

Pass4Sure.101.485Questions

VCEplus.com

Number: 101
Passing Score: 800
Time Limit: 120 min
File Version: 35.0

Pass 4 Sure

101

Application Delivery Fundamentals

- ★ Made Questions into Sections, now we can learn by Sections with this assistance.
- ★ This is the best VCE I ever constructed. Attempt fellows and if any proposal please overhaul this.
- ★ These are the most exact study questions. Simply concentrate on these and sit in your exam.
- ★ Changed few inquiries, settled few spelling errors and grammatical mistakes.
- ★ Numerous new inquiries are included , Good for survey feel free to pass the exam now.

Exam A

QUESTION 1

Which two processes are involved when BIGIP systems issue traps? (Choose two.)

- A. bigd
- B. alertd
- C. smtpd
- D. sysloging

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 2

A monitor has been defined using the HTTP monitor template. The send and receive strings were customized, but all other settings were left at their defaults. Which resources can the monitor be assigned to?

- A. Only specific pool members.
- B. Most virtual servers.
- C. Most nodes.
- D. Most pools

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 3

After editing and saving changes to the configuration file containing virtual servers, what is the immediate result?

- A. The new configuration is verified and loaded.
- B. The new configuration is verified not loaded.
- C. The new configuration is verified.
- D. The new configuration is loaded but not verified.

- E. The new configuration is neither verified nor loaded.
- F. The new configuration is verified and loaded if it is syntactically correct.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 4

When a virtual server has an HTTP profile with compression enabled, which traffic is compressed by the BIG-IP?

- A. Selected traffic from the BIG-IP to the client.
- B. All server-side traffic for that virtual server.
- C. Selected traffic from the pool member to the BIG-IP.
- D. All client-side traffic for that virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 5

Which two statements are true concerning capabilities of current BIG-IP platforms? (Choose two.)

- A. The 1600 hosts more ports than the 3900.
- B. All current BIG-IP platform use both an ASIC. And CPU(s) to process traffic.
- C. All current BIG-IP platform can perform hardware compression.
- D. Only 2U BIG-IP Platform have an option of a second power supply.
- E. All BIG-IP have capacity to perform bulk encryption I decryption of SSL traffic independent of the CPU.

Correct Answer: BE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 6

Which is the result when multiple monitors are assigned to a pool member?

- A. The member is marked available if sufficient monitors succeed, and as unavailable if insufficient monitors succeed.
- B. The member is marked as available if any of the monitors succeed.
- C. The member is marked as unavailable if any of the monitors fails.
- D. The member is marked available if all monitors succeed, and as marginal if one or more monitors fail(s).

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 7

A site wishes to use an external monitor. Other than what is coded in the monitor script, what information must be configured on the BIGIP for the monitor to be functional? (Choose two.)

- A. BIG-IP services that are running on the system to be tested.
- B. BIG-IP the IP addresses of the devices that will be tested. Must know which
- C. BIG-IP node or member the result are to be applied to. Must know all
- D. BIG-IP must know the name of the program.
- E. BIG-IP must know which function the program is going to test. Must know

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 8

Which statement describes advanced shell access correctly?

- A. Users with advanced shell access can always change, add, or delete LTM objects in all partitions. Users with? Advanced shell access can always, change, add, or delete LTM objects in all partitions.
- B. Users with advanced shell access are limited to changing, adding, or deleting LTM object in any single partition. Users with? Advanced shell accesses are limited to changing, adding, or deleting LTM object on any single partition.

- C. Users with advance shell access have the same right as those with msh access, but theright extend to all partition rather than to Users with advance shell access have the sameright as those with msh access, but right extend to all partition rather than to a singlepartition.
- D. All Users can be given advanced shell access. All users can be given advance shellaccess.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

specified answer

QUESTION 9

Adivinar (?)

- A. The context determines the values of commands that vary between client and server.
- B. The context has no impact on events.
- C. The context determines which events are available for iRule processing.
- D. The context determines which pools are available for load balancing.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 10

The partial configuration below includes an iRule, a virtual server, and pools. When trafficfrom the client at 160.10.10.10:2056 connects to the virtual server Test_VS and sends anHTTP request, what will the client's source address be translated to as the traffic is sent tothe chosen pool member?

```
poolTest_Pool { member 10.10.10.10:80 member 10.10.10.11:80 } snatpoollower_range { member 10.10.10.1 } snatpoolupper_range { member 10.10.10.2 } ruleTest_iRule { when CLIENT_ACCEPTED.{ if { [TCP::local_port] < 2024 }{ snatpool lower_range } else { snatpoolupper_range } } virtualTest_VS { destination 200.10.10.1 :http pool Test_Pool rule Test_i Rule }
```

- A. 160.10.10.10.
- B. It could be either 10.10.10.10 or 10.10.10.11.
- C. 10.10.10.2.
- D. 200.10.10.1.
- E. 10.10.10.1.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 11

What is the expected difference between two source address persistence profiles if profile A has a mask of 255.255.255.0 and profile B has a mask of 255.255.0.0?

- A. Profile A will have more clients matching existing persistence records.
- B. There are no detectable differences.
- C. Profile B has a greater potential number of persistence records.
- D. Profile B will have fewer persistence records for the same client base.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

modified answer

QUESTION 12

A BIGIP has two SNATs, a pool of DNS servers and a virtual server configured to load balance UDP traffic to the DNS servers. One SNAT's address is 64.100.130.10; this SNAT is defined for all addresses. The second SNAT's address is 64.100.130.20; this SNAT is defined for three specific addresses, 172.16.3.54, 172.16.3.55, and 172.16.3.56. The virtual server's destination is 64.100.130.30:53. The SNATs and virtual server have default VLAN associations. If a client with IP address 172.16.3.55 initiates a request to the virtual server,

What is the source IP address of the packet as it reaches the chosen DNS server?

- A. 64.100.130.30
- B. 172.16.3.55
- C. 64.100.130.20
- D. 64.100.130.10

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

correct answer

QUESTION 13

A steaming profile will do which of the following?

- A. Search and replace all occurrences of a specified string only in responses processed by a virtual server.
- B. Search and replace all occurrences of a specified string only in request processed by a virtual server.
- C. Search and replace all occurrences of a specified string in requests and responses processed by a virtual server.
- D. Search and replace the first occurrence of a specified of a specified string in either a request or response processed by a virtual server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 14

A monitor has been defined using the HTTP monitor template. The send and receive strings were customized, but all other settings were left at their defaults. Which resources can the monitor be assigned to?

- A. only specific pool members
- B. most virtual servers
- C. most nodes
- D. most pools

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 15

When DNS_REV is used as the probe protocol by the GTM System, which information is expected in the response from the probe?

- A. A reverse name lookup of the GTM System
- B. The list of root servers known by the local DNS
- C. The FQDN of the local DNS being probed for metric information
- D. The revision number of BIND running on the requesting DNS server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 16

Which three can be a part of a pool's definition? (Choose three.)

- A. Link
- B. Monitors
- C. Wide IPs
- D. Persistence
- E. Data Centers
- F. Virtual Servers

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 17

Which two must be included in a Wide-IP definition for the Wide-IP to resolve a DNS query? (Choose two.)

- A. a name
- B. a monitor
- C. a load balancing method
- D. one or more virtual servers

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 18

A GTM System would like to ensure that a given LTM System is reachable and iQuerycommunication is allowed prior to sending it client request. What would be the simplestmonitor template to use?

- A. TCP
- B. ICMP
- C. HTTP
- D. BIGIP
- E. SNMP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 19

Which two ports must be enabled to establish communication between GTM Systems andother BIG IP Systems? (Choose two.)

- A. 22
- B. 53
- C. 443
- D. 4353
- E. 4354

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 20

When probing LDNSs, which protocol is used by default?

- A. TCP
- B. ICMP
- C. DNS_REV
- D. DNS_DOT

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

What is the difference between primary and secondary DNS servers?

- A. Only primary servers can issue authoritative responses.
- B. Primary servers host the original copy of the zone database file.
- C. Primary servers resolve names more efficiently than secondary servers.
- D. Secondary servers act as backups and will respond only if the primary fails.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

If the config tool is complete, which two access methods are available by default for GTMadministration and configuration? (Choose two.)

- A. network access via http
- B. network access via https
- C. network access via telnet
- D. direct access via serial port

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

updated answers

QUESTION 23

A GTM System performs a name resolution that is not a Wide-IP. The name is in a domainfor which the GTM System is authoritative. Where does the information come from?

- A. It comes from BIND database (zone) files on the GTM System.
- B. GTM System cannot resolve a host name that is not a Wide-IP.
- C. It comes from the database of previously cached name resolutions.
- D. It comes from a zone transfer initiated when the request was received

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 24

How do you support non-intelligent DNS resolution in an environment with GTM Systems and standard DNS servers? (Choose two.)

- A. The GTM System must be a secondary server in all of your zones.
- B. Your GTM System must delegate some DNS names to the DNS Servers.
- C. Your DNS servers may delegate some DNS names to the GTM Systems.
- D. The GTM System may have a Listener set for your DNS server's address.
- E. The GTM System may have a Listener set for the GTM's loopback address.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 25

iQuery is a proprietary protocol that distributes metrics gathered from which three sources?(Choose three.)

- A. SNMP
- B. DNS root servers
- C. Path probes such as ICMP
- D. Monitors from LTM Systems
- E. Monitors from Generic Host Servers

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 26

What is the purpose of the GTM Systems Address Exclusion List concerning local DNSservers?

- A. To prevent probing of specific local DNSs
- B. To prevent name resolution to specific Virtual Servers
- C. To prevent name resolution for requests from specific local DNSs
- D. To prevent probing of any local DNS servers by specific F5 devices

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 27

Which three must be done so that Generic Host Servers can be monitored using SNMP?(Choose three.)

- A. The SNMP monitor must be added to all BIG-IP Systems.
- B. The Generic Host Server must be running the big3d agent.
- C. The GTM System must be configured for the appropriate MIB .
- D. The Generic Host Server must be added to the GTM Configuration.
- E. The Generic Host Server must be enabled to answer SNMP queries.

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

verified answer

QUESTION 28

Monitors can be assigned to which three resources? (Choose three.)

- A. Pools
- B. Servers
- C. Wide IPs
- D. Data Centers
- E. Pool Members

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

answer is valid

QUESTION 29

Which two daemons only run after the entire license process has been completed? (Choosetwo.)

- A. zrd
- B. tmm
- C. ntpd
- D. gtmd

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 30

What does the bigip_add script do?

- A. Add BIG-IP servers to the wideip.conf file.
- B. Add an existing GTM System to a sync group.
- C. Synchronize configuration files between BIG-IP Systems.
- D. Exchange web certificates and keys between BIG-IP Systems.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 31

Which dynamic load balancing mode affects load-balancing decisions based on packet metrics?

- A. Packet Rate.
- B. Completion Rate.
- C. Least Connections.
- D. Virtual Server Capacity.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 32

If the GTM System receives a packet destined for one of its Listener addresses the GTM will process the request ...

- A. either through Wide-IP processing or BIND processing
- B. through Wide-IP processing and may process it through BIND processing
- C. through BIND processing and may process it through Wide-IP processing
- D. through Wide-IP processing and BIND processing and choose the best answer between the two

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 33

Which file contains the list of events for which the GTM System will send traps to an SNMP manager?

- A. /etc/snmpd.conf
- B. /etc/syslog-ng.conf
- C. /etc/alertd/alert.conf
- D. /etc/gtm_snmptrap.conf

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 34

Which three parameters can be specified within the Setup Utility? (Choose three.)

- A. Password of the "root" user
- B. IP address of an NTP server
- C. IP address of an initial WideIP
- D. IP address restrictions for ssh access
- E. All necessary administrative IP addresses (including floating addresses)

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

updated options

QUESTION 35

Which of the following are correct regarding Wildcard entities? (Choose 2)

- A. Wildcard entities are the basis for positive security logic.
- B. Wildcard entities are the basis for negative security logic.
- C. Wildcard entities require the need to learn only from violations.
- D. Wildcard entities can be applied to file types, URLs, cookies and parameters.

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 36

Flow login allows for more granular protection of login and logout URLs within webapplications. Which of the following are components of flow login?

(Choose 3)

- A. Schema
- B. Login URLs
- C. Login pages
- D. Attack signatures
- E. Access validation

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 37

The BIG-IP ASM System is configured with a virtual server that contains an HTTP classprofile and the protected pool members are associated within the HTTP class profile pooldefinition. The status of this virtual server is unknown (Blue). Which of the following conditions will make this virtual server become available (Green)?

- A. Assign a successful monitor to the virtual server
- B. Assign a successful monitor to the members of the HTTP class profile pool
- C. Associate a fallback host to the virtual server and assign a successful monitor to the fallback host
- D. Associate a default pool to the virtual server and assign a successful monitor to the poolmembers

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 38

Which of the following does not pertain to protecting the Requested Resource (URI) element?

- A. File type validation
- B. URL name validation
- C. Domain cookie validation
- D. Attack signature validation

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 39

Which of the following protocol protections is not provided by the Protocol SecurityManager?

- A. FTP
- B. SSH
- C. HTTP
- D. SMTP

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 40

Which of the following is correct regarding User-defined Attack signatures?

- A. User-defined signatures use an F5-supplied syntax
- B. User-defined signatures may only use regular expressions
- C. Attack signatures may be grouped within system-supplied signatures
- D. User-defined signatures may not be applied globally within the entire policy

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 41

Which of the following methods of protection is not available within the Protocol SecurityManager for HTTP traffic?

- A. Data guard

- B. Attack signatures
- C. Evasion techniques
- D. File type enforcement

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 42

There are many user roles configurable on the BIG-IP ASM System. Which of the following user roles have access to make changes to ASM policies? (Choose 3)

- A. Guest
- B. Operator
- C. Administrator
- D. Web Application Security Editor
- E. Web Application Security Administrator

Correct Answer: CDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 43

In the following configuration, a virtual server has the following HTTP class configuration:

HTTP Class 1 = Host pattern www.f5.com HTTP Class 2 = No filters A request arriving for WWW.F5.COM will be matched by which class(es)?

- A. Class 1
- B. Class 2
- C. Both Class 1 and Class 2
- D. The request will be dropped

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

answer is perfect

QUESTION 44

Learning suggestions in the Policy Building pages allow for which of the following? (Choose2)

- A. XML-based parameters and associated schema are automatically learned.
- B. Blocking response pages can be automatically generated from web site content.
- C. Flow level parameters are displayed when found and can be accepted into the current policy
- D. The administrator may modify whether the BIG-IP ASM System will learn, alarm, or block detected violations.
- E. Maximum acceptable values for length violations are calculated and can be accepted into the security policy by the administrator.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 45

Which of the following statements are correct regarding positive and negative security models? (Choose 2)

- A. Positive security model allows all transactions by default.
- B. Negative security model denies all transactions by default.
- C. Negative security model allows all transactions by default and rejects only transactions that contain attacks.
- D. Positive security model denies all transactions by default and uses rules that allow only those transactions that are considered safe and valid.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 46

Which events are valid iRule events triggered by BIG-IP ASM processing? (Choose 2)

- A. ASM_REQUEST_BLOCKING
- B. ASM_REQUEST_ACCEPTED

- C. ASM_REQUEST_VIOLATION
- D. ASM_RESPONSE_BLOCKING

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 47

Which of the following methods of protection is not available within the Protocol SecurityManager for FTP protection?

- A. Session timeout
- B. Command length
- C. Allowed commands
- D. Anonymous FTP restriction

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 48

Logging profiles are assigned to?

- A. HTTP class
- B. Security policies
- C. Web applications
- D. Attack signatures

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 49

Which of the following is a language used for content provided by a web server to a webclient?

- A. FTP
- B. TCP
- C. HTTP
- D. HTML

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 50

Which of the following methods are used by the BIGIP ASM System to protect againstSQL injections?

