtual Servers
C. Local Traffic > Network Map
D. Statistics

Answer: C
Explanation:
To confirm functionality across a complex environment, the "Network Map" is the most efficient troubleshooting tool in the Configuration Utility. It provides a hierarchical, visual representation of the traffic management objects. A single glance allows the administrator to see the status of a Virtual Server (Green/Red/Yellow), the status of its associated pool, the health of individual pool members, and which iRules are currently attached. This view is superior to the standard "Virtual Server List" for troubleshooting because it maps the dependencies between objects. For example, if a Virtual Server is "Red," the Network Map will show if that status is inherited from a failed pool or a specific monitor failing on a pool member. Reviewing these basic stats in the Network Map helps the administrator quickly isolate whether a failure is at the service level (Virtual Server), the logic level (iRule), or the hardware level (Pool Member).

QUESTION 5
In an F5 BIG-IP system, a pool is configured with a health monitor and the "ManualResume" feature is Enabled. If a poolmember is marked Offline(Red) due to a health monitor failure, what will be the status of the member once the health monitor successfully passes again?

A. Offline (Disabled)
B. Offline (Enabled)
C. Available (Disabled)

D. Available (Enabled)

Answer: A
Explanation:
The "Manual Resume" feature is a safety mechanism used when a pool is not working as expected due to flapping services or unstable backend applications. Normally, when a health monitor fails, the pool member is marked "Offline" (Red), and when the monitor passes, it automatically returns to "Available" (Green). However, if "Manual Resume" is enabled, the BIG-IP will not automatically put the member back into rotation after a failure. Even if the health check begins to pass again, the member remains in an "Offline (Disabled)" state. This requires an administrator to manually intervene and re-enable the member. This is a common point of confusion when troubleshooting; a member may show passing health checks but still not receive traffic because it is waiting for a manual administrative "resume" command. This feature is intended to prevent "unhealthy" servers from receiving traffic until an engineer has confirmed the root cause of the initial failure was resolved.

QUESTION 6
Some users who connect to a busy Virtual Server have connections reset by the BIG-IP system. Pool member resources are NOT a factor in this behavior. What is a possible cause for this behavior?

A. The Connection Rate Limit is set too high
B. The server SSL Profile has NOT been reconfigured.
C. The Connection Limit is set too low.
D. The Rewrite Profile has NOT been configured.

Answer: C
Explanation:
When troubleshooting intermittent connection resets on a "busy" Virtual Server, the administrator must examine the configured thresholds. A "Connection Limit" is a hard cap on the number of concurrent connections a Virtual Server or pool member can handle. If this limit is set too low, the BIG-IP will reset any new connection attempts once the threshold is reached. The key indicator in this scenario is that the problem only affects "some users" and happens when the server is "busy," suggesting that the system is hitting a capacity ceiling rather than suffering from a persistent configuration error. Unlike a missing SSL profile, which would likely cause all connections to fail, or a "Connection Rate Limit," which throttles how fast connections arrive, a "Connection Limit" focuses on the total volume. Identifying this as the cause requires reviewing the Virtual Server's statistics to see if the "Current Connections" count is consistently peaking at the configured limit value.

QUESTION 7
Due to a change in application requirements, a BIG-IP Administrator needs to modify the configuration of a Virtual Server to include a Fallback Persistence Profile. Which persistence profile type should the BIG-IP Administrator use for this purpose?

A. SSL
B. Hash
C. Universal
D. Source Address Affinity

Answer: D
Explanation:

Persistence is critical for ensuring that a client's session remains with the same pool member throughout its duration. If primary persistence (like Cookie Persistence) fails--for instance, because the client has disabled cookies--load balancing will not work as expected, and the session may be broken. A "Fallback Persistence Profile" provides a backup method. The most common and reliable fallback method is "Source Address Affinity". This method tracks the client's IP address in the BIG-IP's persistence table and ensures that any subsequent requests from that IP are routed to the same pool member, even if the primary persistence token is missing. Troubleshooting session drops often involves checking if a fallback method is configured to handle scenarios where the primary method is unsupported by the client's browser or environment. Without a fallback, the BIG-IP would revert to standard load balancing, potentially sending the client to a different server that lacks their session data.

QUESTION 8
A BIG-IP device sends out the following SNMP trap:

```
big-ipo.f5.com - bigipExternalLinkChange Link: 1.0 is DOWN.
```

Where in the BIG-IP Configuration utility should the BIG-IP Administrator verify the current status of Link 1.0?

A. System > Platform
B. Network > Trunks > Trunk List
C. Statistics > Performance > System
D. Network > Interfaces > Interface List

Answer: D
Explanation:
Identifying network-level performance issues often starts with investigating hardware-level alerts. In F5 terminology, a "Link" like "1.0" or "1.1" refers to a physical interface on the appliance. When an SNMP trap reports that a link is "DOWN," it indicates a loss of signal or an administrative shutdown of the physical port. To verify this, the administrator must navigate to Network > Interfaces > Interface List. This screen provides real-time status, showing whether the interface is "up," "down," or "uninitialized," as well as any media speed or duplex mismatches that could be causing performance degradation. Troubleshooting this is the first step in resolving "pool member down" or "VLAN failsafe" issues, as a down interface will take down any VLANs associated with it, immediately halting all traffic flow for the services relying on that physical path.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**