- A. HTTP RFC compliancy checks
- B. Meta-character enforcement and attack signatures
- C. HTTP RFC compliancy checks and length restrictions
- D. Response scrubbing, HTTP RFC compliancy checks, and meta-character enforcement

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 51

Which of the following can be associated with an XML profile?

- A. Flow
- B. Method
- C. Parameter
- D. File type

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 52

An HTTP class is available ..

- A. on any BIG-IP LTM system
- B. only when ASM is licensed.
- C. only when ASM or WA are licensed.
- D. only when a specific license key is required.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 53

Which of the following methods of protection operates on server responses?

- A. Dynamic parameter protection
- B. Response code validation and response scrubbing
- C. Response code validation and HTTP method validation
- D. HTTP RFC compliancy check and meta-character enforcement

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 54

Which of the following is not a configurable parameter data type?

- A. Email
- B. Array

- C. Binary
- D. Decimal

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

When we have a * wildcard entity configured in the File Type section with tightening enabled, the following may occur when requests are passed through the policy. Which is the most accurate statement?

- A. File type violations will not be triggered.
- B. File type violations will be triggered and learning will be available based on these violations.
- C. File type entities will automatically be added to the policy (policy will tighten).
- D. File type violations will not be triggered and the entity learning section will be populated with file type recommendations.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 56

A request is sent to the BIGIP ASM System that generates a Length error violation. Which of the following length types provides a valid learning suggestion? (Choose 3)

- A. URL
- B. Cookie
- C. Response
- D. POST data
- E. Query string

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 57

There is multiple HTTP class profiles assigned to a virtual server. Each profile has Application Security enabled. Which statement is true?

- A. Traffic will process through every HTTP class profile every time.
- B. Traffic will process through the first HTTP class profile that it matches and then stops.
- C. Traffic will process through one HTTP class profile and if the traffic matches another
- D. Traffic will only process through the HTTP class profile that it matches but always processes through the whole list and will process through each HTTP class profile it matches.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

answer is updated

QUESTION 58

A security audit has determined that your web application is vulnerable to a cross-site scripting attack. Which of the following measures are appropriate when building a security policy? (Choose 2)

- A. Cookie length must be restricted to 1024 bytes.
- B. Attack signature sets must be applied to any user input parameters.
- C. Parameter data entered for explicit objects must be checked for minimum and maximum values.
- D. Parameter data entered for flow level parameters must allow some meta-characters but not others.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 59

The BIG-IP ASM System sets two types of cookies to enforce elements in the security policy. The two types are main and frame cookies. What is the purpose of the frame cookie? (Choose 2)

- A. Validates domain cookies

- B. Detects session expiration
- C. Stores dynamic parameters and values
- D. Handles dynamic parameter names and flow extractions

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 60

Which statement is correct concerning differences between BIG-IP ASM platforms?

- A. The 3900 has more ports than the 6800.
- B. The 3900 and 6800 have the same number of ports.
- C. The 3900 and 6800 can support both the module and standalone versions of BIG-IP ASM.
- D. The 3900 can support both module and standalone versions of BIG-IP ASM whereas the 6800 can support only the module version of BIG-IP ASM.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 61

Which of the following mitigation techniques is based on anomaly detection? (Choose 2)

- A. Brute force attack prevention.
- B. Cross-site request forgery prevention.
- C. Web scraping attack prevention.
- D. Parameter tampering prevention.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 62

Which of the following are default settings when using the Policy Builder to build a security policy based on the QA lab deployment scenario? (Choose 2)

- A. All learned entities are placed in staging.
- B. Attack signatures are not placed in staging.
- C. The security policy is placed in blocking mode.
- D. Tightening is enabled only on file types and parameters.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

valuable answers

QUESTION 63

Which of the following statements are incorrect regarding protection of web services?(Choose 2)

- A. The BIG-IP ASM System checks to ensure web services use cookies.
- B. The BIG-IP ASM System parses XML requests and XML responses.
- C. The BIG-IP ASM System checks to ensure XML documents are well formed.
- D. The BIG-IP ASM System uses attack signatures to enforce negative security logic.
- E. The BIG-IP ASM System checks for XML syntax, schema validation, and WSDL validation.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 64

Which of the following is correct regarding static parameters?

- A. A static parameter is stored in a frame cookie.
- B. A static parameter is pre-defined by the web application logic.
- C. A static parameter is learned only by using the Deployment Wizard.
- D. A static parameter is mapped once when creating the application flow model.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 65

When configuring the BIG-IP ASM System in redundant pairs, which of the following are synchronized? (Choose 2)

- A. License file
- B. Security policies
- C. Web applications
- D. Request information
- E. Traffic learning information

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 66

Sensitive parameter is a feature used to hide sensitive information from being displayed in which of the following?

- A. Client request
- B. Server response
- C. GUI and logs of BIGIP ASM System
- D. Configuration file of BIGIP ASM System

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 67

Tightening is a feature of which type of entity?

- A. Explicit URLs
- B. Attack signatures
- C. Flow login URLs
- D. Wildcard parameters

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 68

Which of the following is not a feature of a standalone BIG-IP ASM System?

- A. Attack signatures
- B. Multiple pool members
- C. Positive security model
- D. Real-time traffic policy builder
- E. Pre-defined security policy templates

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 69

What are the best reasons for using the Deployment Wizard? (Choose 3)

- A. Flow-level parameters checking is required.
- B. The application encoding scheme needs to be determined by the BIG-IP ASM System.
- C. Sufficient time is available to allow completely automated policy building based on observing live traffic.
- D. The application platform must be protected against known attacks for the specific operating system, web server, and database.

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 70

When building a policy based on live traffic using the automated policy builder, which of the following elements will not be taken into account when analyzing the traffic?

- A. The size of the response
- B. The requested resource (URI)
- C. The response code from the web server
- D. The parameter values of static based parameters

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 71

Which method of protection is not provided by the Rapid Deployment policy template?

- A. Data leakage
- B. Buffer overflow
- C. HTTP protocol compliance
- D. Dynamic parameter validation

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 72

Which of the following are properties of an ASM logging profile? (Choose 2)

- A. storage type
- B. storage filter
- C. storage policy

D. web application

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 73

Which of the following methods of protection are used by the BIG-IP ASM System to mitigate buffer overflow attacks?

- A. HTTP RFC compliancy checks
- B. Length restrictions and attack signatures
- C. Length restrictions and site cookie compliancy checks
- D. Meta-character enforcement and HTTP RFC compliancy check

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

modified answers

QUESTION 74

The Web Application Security Administrator user role can perform which of the following functions? (Choose 2)

- A. Modify HTTP class profiles.
- B. Create new HTTP class profiles.
- C. Create new Attack signature sets.
- D. Assign HTTP class profiles to virtual servers.
- E. Configure Advanced options within the BIG-IP ASM System.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 75

The following request is sent to the BIGIP ASM System:

GET http://www.example.local/financials/week1.xls?display=yes&user=john&logon=true

Which of the following components in this requests line represent the query string?

- A. .xls
- B. /week1.xls
- C. /financials/week1.xls
- D. display=yes&user=john&logon=true

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 76

Which level of parameter assumes the highest precedence in BIG-IP ASM System processing logic?

- A. Flow
- B. Object
- C. Global
- D. URL

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 77

Which of the following storage type combinations are configurable in an ASM logging profile?

- A. Local and Syslog
- B. Local and Remote
- C. Remote and Syslog
- D. Remote and Reporting Server

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 78

When implementing Data Guard, BIG-IP ASM scans for suspicious patterns in? (Choose 2)

- A. All client requests
- B. All server responses
- C. Specific client requests
- D. Specific server responses

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 79

Which of the following methods of protection are used by BIG-IP ASM to mitigate buffer overflow attacks?

- A. HTTP RFC compliancy check
- B. Length restrictions and attack signatures
- C. Length restrictions and meta character enforcement
- D. Meta character enforcement and HTTP RFC compliancy check

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 80

A web client accesses a web application using what protocol?

- A. TCP
- B. XML
- C. HTML
- D. HTTP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 81

In the following request, which portion represents a parameter name?

- A. Yes
- B. User
- C. Week1
- D. Financials

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 82

Which of the following is not a method of protection for user-input parameters?

- A. Value extraction
- B. Attack signatures
- C. Length restriction
- D. Meta character enforcement

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 83

Which three statements describe a characteristic of profiles? (Choose three.)

- A. Default profiles cannot be created or deleted.
- B. Custom profiles are always based on a parent profile.
- C. A profile can be a child of one profile and a parent of another.
- D. All changes to parent profiles are propagated to their child profiles.
- E. While most virtual servers have at least one profile associated with them, it is not required.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 84

A virtual server is defined using a source-address based persistence profile. The last five connections were A, B, C, A, C. Given the conditions shown in the graphic, if a client with IP address 205.12.45.52 opens a connection to the virtual server, which member will be used for the connection?

All entries for the one virtual server and pool		
Persistence Values	Member	Age (Seconds)
200.10.0.0	10.10.20.1:80	63
201.12.0.0	10.10.20.3:80	43
153.15.0.0	10.10.20.2:80	76
205.12.0.0	10.10.20.4:80	300
195.64.0.0	10.10.20.3:80	22
198.22.0.0	10.10.20.5:80	176
214.77.0.0	10.10.20.1:80	43

Web_Pool Statistics					
Member	Member Ratio	Member Priority	Outstanding Layer 7 Requests	Connection Count	Status
A: 10.10.20.1:80	3	5	6	18	Available
B: 10.10.20.2:80	3	5	6	12	Available
C: 10.10.20.3:80	3	5	12	5	Disabled
D: 10.10.20.4:80	1	1	8	19	Offline
E: 10.10.20.5:80	1	1	4	9	Available

Virtual Server, Pool and Persistence Profile Settings					
VS_Web_Pool Settings		Web_Pool Settings		Source Persist Settings	
Destination	172.160.22.3:80	Load Balancing	Least Connectons	Mode	Source Address
Profile(s)	TCP	Priority Activation	Less than 2	Netmask	255.255.0.0
Pool	Web_Pool	Montitor	Done	Timeout	360 seconds
iRules	None				
Persistence	Source_Persist				

- A. 10.10.20.1:80
- B. 10.10.20.2:80
- C. 10.10.20.3:80
- D. 10.10.20.4:80
- E. 10.10.20.5:80

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 85

How is persistence configured?

- A. Persistence is an option within each pool's definition.
- B. Persistence is a profile type; an appropriate profile is created and associated with virtual server.
- C. Persistence is a global setting; once enabled, load-balancing choices are superceded by the persistence method that is specified.
- D. Persistence is an option for each pool member. When a pool is defined, each member's definition includes the option for persistence.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 86

Which cookie persistence method requires the fewest configuration changes on the web servers to be implemented correctly?

- A. insert
- B. rewrite
- C. passive
- D. session

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

valid answer

QUESTION 87

Which statement is true concerning cookie persistence?

- A. Cookie persistence allows persistence independent of IP addresses.
- B. Cookie persistence allows persistence even if the data are encrypted from client to pool member.
- C. Cookie persistence uses a cookie that stores the virtual server, pool name, and member IP address in clear text.
- D. If a client's browser accepts cookies, cookie persistence will always cause a cookie to be written to the client's file system.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 88

Assume a virtual server has a ServerSSL profile. What SSL certificates are required on the pool members?

- A. No SSL certificates are required on the pool members.
- B. The pool members' SSL certificates must only exist.
- C. The pool members' SSL certificates must be issued from a certificate authority.
- D. The pool members' SSL certificates must be created within the company hosting the BIG-IPs.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 89

Assume a virtual server is configured with a ClientSSL profile. What would the result be if the virtual server's destination port were not 443?

- A. SSL termination could not be performed if the virtual server's port was not port 443.
- B. Virtual servers with a ClientSSL profile are always configured with a destination port of 443.
- C. As long as client traffic was directed to the alternate port, the virtual server would work as intended.
- D. Since the virtual server is associated with a ClientSSL profile, it will always process traffic sent to port 443.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

verified answer

QUESTION 90

Which is an advantage of terminating SSL communication at the BIG-IP rather than the ultimate web server?

- A. Terminating SSL at the BIG-IP can eliminate SSL processing at the web servers.
- B. Terminating SSL at the BIG-IP eliminates all un-encrypted traffic from the internal network. Terminating SSL at the BIG-IP eliminates all un-encrypted traffic from the internal network.
- C. Terminating SSL at the BIG-IP eliminates the need to purchase SSL certificates from a certificate authority.
- D. Terminating SSL at the BIG-IP eliminates the need to use SSL acceleration hardware anywhere in the network.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 91

Assume a client's traffic is being processed only by a NAT; no SNAT or virtual server processing takes place. Also assume that the NAT definition specifies a NAT address and an origin address while all other settings are left at their defaults. If the origin server were to initiate traffic via the BIG-IP, what changes, if any, would take place when the BIG-IP processes such packets?

- A. The BIG-IP would drop the request since the traffic didn't arrive destined to the NAT address. The BIG-IP would drop the request since the traffic didn't arrive destined to the NAT address.
- B. The source address would not change, but the destination address would be changed to the NAT address.
- C. The source address would be changed to the NAT address and destination address would be left unchanged.
- D. The source address would not change, but the destination address would be changed to a self-IP of the BIG-IP.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 92

A site wishes to perform source address translation on packets arriving from the Internet for clients using some pools but not others. The determination is not based on the client's IP address, but on the pool they are load balanced to. What could best accomplish this goal?

- A. A SNAT for all addresses could be defined, and then disable the SNAT processing for select pools.
- B. The decision to perform source address translation is always based on VLAN. Thus, the goal cannot be achieved.
- C. For each virtual server, regardless of their default load balancing pools, association with SNAT pools could vary dependent upon need.
- D. The decision to perform source address translation is always based on a client's address (or network). Thus, this goal cannot be achieved.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 93

Which two statements are true about SNATs? (Choose two.)

- A. SNATs are enabled on all VLANs, by default.
- B. SNATs can be configured within a Profile definition.
- C. SNATs can be configured within a Virtual Server definition.
- D. SNAT's are enabled only on the VLAN where origin traffic arrives, by default

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 94

A BIG-IP has two load balancing virtual servers at 150.150.10.10:80 and 150.150.10.10:443. The port 80 virtual server has SNAT automap configured. There is also a SNAT configured at 150.150.10.11 set for a source address range of 200.200.1.0 / 255.255.255.0. All other settings are at their default states. If a client with the IP address 200.200.1.1 sends a request to https://150.150.10.10, what is the source IP address when the associated packet is sent to the pool member?

- A. 200.200.1.1
- B. 150.150.10.11
- C. Floating self IP address on VLAN where the packet leaves the system
- D. Floating self IP address on VLAN where the packet arrives on the system

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

verified answer

QUESTION 95

Which statement is true concerning SNATs using automap?

- A. Only specified self-IP addresses are used as automap addresses.
- B. SNATs using automap will translate all client addresses to an automap address.
- C. A SNAT using automap will preferentially use a floating self-IP over a non-floating self-IP.
- D. A SNAT using automap can be used to translate the source address of all outgoing traffic to the same address regardless of which VLAN the traffic is sent through.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 96

Which two statements are true about NATs? (Choose two.)

- A. NATs support UDP, TCP, and ICMP traffic.
- B. NATs can be configured with mirroring enabled or disabled.
- C. NATs provide a one-to-one mapping between IP addresses.
- D. NATs provide a many-to-one mapping between IP addresses.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 97

Which statement describes a typical purpose of iRules?

- A. iRules can be used to add individual control characters to an HTTP data stream.
- B. iRules can be used to update the timers on monitors as a server load changes.iRules can be used to update the timers on monitors as a server? load changes.
- C. iRules can examine a server response and remove it from a pool if the response is unexpected.iRules can examine a server? response and remove it from a pool if the response is unexpected
- D. iRules can be used to look at client requests and server responses to choose a pool member to select for load balancing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is vdrified

QUESTION 98

A virtual server is listening at 10.10.1.100:80 and has the following iRule associated with it: when HTTP_REQUEST { if { [HTTP::header User-Agent] contains "MSIE" } { pool MSIE_pool } else { pool Mozilla_pool } If a user connects to http://10.10.1.100/foo.html and their browser does not specify a User-Agent, which pool will receive the request?

- A. MSIE_pool
- B. Mozilla_pool
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 99

Which event is always triggered when the client sends data to a virtual server using TCP?

- A. HTTP_DATA
- B. CLIENT_DATA
- C. HTTP_REQUEST
- D. VS_CONNECTED

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 100

A virtual server is listening at 10.10.1.100:any and has the following iRule associated with it: when CLIENT_ACCEPTED { if {[TCP::local_port] equals 21 } { pool ftppool } elseif {[TCP::local_port] equals 23 } { pool telnetpool } If a user connects to 10.10.1.100 and port 22, which pool will receive the request?

- A. ftppool
- B. telnetpool
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 101

When configuring a Virtual Server to use an iRule with an HTTP_REQUEST event, which lists required steps in a proper order to create all necessary objects?

- A. create profiles, create the iRule, create required pools, create the Virtual Server
- B. create the Virtual Server, create required pools, create the iRule, edit the Virtual Server
- C. create a custom HTTP profile, create required pools, create the Virtual Server, create the iRule
- D. create required pools, create a custom HTTP profile, create the iRule, create the Virtual Server

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 102

Which statement is true concerning a functional iRule?

- A. iRules use a proprietary syntax language.
- B. iRules must contain at least one event declaration.
- C. iRules must contain at least one conditional statement.
- D. iRules must contain at least one pool assignment statement.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 103

What is the purpose of floating self-IP addresses?

- A. to define an address that grants administrative access to either system at any time
- B. to define an address that allows either system to initiate communication at any time
- C. to define an address that allows network devices to route traffic via a single IP address
- D. to define an address that gives network devices greater flexibility in choosing a path to forward traffic

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 104

Which parameters are set to the same value when a pair of BIG-IP devices are synchronized?

- A. host names
- B. system clocks
- C. profile definitions
- D. VLAN fail-safe settings
- E. MAC masquerade addresses

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 105

Which two statements are true concerning the default communication between a redundant pair of BIG-IP systems? (Choose two.)

- A. Synchronization occurs via a TCP connection using ports 683 and 684.
- B. Connection mirroring data is shared via a TCP connection using port 1028.
- C. Persistence mirroring data is shared via a TCP connection using port 1028.
- D. Connection mirroring data is shared through the serial fail-over cable unless network fail-over is enabled.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 106

Which two methods can be used to determine which BIG-IP is currently active? (Choose two.)

- A. The bigtop command displays the status.
- B. Only the active system's configuration screens are active.
- C. The status (Active/Standby) is embedded in the command prompt.
- D. The ifconfig -a command displays the floating addresses on the active system.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 107

As a part of the Setup Utility, the administrator sets the host name for the BIG-IP. What would be the result if the two systems in a redundant pair were set to the same host name?

- A. Host names do not matter in redundant pair communication.
- B. In a redundant pair, the two systems will always have the same host name. The parameter is synchronized between the systems.
- C. The first time the systems are synchronized the receiving system will be assigned the same self-IP addresses as the source system.
- D. When the administrator attempts to access the configuration utility using the host name, they will always connect to the active system.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 108

When network fail-over is enabled, which of the following is true?

- A. The fail-over cable status is ignored. Fail-over is determined by the network status only.
- B. Either a network failure or loss of voltage across the fail-over cable will cause a fail-over.
- C. A network failure will not cause a fail-over as long as there is a voltage across the fail-over cable.
- D. The presence or absence of voltage over the fail-over cable takes precedence over network fail-over.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 109

Where is connection mirroring configured?

- A. It is an option within a TCP profile.
- B. It is an optional feature of each pool.
- C. It is not configured; it is default behavior.
- D. It is an optional feature of each virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

valuable answer

QUESTION 110

Which statement accurately describes the difference between two load-balancing modes specified as "member" and "node"?

- A. There is no difference; the two terms are referenced for backward compatibility purposes.
- B. When the load-balancing choice references "node", priority group activation is unavailable.
- C. Load-balancing options referencing "nodes" are available only when the pool members are defined for the "any" port.
- D. When the load-balancing choice references "node", the addresses' parameters are used to make the load-balancing choice rather than the

member's parameters.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 111

A site wishes to perform source address translation on packets from some clients but not others. The determination is not based on the client's IP address, but on the virtual servers their packets arrive on. What could best accomplish this goal?

- A. A SNAT for all addresses could be defined, and then disable the SNAT processing for select VLANs.
- B. Some virtual servers could be associated with SNAT pools and others not associated with SNAT pools.
- C. The decision to perform source address translation is always based on VLAN. Thus, the goal cannot be achieved.
- D. The decision to perform source address translation is always based on a client's address (or network). Thus, this goal cannot be achieved.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 112

Assume a client's traffic is being processed only by a NAT; no SNAT or virtual server processing takes place. Also assume that the NAT definition specifies a NAT address and an origin address while all other settings are left at their defaults. If a client were to initiate traffic to the NAT address, what changes, if any, would take place when the BIG-IP processes such packets?

- A. The source address would not change, but the destination address would be translated to the origin address.
- B. The destination address would not change, but the source address would be translated to the origin address.
- C. The source address would not change, but the destination address would be translated to the NAT's address.
- D. The destination address would not change, but the source address would be translated to the NAT's address.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 113

Which must be sent to the license server to generate a new license?

- A. the system's dossier
- B. the system's host name
- C. the system's base license
- D. the system's purchase order number

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

correct answer

QUESTION 114

What is the purpose of provisioning?

- A. Provisioning allows modules that are not licensed to be fully tested.
- B. Provisioning allows modules that are licensed be granted appropriate resource levels.
- C. Provisioning allows the administrator to activate modules in non-standard combinations.
- D. Provisioning allows the administrator to see what modules are licensed, but no user action is ever required.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 115

When initially configuring the BIG-IP system using the config utility, which two parameters can be set?(Choose two.)

- A. the netmask of the SCCP
- B. the IP address of the SCCP
- C. the port lockdown settings for the SCCP
- D. the netmask of the host via the management port
- E. the IP address of the host via the management port
- F. the port lockdown settings for the host via the management port

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 116

A site has six members in a pool. All of the servers have been designed, built, and configured with the same applications. It is known that each client's interactions vary significantly and can affect the performance of the servers. If traffic should be sent to all members on a regular basis, which load-balancing mode is most effective if the goal is to maintain a relatively even load across all servers?

- A. Ratio
- B. Priority
- C. Observed
- D. Round Robin

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 117

The incoming client IP address is 205.12.45.52. The last five connections have been sent to members C, D, A, B, B. The incoming client? IP address is 205.12.45.52. The last five connections have been sent to members C, D, A, B, B. Given the virtual server and pool definitions and the statistics shown in the graphic, which member will be used for the next connection?

VS_Web_Pool Settings		Web_Pool Parameters	
Destination:	172.160.22.3:80	Load Balancing:	Least Connections
Profiles:	TCP	Priority Group Activation:	Less Than 2
iRules:	None	Monitor:	None
Default Pool:	Web_Pool		
Persistence:	None		

Web_Pool Member Statistics and Settings					
Member	Member Ratio	Member Priority	Outstanding Requests	Current Connections	Status
A: 10.10.20.1:80	3	5	4	56	Unknown
B: 10.10.20.2:80	3	4	4	57	Unknown
C: 10.10.20.3:80	3	5	4	54	Offline
D: 10.10.20.4:80	1	3	1	2	Unknown
E: 10.10.20.5:80	1	1	1	2	Unknown

- A. 10.10.20.1:80
- B. 10.10.20.2:80
- C. 10.10.20.3:80
- D. 10.10.20.4:80
- E. 10.10.20.5:80

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is verified

QUESTION 118

A site has six members in a pool. Three of the servers are new and have more memory and a faster processor than the others. Assuming all other factors are equal and traffic should be sent to all members, which two loadbalancing methods are most appropriate? (Choose two.)

- A. Ratio
- B. Priority
- C. Observed

D. Round Robin

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 119

Which two can be a part of a pool's definition? (Choose two.)

- A. rule(s)
- B. profile(s)
- C. monitor(s)
- D. persistence type
- E. load-balancing mode

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 120

What is required for a virtual server to support clients whose traffic arrives on the internal VLAN and poolmembers whose traffic arrives on the external VLAN?

- A. That support is never available.
- B. The virtual server must be enabled for both VLANs.
- C. The virtual server must be enabled on the internal VLAN.
- D. The virtual server must be enabled on the external VLAN.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 121

A standard virtual server has been associated with a pool with multiple members. Assuming all other settings are left at their defaults, which statement is always true concerning traffic processed by the virtual server?

- A. The client IP address is unchanged between the client-side connection and the server-side connection.
- B. The server IP address is unchanged between the client-side connection and the server-side connection.
- C. The TCP ports used in the client-side connection are the same as the TCP ports server-side connection.
- D. The IP addresses used in the client-side connection are the same as the IP addresses used in the server-side connection.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 122

Monitors can be assigned to which three resources? (Choose three.)

- A. NATs
- B. pools
- C. iRules
- D. nodes
- E. SNATs
- F. pool members
- G. virtual servers

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 123

A site has assigned the ICMP monitor to all nodes and a custom monitor, based on the HTTP template, to a pool of web servers. The HTTP-based monitor is working in all cases. The ICMP monitor is failing for 2 of the pool members nodes. All other settings are default. What is the status of the pool members?

- A. All pool members are up since the HTTP-based monitor is successful.
- B. All pool members are down since the ICMP-based monitor is failing in some cases.
- C. The pool members whose nodes are failing the ICMP-based monitor will be marked disabled.
- D. The pool members whose nodes are failing the ICMP-based monitor will be marked unavailable.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 124

A site would like to ensure that a given web server's default page is being served correctly prior to sending it client traffic. They assigned the default HTTP monitor to the pool. What would the member status be if it sent an unexpected response to the GET request?

- A. The pool member would be marked offline (red).
- B. The pool member would be marked online (green).
- C. The pool member would be marked unknown (blue).
- D. The pool member would alternate between red and green.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 125

A site is load balancing to a pool of web servers. Which statement is true concerning BIG-IP's ability to verify whether the web servers are functioning properly or not?

- A. Web server monitors can test the content of any page on the server.
- B. Web server monitors always verify the contents of the index.html page.
- C. Web server monitors can test whether the server's address is reachable, but cannot test a page's content.
- D. Web server monitors can test the content of static web pages, but cannot test pages that would require the web server to dynamically build content.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is valid

QUESTION 126

The current status of a given pool is offline (red). Which condition could explain that state?

Assume the descriptions below include all monitors assigned for each scenario.

- A. No monitors are currently assigned to any pool, member or node.
- B. The pool has a monitor assigned to it, and none of the pool members passed the test.
- C. The pool has a monitor assigned to it, and only some of the pool's members passed the test.
- D. A monitor is assigned to all nodes and all nodes have passed the test. The pool's members have no specific monitor assigned to them.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 127

What is the purpose of floating self-IP addresses?

- A. to define an address that grants administrative access to either system at any time
- B. to define an address that allows either system to initiate communication at any time
- C. to define an address that allows network devices to route traffic via a single IP address
- D. to define an address that gives network devices greater flexibility in choosing a path to forward traffic

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 128

Which parameters are set to the same value when a pair of BIG-IP devices are synchronized?

- A. host names
- B. system clocks

- C. profile definitions
- D. VLAN fail-safe settings
- E. MAC masquerade addresses

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

answer is accurated

QUESTION 129

Which two statements are true concerning the default communication between a redundant pair of BIG-IP systems? (Choose two.)

- A. Synchronization occurs via a TCP connection using ports 683 and 684.
- B. Connection mirroring data is shared via a TCP connection using port 1028.
- C. Persistence mirroring data is shared via a TCP connection using port 1028.
- D. Connection mirroring data is shared through the serial fail-over cable unless network fail-over is enabled.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 130

Which two methods can be used to determine which BIG-IP is currently active? (Choose two.)

- A. The bigtop command displays the status.
- B. Only the active system's configuration screens are active.
- C. The status (Active/Standby) is embedded in the command prompt.
- D. The ifconfig -a command displays the floating addresses on the active system.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 131

As a part of the Setup Utility, the administrator sets the host name for the BIG-IP. What would be the result if the two systems in a redundant pair were set to the same host name?

- A. Host names do not matter in redundant pair communication.
- B. In a redundant pair, the two systems will always have the same host name. The parameter is synchronized between the systems.
- C. The first time the systems are synchronized the receiving system will be assigned the same self-IP addresses as the source system.
- D. When the administrator attempts to access the configuration utility using the host name, they will always connect to the active system.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 132

When network fail-over is enabled, which of the following is true?

- A. The fail-over cable status is ignored. Fail-over is determined by the network status only.
- B. Either a network failure or loss of voltage across the fail-over cable will cause a fail-over.
- C. A network failure will not cause a fail-over as long as there is a voltage across the fail-over cable.
- D. The presence or absence of voltage over the fail-over cable takes precedence over network fail-over.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 133

Where is connection mirroring configured?

- A. It is an option within a TCP profile.
- B. It is an optional feature of each pool.
- C. It is not configured; it is default behavior.
- D. It is an optional feature of each virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 134

Which statement is true regarding fail-over?

- A. Hardware fail-over is disabled by default.
- B. Hardware fail-over can be used in conjunction with network failover.
- C. If the hardware fail-over cable is disconnected, both BIG-IP devices will always assume the active role.
- D. By default, hardware fail-over detects voltage across the fail-over cable and monitors traffic across the internal VLAN.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 135

Where is persistence mirroring configured?

- A. It is always enabled.
- B. It is part of a pool definition.
- C. It is part of a profile definition.
- D. It is part of a virtual server definition.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 136

Assume the bigd daemon fails on the active system. Which three are possible results? (Choose three.)

- A. The active system will restart the bigd daemon and continue in active mode.

- B. The active system will restart the tmm daemon and continue in active mode.
- C. The active system will reboot and the standby system will go into active mode.
- D. The active system will fail-over and the standby system will go into active mode.
- E. The active system will continue in active mode but gather member and node state information from the standby system.

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 137

What is the purpose of MAC masquerading?

- A. to prevent ARP cache errors
- B. to minimize ARP entries on routers
- C. to minimize connection loss due to ARP cache refresh delays
- D. to allow both BIG-IP devices to simultaneously use the same MAC address

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

updated answer

QUESTION 138

Which process or system can be monitored by the BIG-IP system and used as a fail-over trigger in a redundant pair configuration?

- A. bandwidth utilization
- B. duplicate IP address
- C. CPU utilization percentage
- D. VLAN communication ability

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 139

Assuming there are open connections through an active system's NAT and a fail-over occurs, by default, what happens to those connections?

- A. All open connections will be lost.
- B. All open connections will be maintained.
- C. The "Mirror" option must be chosen on the NAT and the setting synchronized prior to the connection establishment.
- D. Long-lived connections such as Telnet and FTP will be maintained while short-lived connections such as HTTP will be lost.
- E. All open connections are lost, but new connections are initiated by the newly active BIG-IP, resulting in minimal client downtime.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

answer is updated

QUESTION 140

A virtual server is defined per the charts. The last five client connections were to members C, D, A, B, B. Given the conditions shown in the above graphic, if a client with IP address 205.12.45.52 opens a connection to the virtual server, which member will be used for the connection?

VS_Web_Pool Settings		Web_Pool Parameters	
Destination:	10.10.20.100:80	Load Balancing:	Least Connections
Profiles:	TCP, HTTP	Priority Group	
iRules:	None	Activation:	Less Than 2
Default Pool:	Web_Pool	Monitor:	Custom_HTTP
Persistence:	None		

Web_Pool Member Statistics and Settings					
Member	Member Ratio	Member Priority	Outstanding Requests	Current Connections	Status
A: 172.16.20.1:80	3	5	4	56	Unavailable
B: 172.16.20.2:80	3	4	4	42	Available
C: 172.16.20.3:80	3	5	4	54	Unavailable
D: 172.16.20.4:80	1	3	1	22	Available
E: 172.16.20.5:80	1	1	1	1	Available

- A. 172.16.20.1:80
- B. 172.16.20.2:80
- C. 172.16.20.3:80
- D. 172.16.20.4:80
- E. 172.16.20.5:80

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 141

Which three parameters could be used to determine whether a connection request will have the source address translated as the request is processed? (Choose three.)

- A. The client's router's IP address.
- B. The client's browser's preferred language.
- C. The client's IP netmask.
- D. The client's TCP port.
- E. The client's IP address.
- F. The client IP fragment offset.

Correct Answer: BDE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 142

What does the insert XForwarded option in an HTTP profile do?

- A. A BIG-IP self-IP is inserted in the source address field on the server-side connection.
- B. A BIG-IP self-IP is inserted in the source address field on the client-side connection.
- C. The client IP addresses are inserted into messages sent to remote syslog servers.
- D. The client IP addresses are inserted into HTTP header.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 143

When defining a load-balancing pool using the command line, if the load-balancing method is not specified, what is the result:

- A. The default load-balancing method would be used.
- B. The load-balancing method of the previous pool would be used.
- C. The system would prompt the user for a load-balancing method.
- D. An error would be displayed since no load-balancing method was specified.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 144

What occurs when a save-config command is issued?

- A. The current configuration files are backed up.
- B. The current configuration files are verified for syntax, then the running configuration is installed in memory.
- C. The current configuration files are loaded into memory.
- D. The current configuration files are saved into an archive format.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 145

How many events can be referenced in a given iRule?

- A. iRules are limited to one event, but a virtual server could be associated with multiple rules.
- B. iRules can have multiple events.
- C. Exactly one.
- D. iRules can have up to event if one is client-side and one is server-side.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 146

Which statement is true regarding OneConnect processing?

- A. The virtual server must have UDP profile.
- B. Server-side request can utilize existing client-side connections.
- C. The number of client connection is reduced.
- D. Client-side request can utilized existing server-side connections

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 147

Which statement concerning virtual servers is true?

- A. Virtual servers can keep idle server connections open indefinitely.
- B. Virtual servers can compress data between the BIG-IP and servers.
- C. Virtual servers cannot perform load balancing without performing address translation.
- D. Virtual servers can reuse connections between the BIG-IP and server for multiple HTTPGETs.
- E. Virtual server processing always translates the virtual server address to the address of the chosen pool member.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 148

Which is a potential result when a trunk is configured on a BIG-IP?

- A. No additional trunks can be configuration since each BIG-IP is limited to one trunk
- B. Packets flowing to the VLAN could arrive on any of the interfaces in the trunk
- C. Since any VLANs associated with the trunk are necessarily associated with multiple interfaces, the VLAN using the must use tagged packets.
- D. VLAN fail-safe is not available for any VLAN associated with any trunks.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 149

A site wishes to perform source address translation on packets arriving from the Internet for clients using some pools but not others. The determination is not based on the client's IP address, but on the pool they are loadbalanced to. What could best accomplish this goal?

- A. A SNAT for all addresses could be defined, and then disable the SNAT processing for select pools.
- B. The decision to perform source address translation is always based on VLAN. Thus, the goal cannot be achieved.
- C. For each virtual server, regardless their default load balancing pools, association with SNAT pools could vary dependent upon need.
- D. The decision to perform source address translation is always based on a client's address (or network). Thus, this goal cannot be achieved.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 150

Which two statements are true about SNATs? (Choose two.)

- A. SNATs are enabled on all VLANs, by default.
- B. SNATs can be configured within a Profile definition.
- C. SNATs can be configured within a Virtual Server definition.

D. SNAT's are enabled only on the VLAN where origin traffic arrives, by default

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

updated answers

QUESTION 151

A BIG-IP has two load balancing virtual servers at 150.150.10.10:80 and 150.150.10.10:443. The port 80 virtual server has SNAT automap configured. There is also a SNAT configured at 150.150.10.11 set for a source address range of 200.200.1.0 / 255.255.255.0. All other settings are at their default states. If a client with the IP address 200.200.1.1 sends a request to https://150.150.10.10, what is the source IP address when the associated packet is sent to the pool member?

- A. 200.200.1.1
- B. 150.150.10.11
- C. Floating self IP address on VLAN where the packet leaves the system
- D. Floating self IP address on VLAN where the packet arrives on the system

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 152

Which statement is true concerning SNATs using automap?

- A. Only specified self-IP addresses are used as automap addresses.
- B. SNATs using automap will translate all client addresses to an automap address.
- C. A SNAT using automap will preferentially use a floating self-IP over a non-floating self-IP.
- D. A SNAT using automap can be used to translate the source address of all outgoing traffic to the same address regardless of which VLAN the traffic is sent through.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 153

Which two statements are true about NATs? (Choose two.)

- A. NATs support UDP, TCP, and ICMP traffic.
- B. NATs can be configured with mirroring enabled or disabled.
- C. NATs provide a one-to-one mapping between IP addresses.
- D. NATs provide a many-to-one mapping between IP addresses.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 154

Which statement describes a typical purpose of iRules?

- A. iRules can be used to add individual control characters to an HTTP data stream.
- B. iRules can be used to update the timers on monitors as a server load changes.
- C. iRules can examine a server response and remove it from a pool if the response is unexpected.
- D. iRules can be used to look at client requests and server responses to choose a pool member to select for load balancing

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 155

A virtual server is listening at 10.10.1.100:80 and has the following iRule associated with it:
whenHTTP_REQUEST { if { [HTTP::header User-Agent] contains "MSIE" } { pool MSIE_pool } else { poolMozilla_pool } } If a user connects to http://10.10.1.100.html and their browser does not specify a User-Agent, which pool will receive the request?

- A. MSIE_pool
- B. Mozilla_pool
- C. None. The request will be dropped.

D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 156

You need to terminate client SSL traffic at the BIG-IP and also to persist client traffic to the same pool member based on a BIG-IP supplied cookie. Which four are profiles that would normally be included in the virtualserver's definition? (Choose four.)

- A. TCP
- B. HTTP
- C. HTTPS
- D. ClientSSL
- E. ServerSSL
- F. Cookie-Based Persistence

Correct Answer: ABDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 157

A site needs to terminate client HTTPS traffic at the BIG-IP and forward that traffic unencrypted. Which two are profile types that must be associated with such a virtual server? (Choose two.)

- A. TCP
- B. HTTP
- C. HTTPS
- D. ClientSSL
- E. ServerSSL

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 158

Which three statements describe a characteristic of profiles? (Choose three.)

- A. Default profiles cannot be created or deleted.
- B. Custom profiles are always based on a parent profile.
- C. A profile can be a child of one profile and a parent of another.
- D. All changes to parent profiles are propagated to their child profiles.
- E. While most virtual servers have at least one profile associated with them, it is not required.

Correct Answer: ABC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 159

A virtual server is defined using a source-address based persistence profile. The last five connections were A,B, C, A, C. Given the conditions shown in the graphic, if a client with IP address 205.12.45.52 opens aconnection to the virtual server, which member will be used for the connection?

All entries for the one virtual server and pool		
Persistence Values	Member	Age (Seconds)
200.10.0.0	10.10.20.1:80	63
201.12.0.0	10.10.20.3:80	43
153.15.0.0	10.10.20.2:80	76
205.12.0.0	10.10.20.4:80	300
195.64.0.0	10.10.20.3:80	22
198.22.0.0	10.10.20.5:80	176
214.77.0.0	10.10.20.1:80	43

Web_Pool Statistics					
Member	Member Ratio	Member Priority	Outstanding Layer 7 Requests	Connection Count	Status
A: 10.10.20.1:80	3	5	6	18	Available
B: 10.10.20.2:80	3	5	6	12	Available
C: 10.10.20.3:80	3	5	12	5	Disabled
D: 10.10.20.4:80	1	1	8	19	Offline
E: 10.10.20.5:80	1	1	4	9	Available

Virtual Server, Pool and Persistence Profile Settings					
VS_Web_Pool Settings		Web_Pool Settings		Source Persist Settings	
Destination	172.160.22.3:80	Load Balancing	Least Connectons	Mode	Source Address
Profile(s)	TCP	Priority Activation	Less than 2	Netmask	255.255.0.0
Pool	Web_Pool	Montitor	Done	Timeout	360 seconds
iRules	None				
Persistence	Source_Persist				

examsheets.com

- A. 10.10.20.1:80
- B. 10.10.20.2:80
- C. 10.10.20.3:80
- D. 10.10.20.4:80
- E. 10.10.20.5:80

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 160

How is persistence configured?

- A. Persistence is an option within each pool's definition.
- B. Persistence is a profile type; an appropriate profile is created and associated with virtual server.
- C. Persistence is a global setting; once enabled, load-balancing choices are superseded by the persistence method that is specified.
- D. Persistence is an option for each pool member. When a pool is defined, each member's definition includes the option for persistence.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 161

Assume a virtual server is configured with a ClientSSL profile. What would the result be if the virtual server's destination port were not 443?

- A. SSL termination could not be performed if the virtual server's port was not port 443.
- B. Virtual servers with a ClientSSL profile are always configured with a destination port of 443.
- C. As long as client traffic was directed to the alternate port, the virtual server would work as intended.
- D. Since the virtual server is associated with a ClientSSL profile, it will always process traffic sent to port 443.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 162

A BIG-IP has a virtual server at 150.150.10.10:80 with SNAT automap configured. This BIG-IP also has a SNAT at 150.150.10.11 set for a source address range of 200.200.1.0 / 255.255.255.0. All other settings are at their default states. If a client with the IP address 200.200.1.1 sends a request to the virtual server, what is the source IP address when the associated packet is sent to the pool member?

- A. 200.200.1.1
- B. 150.150.10.11

- C. Floating self IP address on VLAN where the packet leaves the system
- D. Floating self IP address on VLAN where the packet arrives on the system

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 163

Which IP address will the client address be changed to when SNAT automap is specified within a Virtual Server configuration?

- A. The floating self IP address on the VLAN where the packet leaves the system.
- B. The floating self IP address on the VLAN where the packet arrives on the system.
- C. It will alternate between the floating and non-floating self IP address on the VLAN where the packet leaves the system so that port exhaustion is avoided.
- D. It will alternate between the floating and non-floating self IP address on the VLAN where the packet arrives on the system so that port exhaustion is avoided.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 164

A virtual server at 10.10.1.100:80 has the rule listed below applied. when HTTP_REQUEST { if {[HTTP::uri] ends_with "htm" } { pool pool1 } elseif {[HTTP::uri] ends_with "xt" } { pool pool2 } If a user connects to http://10.10.1.100/foo.txt which pool will receive the request?

- A. pool1
- B. pool2
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 165

Which statement is true concerning iRule events?

- A. All iRule events relate to HTTP processes.
- B. All client traffic has data that could be used to trigger iRule events.
- C. All iRule events are appropriate at any point in the client-server communication.
- D. If an iRule references an event that doesn't occur during the client's communication, the client's connection will be terminated prematurely.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 166

Which three iRule events are likely to be seen in iRules designed to select a pool for load balancing? (Choose 3)

- A. CLIENT_DATA
- B. SERVER_DATA
- C. HTTP_REQUEST
- D. HTTP_RESPONSE
- E. CLIENT_ACCEPTED
- F. SERVER_SELECTED
- G. SERVER_CONNECTED

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 167

Which event is always triggered when a client initially connects to a virtual server configured with an HTTP profile?

- A. HTTP_DATA

- B. CLIENT_DATA
- C. HTTP_REQUEST
- D. CLIENT_ACCEPTED

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 168

A virtual server is listening at 10.10.1.100:80 and has the following iRule associated with it:
when HTTP_REQUEST { if {[HTTP::uri] ends_with "txt" } { pool pool1 } elseif {[HTTP::uri] ends_with "php" } { pool pool2 } If a user connects to http://10.10.1.100/foo.html, which pool will receive the request?

- A. pool1
- B. pool2
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

accurate answer

QUESTION 169

A virtual server is listening at 10.10.1.100:any and has the following iRule associated with it:
when CLIENT_ACCEPTED { if {[TCP::local_port] equals 80 } { pool pool1 } elseif {[TCP::local_port] equals 443 } { pool pool2 } If a user connects to 10.10.1.100 and port 22, which pool will receive the request?

- A. pool1
- B. pool2
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 170

Which statement is true about the synchronization process, as performed by the Configuration Utility or by typing `b config sync all`?

- A. The process should always be run from the standby system.
- B. The process should always be run from the system with the latest configuration.
- C. The two `/config/bigip.conf` configuration files are synchronized (made identical) each time the process is run.
- D. Multiple files, including `/config/bigip.conf` and `/config/bigip_base.conf`, are synchronized (made identical) each time the process is run.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 171

Which statement is true concerning the default communication between a redundant pair of BIG-IP devices?

- A. Communication between the systems cannot be effected by port lockdown settings.
- B. Data for both connection and persistence mirroring are shared through the same TCP connection.
- C. Regardless of the configuration, some data is communicated between the systems at regular intervals.
- D. Connection mirroring data is shared through the serial fail-over cable unless network fail-over is enabled.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 172

When upgrading a BIG-IP redundant pair, what happens when one system has been updated but the other has not?

- A. Synching should not be performed.
- B. The first system to be updated will assume the Active role.

- C. This is not possible since both systems are updated simultaneously.
- D. The older system will issue SNMP traps indicating a communication error with the partner.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 173

When using the setup utility to configure a redundant pair, you are asked to provide a "Failover Peer IP". Which address is this?

- A. an address of the other system in its management network
- B. an address of the other system in a redundant pair configuration
- C. an address on the current system used to listen for fail-over messages from the partner BIG- IP
- D. an address on the current system used to initiate mirroring and network fail-over heartbeat messages

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

specified answer

QUESTION 174

Which two statements describe differences between the active and standby systems? (Choose two.)

- A. Monitors are performed only by the active system.
- B. Fail-over triggers only cause changes on the active system.
- C. Virtual server addresses are hosted only by the active system.
- D. Configuration changes can only be made on the active system.
- E. Floating self-IP addresses are hosted only by the active system.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 175

Assuming other fail-over settings are at their default state, what would occur if the fail-over cable were to be disconnected for five seconds and then reconnected?

- A. As long as network communication is not lost, no change will occur.
- B. Nothing. Fail-over due to loss of voltage will not occur if the voltage is lost for less than ten seconds.
- C. When the cable is disconnected, both systems will become active. When the voltage is restored, unit two will revert to standby mode.
- D. When the cable is disconnected, both systems will become active. When the voltage is restored, both systems will maintain active mode.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 176

Where is persistence mirroring configured?

- A. It is always enabled.
- B. It is part of a pool definition.
- C. It is part of a profile definition.
- D. It is part of a virtual server definition.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 177

Given that VLAN fail-safe is enabled on the external VLAN and the network that the active BIG- IP's external VLAN is connected to has failed, which statement is always true about the results?

- A. The active system will note the failure in the HA table.
- B. The active system will reboot and the standby system will go into active mode.
- C. The active system will fail-over and the standby system will go into active mode.
- D. The active system will restart the traffic management module to eliminate the possibility that BIG-IP is the cause for the network failure.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 178

Where is connection mirroring configured?

- A. It is an option within a TCP profile.
- B. It is an optional feature of each pool.
- C. It is not configured; it is default behavior.
- D. It is an optional feature of each virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 179

Assuming there are open connections through an active system's virtual servers and a fail-over occurs, by default, what happens to the connections?

- A. All open connections are lost.
- B. All open connections are maintained.
- C. When persistence mirroring is enabled, open connections are maintained even if a fail-over occurs.
- D. Long-lived connections such as Telnet and FTP are maintained, but short-lived connections such as HTTP are lost.
- E. All open connections are lost, but new connections are initiated by the newly active BIG-IP, resulting in minimal client downtime.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 180

How is MAC masquerading configured?

- A. Specify the desired MAC address for each VLAN for which you want this feature enabled.
- B. Specify the desired MAC address for each self-IP address for which you want this feature enabled.
- C. Specify the desired MAC address for each VLAN on the active system and synchronize the systems.
- D. Specify the desired MAC address for each floating self-IP address for which you want this feature enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 181

Which action will take place when a failover trigger is detected by the active system?

- A. The active device will take the action specified for the failure.
- B. The standby device also detects the failure and assumes the active role.
- C. The active device will wait for all connections to terminate and then fail-over.
- D. The standby device will begin processing virtual servers that have failed, but the active device will continue servicing the functional virtual servers.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 182

Assuming that systems are synchronized, which action could take place if the fail-over cable is connected correctly and working properly, but the systems cannot communicate over the network due to external network problems?

- A. If network fail-over is enabled, the standby system will assume the active mode.
- B. Whether or not network fail-over is enabled, the standby system will stay in standby mode.
- C. Whether or not network fail-over is enabled, the standby system will assume the active mode.
- D. If network fail-over is enabled, the standby system will go into active mode but only until the network recovers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 183

A virtual server is defined per the charts. The last five client connections were to members C, D, A, B, B. Given the conditions shown in the above graphic, if a client with IP address 205.12.45.52 opens a connection to the virtual server, which member will be used for the connection?

VS_Web_Pool Settings		Web_Pool Parameters	
Destination:	10.10.20.100:80	Load Balancing	Least Connections
Profiles:	TCP, HTTP	Priority Group	
iRules:	None	Activation:	Less Than 2
Default Pool:	Web_Pool	Monitor:	Custom_HTTP
Persistence:	None		

Web_Pool Member Statistics and Settings					
Member	Member Ratio	Member Priority	Outstanding Requests	Current Connections	Status
A: 172.16.20.1:80	3	5	4	56	Unavailable
B: 172.16.20.2:80	3	4	4	42	Available
C: 172.16.20.3:80	3	5	4	54	Unavailable
D: 172.16.20.4:80	1	3	1	22	Available
E: 172.16.20.5:80	1	1	1	18	Available

- A. 172.16.20.1:80
- B. 172.16.20.2:80
- C. 172.16.20.3:80
- D. 172.16.20.4:80
- E. 172.16.20.5:80

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 184

Which cookie persistence method requires the fewest configuration changes on the web servers to be implemented correctly?

- A. insert
- B. rewrite
- C. passive
- D. session

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is appropriated

QUESTION 185

Which statement is true concerning cookie persistence?

- A. Cookie persistence allows persistence independent of IP addresses.
- B. Cookie persistence allows persistence even if the data are encrypted from client to pool member.
- C. Cookie persistence uses a cookie that stores the virtual server, pool name, and member IP address in cleartext.
- D. If a client's browser accepts cookies, cookie persistence will always cause a cookie to be written to the client's file system.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

verified answer

QUESTION 186

Assume a virtual server has a ServerSSL profile. What SSL certificates are required on the pool members?

- A. No SSL certificates are required on the pool members.
- B. The poolmembers SSL certificates must only exist.
- C. The poolmembers SSL certificates must be issued from a certificate authority.
- D. The poolmembers SSL certificates must be created within the company hosting the BIG-IPs.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 187

Assume a virtual server is configured with a ClientSSL profile. What would the result be if the virtual server's destination port were not 443?

- A. SSL termination could not be performed if the virtual server's port was not port 443.
- B. Virtual servers with a ClientSSL profile are always configured with a destination port of 443.
- C. As long as client traffic was directed to the alternate port, the virtual server would work as intended.
- D. Since the virtual server is associated with a ClientSSL profile, it will always process traffic sent to port 443.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 188

Which is an advantage of terminating SSL communication at the BIG-IP rather than the ultimate web server?

- A. Terminating SSL at the BIG-IP can eliminate SSL processing at the web servers.
- B. Terminating SSL at the BIG-IP eliminates all un-encrypted traffic from the Internal network.
- C. Terminating SSL at the BIG-IP eliminates the need to purchase SSL certificates from a certificate authority.
- D. Terminating SSL at the BIG-IP eliminates the need to use SSL acceleration hardware anywhere in the network.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 189

Assume a client's traffic is being processed only by a NAT; no SNAT or virtual server processing takes place.

Also assume that the NAT definition specifies a NAT address and an origin address while all other settings are left at their defaults. If the origin server

were to initiate traffic via the BIG-IP, what changes, if any, would takeplace when the BIG-IP processes such packets?

- A. The BIG-IP would drop the request since the traffic didnt arrive destined to the NAT address.
- B. The source address would not change, but the destination address would be changed to the NAT address.
- C. The source address would be changed to the NAT address and destination address would be leftunchanged.
- D. The source address would not change, but the destination address would be changed to a self- IP of theBIG-IP.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 190

Which event is always triggered when the client sends data to a virtual server using TCP?

- A. HTTP_DATA
- B. CLIENT_DATA
- C. HTTP_REQUEST
- D. VS_CONNECTED

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 191

A virtual server is listening at 10.10.1.100:any and has the following iRule associated with it:

whenCLIENT_ACCEPTED { if {[TCP::local_port] equals 21 } { pool ftp pool } else if {[TCP::local_port]equals 23 } { pool telnet pool } If a user connects to 10.10.1.100 and port 22, which pool will receive therequest?

- A. ftp pool
- B. telnet pool
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 192

When configuring a Virtual Server to use an iRule with an HTTP_REQUEST event, which lists required steps in a proper order to create all necessary objects?

- A. create profiles, create the iRule, create required pools, create the Virtual Server
- B. create the Virtual Server, create required pools, create the iRule, edit the Virtual Server
- C. create a custom HTTP profile, create required pools, create the Virtual Server, create the iRule
- D. create required pools, create a custom HTTP profile, create the iRule, create the Virtual Server

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 193

Which statement is true concerning a functional iRule?

- A. iRules use a proprietary syntax language.
- B. iRules must contain at least one event declaration.
- C. iRules must contain at least one conditional statement.
- D. iRules must contain at least one pool assignment statement.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 194

On a standalone BIG-IP ASM system, which of the following configuration is valid?

- A. Pool named http_pool with 1 pool member, no persistence, and no load balancing method

- B. Pool named http_pool with 3 pool members, cookie persistence, and ratio load balancing method
- C. Pool named http_pool with 2 pool members, source IP persistence, and least connections load balancing method
- D. Pool named http_pool with 3 pool members, cookie persistence, and least connections load balancing method

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 195

A user is building a security policy using the Deployment Wizard and the Rapid Deployment application template. By default, which settings will be applied to the security policy? (Choose 3)

- A. Data Guard will be enabled
- B. The enforcement mode will be set to transparent
- C. The encoding language will be set to auto detect
- D. Wildcard tightening will be enabled on file types and parameters
- E. The attack signature set applied will be Generic Detection Signatures

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

valid answers

QUESTION 196

Which of the following violations cannot be learned by Traffic Learning?

- A. RFC violations
- B. File type length violations
- C. Attack signature violations
- D. Meta character violations on a specific parameter.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

answer is accurate

QUESTION 197

What is the purpose of the IP addresses listed in the Trusted IP section when using Policy Builder?

- A. Incoming requests with these IP addresses will never get blocked by BIG-IP ASM.
- B. Incoming requests with these IP addresses will not be taken into account as part of the learning process, they will be allowed to do anything.
- C. Incoming requests with these IP addresses will automatically be accepted into the security policy, Policy Builder will validate that future requests with this traffic will not create a violation.
- D. Incoming requests with these IP addresses will be used by Policy Builder to create an alternate more advanced security policy, this additional policy will not be enabled unless forced by the administrator.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 198

Which of the following protocols can be protected by Protocol Security Manager? (Choose 3)

- A. FTP
- B. SSH
- C. HTTP
- D. SMTP
- E. Telnet

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 199

Which of the following user roles have access to make changes to security policies? (Choose 2)

- A. Guest

- B. Operator
- C. Administrator
- D. Web Application Security Editor

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 200

Which of the following is correct concerning HTTP classes?

- A. A single web application can be used by several HTTP classes.
- B. A virtual server can only have one HTTP class associated with it.
- C. A single ASM enabled HTTP class can be used by multiple virtual servers.
- D. Each ASM enabled HTTP class can have several active security policies associated with it.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 201

Which of the following are methods BIG-IP ASM utilizes to mitigate web scraping vulnerabilities? (Choose 2)

- A. Monitors mouse and keyboard events
- B. Detects excessive failures to authenticate
- C. Injects JavaScript code on the server side
- D. Verifies the client supports JavaScript and cookies

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 202

When choosing Fundamental as the Policy Builder security policy type, BIG-IP ASM will learn and enforce the following components? (Choose 2)

- A. Attack signatures
- B. Global parameters
- C. HTTP protocol compliance
- D. URLs and meta characters

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

valid answers

QUESTION 203

The default staging-tightening period for attack signatures and wildcard entities is?

- A. 5 days
- B. 7 days
- C. 10 days
- D. 30 days

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 204

Which of the following platforms support both standalone and modular BIG-IP ASM implementations? (Choose 2)

- A. 3900
- B. 6800
- C. 6900
- D. 8800

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 205

Which must be sent to the license server to generate a new license?

- A. the system's dossier
- B. the system's host name
- C. the system's base license
- D. the system's purchase order number

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 206

What is the purpose of provisioning?

- A. Provisioning allows modules that are not licensed to be fully tested.
- B. Provisioning allows modules that are licensed be granted appropriate resource levels.
- C. Provisioning allows the administrator to activate modules in non-standard combinations.
- D. Provisioning allows the administrator to see what modules are licensed, but no user action is ever required.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 207

The incoming client IP address is 195.64.45.52 and the last five connections have been sent to members A, C,E, D and B. The incoming client IP address is 195.64.45.52 and the last five connections have been sent to members A, C, E, D and B. Given the virtual server, pool, and persistence definitions and statistics shown in the above graphic, which member will be used for the next connection?

Persistence Table		
All entries for the one virtual server and pool		
Persistence Values	Member	Age (Seconds)
200.10.0.0	10.10.20.1:80	63
201.12.0.0	10.10.20.3:80	43
153.15.0.0	10.10.20.2:80	76
205.12.0.0	10.10.20.4:80	300
195.64.0.0	10.10.20.3:80	22
198.22.0.0	10.10.20.5:80	176
214.77.0.0	10.10.20.1:80	43

Web_PoolStatistics					
Member	Member Ratio	Member Priority	Outstanding Layer 7 Requests	Connection Count	Status
10.10.20.1:80	3	5	6	18	Available
10.10.20.2:80	3	5	6	12	Available
10.10.20.3:80	3	5	12	5	Disabled
10.10.20.4:80	1	1	8	19	Offline
10.10.20.5:80	1	1	4	9	Available

Virtual Server, Pool and Persistence Profile Settings					
VS_Web_Pool Settings		Web_Pool Settings		Source Persist Settings	
Destination	172.160.22.3:80	Load Balancing	Least Connections	Mode	Source Address
Profile(s)	TCP	Priority Activation	Less than 2	Netmask	255.255.0.0
Pool	Web_Pool	Monitor	Done	Timeout	360 seconds
iRules	None				
Persistence	Source_Persist				

examsheets.com

- A. 10.10.20.1:80
- B. 10.10.20.2:80
- C. 10.10.20.3:80
- D. 10.10.20.4:80
- E. 10.10.20.5:80
- F. It cannot be determined with the information given.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 208

How is persistence configured?

- A. Persistence is an option within each pool's definition.
- B. Persistence is a profile type; an appropriate profile is created and associated with virtual server.
- C. Persistence is a global setting; once enabled, load-balancing choices are superseded by the persistence method that is specified.
- D. Persistence is an option for each pool member. When a pool is defined, each member's definition includes the option for persistence.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 209

Assume a virtual server has a ServerSSL profile. What SSL certificates are required on the BIG-IP?

- A. No SSL certificates are required on the BIG-IP.
- B. The BIG-IP's SSL certificates must only exist.
- C. The BIG-IP's SSL certificates must be issued from a certificate authority.
- D. The BIG-IP's SSL certificates must be created within the company hosting the BIG-IPs.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 210

Which VLANs must be enabled for a SNAT to perform as desired (translating only desired packets)?

- A. The SNAT must be enabled for all VLANs.

- B. The SNAT must be enabled for the VLANs where desired packets leave the BIG-IP.
- C. The SNAT must be enabled for the VLANs where desired packets arrive on the BIG-IP.
- D. The SNAT must be enabled for the VLANs where desired packets arrive and leave the BIG- IP.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 211

A BIG-IP has a virtual server at 150.150.10.10:80 with SNAT automap configured. This BIG-IP also has a SNAT at 150.150.10.11 set for a source address range of 200.200.1.0 / 255.255.255.0. All other settings are at their default states. If a client with the IP address 200.200.1.1 sends a request to the virtual server, what is the source IP address when the associated packet is sent to the pool member?

- A. 200.200.1.1
- B. 150.150.10.11
- C. Floating self IP address on VLAN where the packet leaves the system
- D. Floating self IP address on VLAN where the packet arrives on the system

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 212

Which IP address will the client address be changed to when SNAT automap is specified within a VirtualServer configuration?

- A. The floating self IP address on the VLAN where the packet leaves the system.
- B. The floating self IP address on the VLAN where the packet arrives on the system.
- C. It will alternate between the floating and non-floating self IP address on the VLAN where the packet leaves the system so that port exhaustion is avoided.
- D. It will alternate between the floating and non-floating self IP address on the VLAN where the packet arrives on the system so that port exhaustion is avoided.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 213

A virtual server at 10.10.1.100:80 has the rule listed below applied. when HTTP_REQUEST { if {[HTTP::uri]ends_with "htm" } { pool pool1 } elseif {[HTTP::uri] ends_with "xt" } { pool pool2 } If a user connects to http://10.10.1.100/foo.txt which pool will receive the request?

- A. pool1
- B. pool2
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 214

Which statement is true concerning iRule events?

- A. All iRule events relate to HTTP processes.
- B. All client traffic has data that could be used to trigger iRule events.
- C. All iRule events are appropriate at any point in the client-server communication.
- D. If an iRule references an event that doesn't occur during the client's communication, the client's connection will be terminated prematurely.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

answer is corrected

QUESTION 215

The current status of a given pool member is unknown? Which condition could explain that state? The current status of a given pool member is unknown? Which condition could explain that state?

- A. The member has no monitor assigned to it.

- B. The member has a monitor assigned to it and the most recent monitor was successful.
- C. The member has a monitor assigned to it and the monitor did not succeed during the most recent timeout period.
- D. The member's node has a monitor assigned to it and the monitor did not succeed during the most recent timeout period.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 216

The ICMP monitor has been assigned to all nodes. In addition, all pools have been assigned custom monitors. If a pool is marked available?The ICMP monitor has been assigned to all nodes. In addition, all pools have been assigned custom monitors. If a pool is marked available (green) which situation is sufficient to cause this?

- A. All of the pool member nodes are responding to the ICMP monitor as expected.All of the pool member nodes are responding to the ICMP monitor as expected.
- B. Less than 50% of the pool member nodes responded to the ICMP echo request.Less than 50% of the pool member nodes responded to the ICMP echo request.
- C. All of the members of the pool have had their content updated recently and their responses no longer match the monitor receiveAll of the members of the pool have had their content updated recently and their responses no longer match the monitor receive rule.
- D. Over 25% of the pool members have had their content updated and it no longer matches the receive rule of the custom monitor.Over 25% of the pool members have had their content updated and it no longer matches the receive rule of the custom monitor.
The other respond as expected.The other respond as expected.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 217

Generally speaking, should the monitor templates be used as production monitors or should they be customized prior to use?

- A. Most templates, such as http and tcp, are as effective as customized monitors.
- B. Monitor template customization is only a matter of preference, not an issue of effectiveness or performance.
- C. Most templates, such as https, should have the receive rule customized to make the monitor more robust.
- D. While some templates, such as ftp, must be customized, those that can be used without modification are not improved by specific changes.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 218

You have a pool of servers that need to be tested. All of the servers but one should be tested every 10 seconds, but one is slower and should only be tested every 20 seconds. How do you proceed?

- A. It cannot be done. All monitors test every five seconds.
- B. It can be done, but will require assigning monitors to each pool member.
- C. It cannot be done. All of the members of a pool must be tested at the same frequency.
- D. It can be done by assigning one monitor to the pool and a different monitor to the slower pool member.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 219

When can a single virtual server be associated with multiple profiles?

- A. Never. Each virtual server has a maximum of one profile.
- B. Often. Profiles work on different layers and combining profiles is common.
- C. Rarely. One combination, using both the TCP and HTTP profile does occur, but it is the exception.
- D. Unlimited. Profiles can work together in any combination to ensure that all traffic types are supported in a given virtual server.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 220

A site needs a virtual server that will use an iRule to parse HTTPS traffic based on HTTP header values. Which two profile types must be associated

with such a virtual server? (Choose two.)

- A. TCP
- B. HTTP
- C. HTTPS
- D. ServerSSL

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 221

You have created a custom profile named TEST2. The parent profile of TEST2 is named TEST1. If additional changes are made to TEST1, what is the effect on TEST2?

- A. All changes to TEST1 are propagated to TEST2.
- B. Some of the changes to TEST1 may propagate to TEST2.
- C. Changes to TEST1 cannot affect TEST2 once TEST2 is saved.
- D. When TEST1 is changed, the administrator is prompted and can choose whether to propagate changes to TEST2.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 222

A OneConnect profile is applied to a virtual server. The LTM Specialist would like the client source IP addresses within the 10.10.10.0/25 range to reuse an existing server side connection.

Which OneConnect profile source mask should the LTM Specialist use?

- A. 0.0.0.0
- B. 255.255.255.0
- C. 255.255.255.128
- D. 255.255.255.224

E. 255.255.255.255

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

accurate answer

QUESTION 223

An LTM device is load balancing telnet and ssh applications in a client/server environment experiencing significant packet delay.

Which setting in the TCP profile should reduce the amount of packet delay?

- A. disable Bandwidth Delay
- B. disable Nagle's Algorithm
- C. enable Proxy Maximum Segment
- D. increase Maximum Segment Retransmissions

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 224

An LTM device is load balancing SIP traffic. An LTM Specialist notices that sometimes the SIP request is being load balanced to the same server as the initial connection. Which setting in the UDP profile will make the LTM device more evenly distribute the SIP traffic?

- A. Enable Datagram LB
- B. Disable Datagram LB
- C. Set Timeout to Indefinite
- D. Set Timeout to Immediate

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 225

Internet clients connecting to a virtual server to download a file are experiencing about 150 ms of latency and no packet loss.

Which built-in client-side TCP profile provides the highest throughput?

- A. tcp
- B. tcp-legacy
- C. tcp-lan-optimized
- D. tcp-wan-optimized

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 226

Windows PC clients are connecting to a virtual server over a high-speed, low-latency network with no packet loss.

Which built-in client-side TCP profile provides the highest throughput for HTTP downloads?

- A. tcp
- B. tcp-legacy
- C. tcp-lan-optimized
- D. tcp-wan-optimized

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 227

Users are experiencing low throughput when downloading large files over a high-speed WAN connection. Extensive packet loss was found to be an issue but CANNOT be eliminated.

Which two TCP profile settings should be modified to compensate for the packet loss in the network? (Choose two.)

- A. slow start
- B. proxy options
- C. proxy buffer low
- D. proxy buffer high
- E. Nagle's algorithm

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 228

An LTM Specialist is working with an LTM device configured with 10 virtual servers on the same domain with a different key/cert pair per virtual. For example www.example.com; ftp.example.com; ssh.example.com; ftps.example.com.

What should the LTM Specialist do to reduce the number of objects on the LTM device?

- A. create a 0 port virtual server and have it answer for all protocols
- B. create a 0.0.0.0:0 virtual server thus eliminating all virtual servers
- C. create a transparent virtual server thus eliminating all virtual servers
- D. create a wildcard certificate and use it on all *.example.com virtual servers

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 229

The pool members are serving up simple static web content.

The current virtual server configuration is given as follows:

```
tmsh list ltm virtual simple
ltm virtual simple {
destination 10.10.10.10:80
ip-protocol tcp
mask 255.255.255.255
```



```

profiles {
  http {}
  httpcompression {}
  oneconnect {}
  tcp {}
}
snat automap
vlans-disabled
}

tmsh list ltm pool simple_pool
ltm pool simple_pool {
  members {
    10.10.10.11:80 {
      address 10.10.10.11 }
    10.10.10.12:80 {
      address 10.10.10.12 }
    10.10.10.12:80 {
      address 10.10.10.13 }
    }
  }
}

```

Which three objects in the virtual server configuration can be removed without disrupting functionality of the virtual server? (Choose three.)

- A. tcp
- B. http
- C. oneconnect
- D. snat automap
- E. httpcompression

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 230

An LTM device is running BIG-IP v10.2.0 software. The LTM Specialist is tasked with upgrading the LTM device to BIG-IP v11.2.0 HF1. The LTM Specialist starts the upgrade process by selecting the uploaded Hotfix and installing to an unused volume. After 10 minutes, the LTM Specialist checks the status of the upgrade process and notices that the process is stalled at 0%.

What should the LTM Specialist verify?

- A. the selected volume has sufficient space available
- B. the base software version exists on the LTM device
- C. the LTM device has been restarted into maintenance mode
- D. the LTM device has an available Internet connection via the management interface

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 231

A stand-alone LTM device is to be paired with a second LTM device to create an active/standby pair. The current stand-alone LTM device is in production and has several VLANs with floating IP addresses configured. The appropriate device service clustering (DSC) configurations are in place on both LTM devices.

Which two non-specific DSC settings should the LTM Specialist configure on the second LTM device to ensure no errors are reported when attempting to synchronize for the first time? (Choose two.)

- A. pools
- B. VLANs
- C. default route
- D. self IP addresses

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 232

What is the correct command to reset an LTM device to its default settings?

- A. tmsh reset-all default
- B. tmsh set /sys config defaults
- C. tmsh load /sys config default

D. tmsh /util bigpipe reset-factory-defaults

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 233

In which file would the LTM Specialist find virtual server configurations?

- A. bigip.conf
- B. bigip_sys.conf
- C. bigip_base.conf
- D. profile_base.conf

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 234

When re-licensing an LTM device from the command line interface, which tmsh command should the LTM Specialist use to generate the required information to provide on the F5 licensing portal?

- A. tmsh run /util get-dossier
- B. tmsh generate /sys dossier
- C. tmsh list /sys registration-key
- D. tmsh install /sys license registration-key

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 235

A device on the network is configured with the same IP address as the management address of the active LTM device, causing the management GUI to be inaccessible.

Which two methods should the LTM Specialist use to access the LTM device in order to change the management IP address? (Choose two.)

- A. Connect via ssh to the AOM IP address.
- B. Connect via ssh to the management address.
- C. Connect to the LTM device via serial connection.
- D. Connect a monitor and keyboard to the LTM device.
- E. Connect via ssh to the standby unit and connect via ssh across the serial link between the devices.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 236

The LTM Specialist is in the process of creating a USB boot drive for the purpose of restoring the BIG-IP software to an LTM device. A separate LTM device has been selected for the purpose of creating the USB boot drive. The BIG-IP software ISO has already been uploaded and mounted on the separate LTM device.

Which command should the LTM Specialist use to trigger the LTM device to install the BIG-IP software to the USB boot drive?

- A. tmsh
- B. install
- C. mkdisk
- D. bigip_software_create

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 237

An LTM Specialist has installed a hotfix that updated the SCCP firmware package.

Which command will ensure that the host subsystem and SCCP reboot?

- A. reboot
- B. full_box_reboot
- C. shutdown -r now
- D. The reboot should be initiated via the HTTPS administration GUI.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 238

Which procedure should an LTM Specialist follow to move a configuration from a 1500 to a 1600 hardware platform during an upgrade?

- A. tmsh save sys config file filename.scf
copy the file from the /var/local/scf directory from one device to the other tmsh load sys config file filename.scf
- B. tmsh save sys backup file filename.scf
copy the file from the /var/local/scf directory from one device to the other tmsh load sys backup file filename.scf
- C. tmsh save sys backup file filename.scf
copy the file from the /var/local/ucs directory from one device to the other tmsh load sys backup file filename.scf
- D. tmsh save sys config file filename.scf
copy the file from the /var/local/ucs directory from one device to the other tmsh load sys config file filename.scf

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 239

What is the recommended procedure for upgrading a major TMOS release on a BIG-IP platform?

- A.
 1. Renew the device license.
 2. Take a configuration backup.
 3. Reboot the device to the non-active volume.
 4. Upload the device code.
 5. Install device code to the current volume.
- B.
 1. Take a configuration backup.

- 2. Upload the device code.
 - 3. Install device code to the non-active volume.
 - 4. Reboot the device to the non-active volume.
 - 5. Renew the device license.
- C. 1. Renew the device license.
- 2. Take a configuration backup.
 - 3. Upload the device code.
 - 4. Install device code to the non-active volume.
 - 5. Reboot the device to the non-active volume.
- D. 1. Take a configuration backup.
- 2. Reboot the device to the non-active volume.
 - 3. Renew the device license.
 - 4. Upload the device code.
 - 5. Install device code to the current volume.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 240

An LTM Specialist uploaded new releases .iso and .md5 files titled "BIGIP-FILENAME" via the GUI.

Which commands are run via the command line from the root directory to verify the integrity of the new .iso file?

- A. `cd /var/shared/images`
`md5sum --check BIGIP-FILENAME.iso`
- B. `cd /shared/images`
`md5sum --check BIGIP-FILENAME.iso`
- C. `cd /var/shared/images`
`md5sum --check BIGIP-FILENAME.iso.md5`
- D. `cd /shared/images`
`md5sum --check BIGIP-FILENAME.iso.md5`

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 241

A virtual server for a set of web services is constructed on an LTM device. The LTM Specialist has created an iRule and applied this iRule to the virtual server:

```
when HTTP_REQUEST {  
  switch [HTTP::uri] {  
    "/ws1/ws.jsp" {  
      log local0. "[HTTP::uri]-Redirected to JSP Pool"  
      pool JSP  
    }  
    default { log local0. "[HTTP::uri]-Redirected to Non-JSP Pool" pool NonJSP  
  }  
}
```

However, the iRule is NOT behaving as expected. Below is a snapshot of the log:

```
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/WS.jsp-Redirected to Non-JSP Pool  
/ws1/WS.jsp-Redirected to Non-JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/ws1/ws.jsp-Redirected to Non-JSP Pool
```

What should the LTM Specialist do to resolve this?

- A. Use the following. switch -lc [HTTP::uri]
- B. Use the following. switch [string tolower [HTTP::uri]]
- C. Set the "Case Sensitivity" option of each member to "None".
- D. Select the "Process Case-Insensitivity" option for the virtual server.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 242

An LTM device has a virtual server configured as a Performance Layer 4 virtual listening on 0.0.0.0:0 to perform routing of packets to an upstream router. The client machine at IP address 192.168.0.4 is attempting to contact a host upstream of the LTM device on IP address 10.0.0.99.

The network flow is asymmetrical, and the following TCP capture displays:

```
# tcpdump -nni 0.0 'host 192.168.0.4 and host 10.0.0.99' tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on 0.0, link-type EN10MB (Ethernet), capture size 96 bytes
```

```
05:07:55.499954 IP 192.168.0.4.35345 > 10.0.0.99.443: S 3205656213:3205656213(0) ack 3267995082 win 1480
05:07:55.499983 IP 10.0.0.99.443 > 192.168.0.4.35345: R 1:1(0) ack 1 win 0
05:07:56.499960 IP 192.168.0.4.35345 > 10.0.0.99.443: S 3205656213:3205656213(0) ack 3267995082 win 1480
05:07:56.499990 IP 10.0.0.99.443 > 192.168.0.4.35345: R 1:1(0) ack 1 win 0 4 packets captured
```

Which option within the fastL4 profile needs to be enabled by the LTM Specialist to prevent the LTM device from rejecting the flow?

- A. Loose Close
- B. Loose Initiation
- C. Reset on Timeout
- D. Generate Initial Sequence Number

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 243

An LTM Specialist has configured a virtual server for `www.example.com`, load balancing connections to a pool of application servers that provide a shopping cart application. Cookie persistence is enabled on the virtual server. Users are able to connect to the application, but the user's shopping cart fails to update. A traffic capture shows the following:

Request:

GET /cart/updatecart.php HTTP/1.1

Host: `www.example.com`

Connection: keep-alive

Cache-Control: max-age=0

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.4 (KHTML, like Gecko) Chrome/22.0.1229.94 Safari/537.4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate, sdch

Accept-Language: en-US,en;q=0.8

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3

Cookie: BIGipServerwebstore_pool=353636524.20480.0000

Response:

HTTP/1.1 200 OK

Date: Wed, 24 Oct 2012 18:00:13 GMT

Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.1
Set-Cookie: cartID=647A5EA6657828C69DB8188981CB5; path=/; domain=wb01.example.com Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

No changes can be made to the application.

What should the LTM Specialist do to resolve the problem?

- A. Use an iRule to rewrite the cartID cookie domain.
- B. Create a universal persistence profile on the cartID cookie.
- C. Enable source address persistence as a fallback persistence method.
- D. Create a cookie persistence profile with "match across services" enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 244

An LTM Specialist has been asked to configure a virtual server to distribute connections between a pool of two application servers with addresses 172.16.20.1 and 172.16.20.2. The application servers are listening on TCP ports 80 and 443. The application administrators have asked that clients be directed to the same node for both HTTP and HTTPS requests within the same session.

Virtual servers vs_http and vs_https have been created, listening on 1.2.3.100:80 and 1.2.3.100:443, respectively.

Which configuration option will result in the desired behavior?

- A. Create pool app_pool with members 172.16.20.1:any and 172.16.20.2:any Assign app_pool as the default pool for both vs_http and vs_https Disable port translation for vs_http and vs_https
- B. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80 Assign pool http_pool as the default pool for both vs_https and vs_https Disable port translation for vs_https Create an SSL persistence profile with "match across virtual servers" enabled Assign the persistence profile to vs_http.
- C. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80 Create pool https_pool with members 172.16.20.1:443 and 172.16.20.2:443 Assign http_pool as the default pool for vs_http Assign https_pool as the default pool for vs_https Create a source address persistence profile with "match across services" enabled Assign the persistence profile to vs_http and vs_https
- D. Create pool http_pool with members 172.16.20.1:80 and 172.16.20.2:80 Create pool https_pool with members 172.16.20.1:443 and 172.16.20.2:443 Assign http_pool as the default pool for vs_http

Assign https_pool as the default pool for vs_https

Create an SSL persistence profile with "match across virtual servers" enabled Assign the persistence profile to vs_http

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 245

An LTM Specialist is investigating reports from users that SSH connections are being terminated unexpectedly. SSH connections are load balanced through a virtual server. The users experiencing this problem are running SQL queries that take upwards of 15 minutes to return with no screen output. The virtual server is standard with a pool associated and no other customizations.

What is causing the SSH connections to terminate?

- A. UDP IP ToS
- B. TCP idle timeout
- C. The virtual server has no persistence.
- D. The pool has Reselect Retries set to 0.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 246

Users in a branch office are reporting a website is always slow. No other users are experiencing the problem. The LTM Specialist tests the website from the external VLAN along with testing the servers directly. All tests indicate normal behavior. The environment is a single HTTP virtual server on the external VLAN with a single pool containing three HTTP pool members on the internal VLAN.

Which two locations are most appropriate to collect additional protocol analyzer data? (Choose two.)

- A. a user's machine
- B. the switch local to the user
- C. the LTM device's internal VLAN
- D. the LTM device's external VLAN
- E. a user's Active Directory authentication

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 247

An LTM Specialist has a single HTTPS virtual server doing SSL termination. No server SSL profile is defined. The pool members are on the internal VLAN answering on HTTP port 80.

Users with certain browsers are experiencing issues.

Which two locations are most appropriate to gather packets needed to determine the SSL issue? (Choose two.)

- A. server interface
- B. user's computer
- C. LTM device's external VLAN
- D. LTM device's internal VLAN
- E. LTM device's management interface

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 248

A user is having issues with connectivity to an HTTPS virtual server. The virtual server is on the LTM device's external vlan, and the pools associated with the virtual server are on the internal vlan. An LTM Specialist does a tcpdump on the external interface and notices that the host header is incomplete.

In which location should the LTM Specialist put a traffic analyzer to gather the most pertinent data?

- A. server
- B. external VLAN
- C. internal VLAN
- D. client machine

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

modified answer

QUESTION 249

An application owner claims an LTM device is delaying delivery of an HTTP application. The LTM device has two VLANs, an internal and an external. The application servers reside on the internal VLAN. The virtual server and clients reside on the external VLAN.

With appropriate filters applied, which solution is most efficient for obtaining packet captures in order to investigate the claim of delayed delivery?

- A. one capture on interface 0.0
- B. one capture on the internal interface
- C. one capture on the external interface
- D. one capture on the management interface

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 250

A client (10.10.1.30) connecting to an HTTPS virtual server (10.10.1.100) with a clientssl profile is getting an SSL error.

Which options will trace this issue?

- A. tcpdump -i external -X -e -nn -vvv -w /shared/ssl_problem.cap port 443 and host 10.10.1.30 ssldump -r /shared/ssl_problem.cap -n -x
- B. tcpdump -i external -s 0 -w /shared/ssl_problem.cap port 443 and host 10.10.10.30 and host 10.10.1.100
ssldump -r /shared/ssl_problem.cap -n -x
- C. tcpdump -i external -X -s 0 -vvv src host 10.10.10.30 and dst host 10.10.1.100 and port 443 > /shared/ssl_problem.cap
ssldump -r /shared/ssl_problem.cap -n -x
- D. tcpdump -i external -X -e -nn -vv port 443 and host 10.10.1.100 and host 10.10.1.30 > /shared/ssl_problem.cap
ssldump -n -x < /shared/ssl_problem.cap

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 251

An LTM device is deployed in a one-armed topology. The virtual server, clients, and web servers are connected on the LTM device internal VLAN. A client tries to connect to the virtual server and is unable to establish a connection. A packet capture from the LTM device internal VLAN shows that the HTTP request is being forwarded to the web server.

From which two additional locations should protocol analyzer data be collected? (Choose two.)

- A. network interface of web server
- B. network interface of client machine
- C. internal VLAN interface of LTM device
- D. external VLAN interface of LTM device
- E. any network interface of the Internet firewall

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 252

An LTM Specialist configures a new HTTP virtual server on an LTM device external VLAN. The web servers are connected to the LTM device internal VLAN. Clients trying to connect to the virtual server are unable to establish a connection. A packet capture shows an HTTP response from a web server to the client and then a reset from the client to the web server.

From which two locations could the packet capture have been collected? (Choose two.)

- A. network interface of web server
- B. network interface of client machine
- C. internal VLAN interface of the LTM device
- D. external VLAN interface of the LTM device
- E. management VLAN interface of the LTM device

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 253

The LTM Specialist is writing a custom HTTP monitor for a web application and has viewed the content by accessing the site directly via their browser. The monitor continually fails. The monitor configuration is:

```
ltm monitor http /Common/exampleComMonitor {  
  defaults-from /Common/http  
  destination *:*  
  interval 5  
  recv "Recent Searches"  
  send "GET /app/feed/current?uid=20145 HTTP/1.1\r\nHost: www.example.com\r\nAccept- Encoding: gzip, deflate\r\n\r\nConnection: close\r\n\r\n\r\n"  
  time-until-up 0  
  timeout 16  
}
```

A trace shows the following request and response:

Request:

```
GET /app/feed/current?uid=20145 HTTP/1.1  
Host www.example.com  
Accept-Encoding gzip, deflate  
Connection: close
```

Response:

```
HTTP/1.1 302 Moved Temporarily  
Date Wed, 17 Oct 2012 18:45:52 GMT  
Server Apache  
Location https://example.com/login.jsp  
Content-Encoding gzip  
Content-Type text/html; charset=UTF-8  
Set-Cookie JSESSIONID=261EFFBDA8EC3036FBCC22D991AC6835; Path=/app/feed/current?uid=20145
```

What is the problem?

- A. The request does NOT include a User-Agent header.
- B. The HTTP monitor does NOT support monitoring jsp pages.
- C. The request does NOT include any cookies and the application is expecting a session cookie.
- D. The request includes an Accept-Encoding so the server is responding with a gzipped result and LTM monitors CANNOT handle gzipped responses.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 254

An LTM Specialist configures an HTTP monitor as follows:

```
ltm monitor http stats_http_monitor {  
  defaults-from http  
  destination *:*  
  interval 5  
  recv "Health check: OK"  
  send "GET /stats/stats.html HTTP/1.1\r\nHost: www.example.com\r\nAccept-EncodinG. gzip, deflate\r\nConnection: close\r\n\r\n"  
  time-until-up 0  
  timeout 16  
}
```

The monitor is marking all nodes as down. A trace of the HTTP conversation shows the following:

```
GET /stats/stats.html HTTP/1.1  
Host: www.example.com  
Accept-EncodinG.gzip, deflate  
Connection: close
```

```
HTTP/1.1 401 Authorization Required  
DatE.Tue, 23 Oct 2012 19:38:56 GMT  
Server: Apache/2.2.15 (Unix)  
WWW-AuthenticatE.Basic realm="Please enter your credentials" Content-LengtH.480  
Connection: close  
Content-TypE.text/html; charset=iso-8859-1
```

Which action will resolve the problem?

- A. Add an NTLM profile to the virtual server.
- B. Add a valid username and password to the monitor.
- C. Use an HTTPS monitor with a valid certificate instead.
- D. Add a backslash before the colon in the receive string.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 255

The following decoded TCPDump capture shows the trace of a failing health monitor.

```
00:00:13.245104 IP 10.29.29.60.51947 > 10.0.0.12.http: P 1:59(58) ack 1 win 46 <nop,nop,timestamp 2494782300 238063789> out slot1/tmm3 lis=
0x0000: 4500 006e 3b19 4000 4006 ce0c 0a1d 1d3c E..n;. @. @.....< 0x0010: 0a00 000c caeb 0050 8be5 aca3 dd65 e3e1 .....P.....e.. 0x0020: 8018
002e 1b41 0000 0101 080a 94b3 5b5c .....A.....[ 0x0030: 0e30 90ad 4745 5420 2f74 6573 745f 7061 .0..GET./test_pa 0x0040: 6765 2e68 746d 6c20
4854 5450 312e 310d ge.html.HTTP1.1. 0x0050: 0a48 6f73 743a 200d 0a43 6f6e 6e65 6374 .Host:...Connect 0x0060: 696f 6e3a 2043 6c6f 7365 0d0a
0d0a 0105 ion:.Close.....
0x0070: 0100 0003 00 .....
00:00:13.245284 IP 10.0.0.12.http > 10.29.29.60.51947: .ack 59 win 362 <nop,nop,timestamp 238063789 2494782300> in slot1/tmm3 lis=
0x0000 0ffd 0800 4500 00c9 6f68 4000 8006 755d ....E...oh@...u] 0x0010 0a29 0015 0a29 0103 0050 e0d6 4929 90eb .)...)...P..I).. 0x0020 6f12 d83c
8019 fab3 9b31 0000 0101 080a o..<.....1..... 0x0030 0068 4e10 5240 6150 4854 5450 2f31 2e31 .hN.R@aPHTTP/1.1 0x0040 2034 3030 2042 6164
2052 6571 7565 7374 .400.Bad.Request 0x0050 0d0a 436f 6e74 656e 742d 5479 7065 3a20 ..Content-Type:. 0x0060 7465 7874 2f68 746d 6c0d 0a44
6174 653a text/html..Date:
0x0070 2054 6875 2c20 3231 204a 616e 2032 3031 .Mon.,01.Jan.201 0x0080 3020 3138 3a35 383a 3537 2047 4d54 0d0a 2.00:00:01.GMT.. 0x0090
436f 6e6e 6563 7469 6f6e 3a20 636c 6f73 Connection:.clos 0x00a0 650d 0a43 6f6e 7465 6e74 2d4c 656e 6774 e..Content-Lengt 0x00b0 683a 2032
300d 0a0d 0a3c 6831 3e42 6164 h:.20....<h1>Bad 0x00c0 2052 6571 7565 7374 3c2f 6831 3e .Request</h1>
```

The health monitor is sending the string shown in the capture; however, the server response is NOT as expected. The correct response should be an HTML page including the string 'SERVER IS UP'.

What is the issue?

- A. The /test_page.html does NOT exist on the web server.
- B. Incorrect syntax in send string. 'HTTP1.1' should be 'HTTP/1.1'.
- C. Incorrect syntax in send string. 'Connection: Close' should be 'Connection: Open'.
- D. The wrong HTTP version is specified in the send string. Version 1.2 should be used instead of version 1.1.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 256

An LTM device is monitoring pool members on port 80. The LTM device is using an HTTP monitor with a send string of GET / and a blank receive string.

What would cause the pool members to be marked down?

- A. A pool member responds with an HTTP 200 series response code.

- B. A pool member responds with an HTTP 300 series response code.
- C. A pool member responds with an HTTP 400 series response code.
- D. A pool member responds with an HTTP 500 series response code.
- E. A pool member does NOT acknowledge the connection SYN on port 80.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 257

An LTM device is monitoring three pool members. One pool member is being marked down.

What should the LTM Specialist enable to prevent the server from being flooded with connections once its monitor determines it is up?

- A. manual resume
- B. packet shaping
- C. hold down timer
- D. slow ramp timer
- E. fastest load balance algorithm

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 258

An LTM device is serving an FTP virtual server that has three pool members. The FTP pool members are monitored via TCP port 21. Customers are reporting that they are able to log in, but are sometimes unable to upload files to the server.

Which monitor should the LTM Specialist configure to verify that the servers can handle file uploads?

- A. FTP
- B. Inband
- C. External
- D. Scripted

E. Real Server

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 259

An LTM HTTP pool has an associated monitor that sends a string equal to 'GET /test.html'.

Which two configurations could an LTM Specialist implement to allow server administrators to disable their pool member servers without logging into the LTM device? (Choose two.)

- A. Set monitor to transparent and ask the server team to set string `TRANSPARENT' in test.html.
- B. Set `receive string' equal to 'SERVER UP' and ask the server team to set string `SERVER DOWN' in test.html.
- C. Set `alias' equal to 'SERVER DOWN' and ask the server team to set string `SERVER DOWN' in test.html.
- D. Set `receive disable string' equal to 'SERVER DOWN' and ask the server team to set string `SERVER DOWN' in test.html.
- E. Set `disable pool member' equal to 'SERVER UP' and ask the server team to set string `SERVER DOWN' in test.html.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 260

An LTM Specialist is receiving reports from customers about multiple applications failing to work properly. The LTM Specialist looks at the services running and notices that the bigd process has NOT started.

How are monitored LTM device objects marked when the bigd process is stopped?

- A. red or offline
- B. blue or unchecked
- C. green or available
- D. unchanged until bigd is restarted

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 261

An LTM Specialist is setting up a monitor for an HTTP 1.1 server. The response to a GET / is:

HTTP/1.1 302 Moved Temporarily

Location: http://www.example.com/new/location.html

Which send string settings should the LTM Specialist use to force a proper response?

- A. GET / HTTP/1.0\r\nHost: host.domain.com\r\nConnection: Close\r\n\r\n
- B. GET /new/location.html HTTP/1.1\r\nHost: www.example.com\r\nConnection: Close\r\n\r\n
- C. GET / HTTP/1.1\r\nHost: www.example.com/new/location.html\r\nConnection: Close\r\n\r\n
- D. GET /new/location.html HTTP/1.1\r\nHost: host.domain.com/new/locations.html\r\nConnection: Close\r\n\r\n

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

verified answer

QUESTION 262

An LTM Specialist defines a receive string in the HTTP monitor and then assigns it to the HTTP pool. The monitor has an interval of 5 seconds and a timeout of 16 seconds.

If the receive string is NOT seen in the the HTTP payload after 20 seconds, how does the LTM device mark the monitor status?

- A. offline
- B. unknown
- C. available
- D. unavailable
- E. forced offline

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 263

An LTM Specialist receives a request to monitor the network path through a member, but NOT the member itself.

Which monitor option should the LTM Specialist enable or configure?

- A. Reverse
- B. Up interval
- C. Transparent
- D. Alias address
- E. Time until up

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 264

An LTM Specialist is creating a custom EAV monitor.

In which directory should the LTM Specialist upload the script?

- A. /usr/monitor
- B. /usr/monitors
- C. /config/monitors
- D. /usr/bin/monitors
- E. /config/templates

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 265

An FTP monitor is NOT working correctly.

Which three pieces of information does the LTM Specialist need to provide to ensure a properly working FTP monitor? (Choose three.)

- A. alias
- B. File path
- C. username
- D. password
- E. FTP server port
- F. FTP server IP address

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 266

Which iRule statement demotes a virtual server from CMP?

- A. set ::foo 123
- B. set static::foo 123
- C. persist source_addr 1800
- D. [class match \$HTTP_CONTENT contains my_data_class]

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 267

What is the effect of an iRule error such as referencing an undefined variable?

- A. The iRule execution will continue with the next statement.
- B. The execution of the current event within the iRule will be terminated.
- C. The iRule execution will be terminated, and both the client and server side connections will be reset.
- D. The connection will continue, but the iRule will NOT be executed again for the lifetime of the connection.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 268

What does the following iRule do?

```
when CLIENT_ACCEPTED {  
  if { [matchclass [IP::client_addr] equals WebClient1-Whitelist1] } { #log local0. "Valid client IP: [IP::client_addr] - forwarding traffic" #Pool WebClient1  
  } else {  
    log local0. "Invalid client IP: [IP::client_addr] - discarding" discard  
  }  
}
```

- A. The iRule compares a client IP to a list. If the client IP is on the list, discard and log the discard.
- B. The iRule compares a client IP to a list. If the client IP is NOT on the list, discard and log the discard.
- C. The iRule compares a client IP to a list. If the client IP is on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the discard.
- D. The iRule compares a client IP to a list. If the client IP is NOT on the list, the client is sent to Pool WebClient1. Otherwise, discard and log the discard.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 269

What do the following iRule commands do when they are used in the same iRule?

```
set hsl [HSL::open -proto UDP -pool syslog_server_pool] HSL::send $hsl "<190> [HTTP::host] from [whereis [IP::client_addr] country continent state city zip] , IP: [IP::client_addr]"
```

- A. The commands set up a high-speed logging connection and then send the geographical database to the server.
- B. The commands set up a high-speed logging connection and then send the host header and client geographical detail to the connection.
- C. The commands set up a high-speed logging connection and then send the host header, HTTP payload, and client geographical detail to the connection.
- D. The commands set up a high-speed logging connection to the LTM device and then send the host header and client geographical detail to the

connection.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 270

An LTM Specialist configures the following iRule on an LTM device:

```
when HTTP_REQUEST {  
  if {[string tolower [HTTP::uri]] contains "/URI1/" } { pool Pool1  
  }  
  elseif {[string tolower [HTTP::uri]] contains "/URI2/" } { pool Pool2  
  }  
  elseif {[string tolower [HTTP::uri]] contains "/URI3/" } { pool Pool3  
  }  
  else { pool Pool4}  
}
```

Given the following request: `http://www.example.comURI1/index.html?fu=bar&pass=1234`

Which pool will be selected by the iRule?

- A. Pool1
- B. Pool2
- C. Pool3
- D. Pool4

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 271

Given the iRule:

```
when HTTP_REQUEST {  
  if {[HTTP::username] ne ""} and ([HTTP::password] ne "") { log local0. "client ip [IP::remote_addr] credentials provided [HTTP::username]
```

```
[HTTP::password]"}  
else {  
pool old_application_pool  
}  
}
```

The associated virtual server has a default pool named new_application_pool.
Which functionality does the iRule provide?

- A. Allows clients with credentials to access the old_application_pool and logs the access of clients without credentials to the new_application_pool.
- B. Allows clients without credentials to access the old_application_pool and logs the access of clients with credentials to the new_application_pool.
- C. Allows clients with credentials to access the old_application_pool and logs the attempted access of clients with credentials to the new_application_pool.
- D. Allows clients without credentials to access the old_application_pool and logs the attempted access of clients without credentials to the new_application_pool.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 272

Which three HTTP headers allow an application server to determine the client's language compatibility, browser, operating system type, and compression compatibility? (Choose three.)

- A. Accept
- B. Accept-Encoding
- C. Accept-Language
- D. Host
- E. User-Agent

Correct Answer: BCE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 273

A web application requires the client to provide the destination server and service identification.

Which HTTP header will supply this information?

- A. Host
- B. From
- C. Expect
- D. Connection

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 274

A web application is meant to log the URI of the resource that responded to the client's initial Request-URI.

Which HTTP header will supply this information?

- A. Via
- B. Server
- C. Trailer
- D. Referer

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 275

The end users of a web application need to verify that their browsers received the complete message-body from the web server.

Which HTTP header will accomplish this?

- A. Range
- B. Expect

- C. Accept-Ranges
- D. Content-Length

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 276

An HTTP 1.1 application utilizes chunking.

Which header should be used to notify the client's browser that there are additional HTTP headers at the end of the message?

- A. ETag
- B. From
- C. Trailer
- D. Expect

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 277

A web application sends information about message integrity and content life time to the client.

Which two HTTP headers should be used in sending the client information? (Choose two.)

- A. ETag
- B. Expect
- C. Expires
- D. Content-MD5
- E. Content-Range
- F. Content-Length

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 278

A web developer has created a custom HTTP call to a backend application. The HTTP headers being sent by the HTTP call are:

```
GET / HTTP/1.1
User-Agent: MyCustomApp (v1.0)
Accept: text/html
Cache-Control: no-cache
Connection: keep-alive
Cookie: somecookie=1
```

The backend server is responding with the following:

```
HTTP/1.1 400 Bad Request
Date: Wed, 20 Jul 2012 17:22:41 GMT
Connection: close
```

Why is the HTTP web server responding with a HTTP 400 Bad Request?

- A. The client request does NOT include a Host header.
- B. The User-Agent header contains an invalid character.
- C. The web server is NOT expecting a keep-alive connection.
- D. The web server is configured to accept HTTP 1.0 requests only.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 279

A client is attempting to log in to a web application that requires authentication. The following HTTP headers are sent by the client:

```
GET /owa/ HTTP/1.1
Authorization: Basic dXNlcm5hbWU6cGFzc3dvcmQ=
User-Agent: curl/7.26.0
```

Host: 10.0.0.14
Accept: */*
Accept-Encoding: gzip, deflate

The web server is responding with the following HTTP headers:

HTTP/1.1 401 Unauthorized
Content-Type: text/html
Server: Microsoft-IIS/7.5
WWW-Authenticate: NTLM
Date: Wed, 16 Aug 1977 19:12:31 GMT
Content-Length: 1293

The client has checked the login credentials and believes the correct details are being entered.

What is the reason the destination web server is sending an HTTP 401 response?

- A. The username and password are incorrect.
- B. The server has an incorrect date configured.
- C. The client is using the wrong type of browser.
- D. The wrong authentication mechanism is being used.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 280

The LTM device is configured to provide load balancing to a set of web servers that implement access control lists (ACL) based on the source IP address of the client. The ACL is at the network level and the web server is configured to send a TCP reset back to the client if it is NOT permitted to connect.

The virtual server is configured with the default OneConnect profile.

The ACL is defined on the web server as:

Permit: 192.168.136.0/24
Deny: 192.168.116.0/24

The packet capture is taken of two individual client flows to a virtual server with IP address 192.168.136.100.

Client A - Src IP 192.168.136.1 - Virtual Server 192.168.136.100:

Clientside:

```
09:35:11.073623 IP 192.168.136.1.55684 > 192.168.136.100.80: S 869998901:869998901(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
09:35:11.073931 IP 192.168.136.100.80 > 192.168.136.1.55684: S 2273668949:2273668949(0) ack 869998902 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:35:11.074928 IP 192.168.136.1.55684 > 192.168.136.100.80: .ack 1 win 16425
09:35:11.080936 IP 192.168.136.1.55684 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:35:11.081029 IP 192.168.136.100.80 > 192.168.136.1.55684: .ack 299 win 4678
```

Serverside:

```
09:35:11.081022 IP 192.168.136.1.55684 > 192.168.116.128.80: S 685865802:685865802(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:35:11.081928 IP 192.168.116.128.80 > 192.168.136.1.55684: S 4193259095:4193259095(0) ack 685865803 win 5840 <mss 1460,nop,nop,sackOK,nop,wscale 6>
09:35:11.081943 IP 192.168.136.1.55684 > 192.168.116.128.80: .ack 1 win 4380
09:35:11.081955 IP 192.168.136.1.55684 > 192.168.116.128.80: P 1:299(298) ack 1 win 4380
09:35:11.083765 IP 192.168.116.128.80 > 192.168.136.1.55684: .ack 299 win 108
```

Client B - Src IP 192.168.116.1 - Virtual Server 192.168.136.100:

Clientside:

```
09:36:11.244040 IP 192.168.116.1.55769 > 192.168.136.100.80: S 3320618938:3320618938(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
09:36:11.244152 IP 192.168.136.100.80 > 192.168.116.1.55769: S 3878120666:3878120666(0) ack 3320618939 win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
09:36:11.244839 IP 192.168.116.1.55769 > 192.168.136.100.80: .ack 1 win 16425
09:36:11.245830 IP 192.168.116.1.55769 > 192.168.136.100.80: P 1:299(298) ack 1 win 16425
09:36:11.245922 IP 192.168.136.100.80 > 192.168.116.1.55769: .ack 299 win 4678
```

Serverside:

```
09:36:11.245940 IP 192.168.136.1.55684 > 192.168.116.128.80: P 599:897(298) ack 4525 win
09:36:11.247847 IP 192.168.116.128.80 > 192.168.136.1.55684: P 4525:5001(476) ack 897 win Why was the second client flow permitted by the web server?
```

- A. A global SNAT is defined.
- B. SNAT automap was enabled on the virtual server.
- C. The idle TCP session from the first client was re-used.
- D. A source address persistence profile is assigned to the virtual server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 281

An LTM Specialist is troubleshooting an HTTP monitor. The pool member is accessible directly through a browser, but the HTTP monitor is marking the pool member as down.

GET / HTTP/1.1

HTTP/1.1 400 Bad Request

Date: Tue, 23 Oct 2012 21:39:07 GMT

Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4

mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2

Content-Length: 226

Connection: close

Content-Type: text/html; charset=iso-8859-1

Which issue is the pool member having?

- A. The pool member has too many concurrent connections.
- B. The pool member is rejecting the request because it is invalid.
- C. The pool member lacks the object requested by the monitor.
- D. The pool member is NOT accepting requests from the LTM device IP address.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 282

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "Unable to connect" in the browser, although connections directly to the pool member show the application is functioning correctly. The LTM device configuration is:

```
ltm virtual /Common/vs_https {  
  destination /Common/10.10.1.110:443  
  ip-protocol udp  
  mask 255.255.255.255
```

```
pool /Common/pool_https
profiles {
/Common/udp { }
}
translate-address enabled
translate-port enabled
vlans-disabled
}

ltm pool /Common/pool_https {
members {
/Common/172.16.20.1:443 {
address 172.16.20.1
}
}
}
```

What issue is the LTM Specialist experiencing?

- A. The virtual server is disabled on all VLANs.
- B. The pool member is marked down by a monitor.
- C. The pool member is marked down administratively.
- D. The virtual server is configured for the incorrect protocol.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 283

Under what condition must an appliance license be reactivated?

- A. Licenses only have to be reactivated for RMAs - no other situations.
- B. Licenses generally have to be reactivated during system software upgrades.
- C. Licenses only have to be reactivated when new features are added (IPv6, Routing Modules, etc) - no othersituations.
- D. Never. Licenses are permanent for the platform regardless the version of software installed.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 284

Which three methods can be used for initial access to a BIG-IP system? (Choose three.)

- A. CLI access to the serial console port
- B. SSH access to the management port
- C. SSH access to any of the switch ports
- D. HTTP access to the management port
- E. HTTP access to any of the switch ports
- F. HTTPS access to the management port
- G. HTTPS access to any of the switch ports

Correct Answer: ABF

Section: (none)

Explanation

Explanation/Reference:

updated answers

QUESTION 285

What is the purpose of provisioning?

- A. Provisioning allows modules that are not licensed to be fully tested.
- B. Provisioning allows modules that are licensed be granted appropriate resource levels.
- C. Provisioning allows the administrator to activate modules in non-standard combinations.
- D. Provisioning allows the administrator to see what modules are licensed, but no user action is ever required.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 286

Which three properties can be assigned to nodes? (Choose three.)

- A. ratio values
- B. priority values
- C. health monitors
- D. connection limits
- E. load-balancing mode

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 287

Where is the load-balancing mode specified?

- A. within the pool definition
- B. within the node definition
- C. within the virtual server definition
- D. within the pool member definition

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 288

Which statement accurately describes the difference between two load-balancing modes specified as "member" and "node"?

- A. There is no difference; the two terms are referenced for backward compatibility purposes.
- B. When the load-balancing choice references "node", priority group activation is unavailable.
- C. Load-balancing options referencing "nodes" are available only when the pool members are defined for the "any" port.
- D. When the load-balancing choice references "node", the addresses' parameters are used to make the loadbalancingchoice rather than the member's parameters.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 289

What will likely happen if you were to define a LTM System in the wrong Data Center?

- A. There would be no effect if the LTM System is defined in the wrong Data Center.
- B. The GTM System would not be able to communicate with that LTM System loadbalancing decisions.
- C. Data from probes from that LTM System might result in inaccurate path metrics and
- D. The GTM System would not be able to resolve WideIPs to the addresses associated with that LTM System's Virtual Servers.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 290

When initially configuring the GTM System using the config tool, which two parameters can be set? (Choose two.)

- A. System hostname
- B. IP Address of management port
- C. IP Address of the external VLAN
- D. Default route for management port
- E. Port lockdown of management port

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 291

Without creating a user-defined region, what is the most specific group a topology record can identify?

- A. city

- B. country
- C. continent
- D. state/province
- E. region of country

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 292

The SNMP monitor can collect data based on which three metrics? (Choose three.)

- A. packet rate
- B. memory utilization
- C. content verification
- D. current connections
- E. hops along the network path

Correct Answer: ABD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 293

Which facility logs messages concerning GTM System parameters?

- A. local0
- B. local1
- C. local2
- D. local3

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

modified answer

QUESTION 294

When users are created, which three access levels can be granted through the GTMConfiguration Utility? (Choose three.)

- A. Root
- B. Guest
- C. Operator
- D. Administrator
- E. CLI + Web Read Only

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 295

What is the purpose of Zonerunner?

- A. Zonerunner adds a GUI interface for configuration of Wide-IP names.
- B. Zonerunner adds a GUI interface for configuration of BIND database files for zones where the GTM System is a primary name server.
- C. Zonerunner adds a GUI interface for configuration of BIND database files where the GTM System is not a primary or secondary server.
- D. Zonerunner adds a GUI interface for configuration of BIND database files for zones where the GTM System is a primary or secondary name server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 296

GTM can sign a DNS response using DNSSEC only if the DNS request ...

- A. Has the S-bit set.
- B. Is a part of a DNSSEC zone.
- C. Is for a Wide-IP name on the GTM.

D. Is answered by BIND running on the GTM.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

accurate answer

QUESTION 297

Which statement about Generic Host Servers is true?

- A. GTM Systems can initiate a big3d agent on Generic Host Servers.
- B. GTM Systems cannot provide path metrics for Virtual Servers managed by a Generic Host Server.
- C. GTM Systems can monitor a Generic Host Server and can cause a Generic Host Server to act as a Statistics Collection Server.
- D. GTM Systems can monitor a Generic Host Server but cannot cause a Generic Host Server to act as a Statistics Collection Server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 298

By default, how frequently are log files rotated?

- A. hourly
- B. daily
- C. weekly
- D. There is no default; the administrator sets the frequency.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 299

When configuring monitors for individual pool members, which three options can be selected? (Choose three.)

- A. Inherit the pool's monitor.
- B. Choose a default monitor.
- C. Inherit the Wide-IP's monitor.
- D. Assign a monitor to the specific pool member.
- E. Do not assign any monitor to the specific pool member.

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 300

Which two can be a part of a virtual server's definition? (Choose two.)

- A. rule(s)
- B. pool(s)
- C. monitor(s)
- D. node address(es)
- E. load-balancing method(s)

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 301

Assume a BIG-IP has no NATs or SNATs configured. Which two scenarios are possible when client traffic arrives on a BIG-IP that is NOT destined to a self-IP? (Choose two.)

- A. If the destination of the traffic does not match a virtual server, the traffic will be discarded.
- B. If the destination of the traffic does not match a virtual server, the traffic will be forwarded based on routing tables.
- C. If the destination of the traffic matches a virtual server, the traffic will be processed per the virtual server definition. If the destination of the traffic matches a virtual server, the traffic will be processed per the virtual server? definition.
- D. If the destination of the traffic matches a virtual server, the traffic will be forwarded, but it cannot be load-balanced since no SNAT has been configured.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 302

When configuring a pool member's monitor, which three association options are available? (Choose three.)

- A. inherit the pool's monitor
- B. inherit the node's monitor
- C. configure a default monitor
- D. assign a monitor to the specific member
- E. do not assign any monitor to the specific member

Correct Answer: ADE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 303

If a client's browser does not accept cookies, what occurs when the client connects to a virtual server using cookie persistence?

- A. The connection request is not processed.
- B. The connection request is sent to an ?pology?server.The connection request is sent to an ?pology?server.
- C. The connection request is load-balanced to an available pool member.
- D. The connection request is refused and the client is sent a "server not available" message.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 304

Which statement is true concerning cookie persistence?

- A. Cookie persistence allows persistence independent of IP addresses.
- B. Cookie persistence allows persistence even if the data are encrypted from client to pool member.
- C. Cookie persistence uses a cookie that stores the virtual server, pool name, and member IP address in clear text.
- D. If a client's browser accepts cookies, cookie persistence will always cause a cookie to be written to the client's file system.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 305

The incoming client IP address is 195.64.45.52 and the last five connections have been sent to members A, C, E, D and B. The incoming client IP address is 195.64.45.52 and the last five connections have been sent to members A, C, E, D and B. Given the virtual server, pool, and persistence definitions and statistics shown in the above graphic, which member will be used for the next connection?

Persistence Table		
All entries for the one virtual server and pool		
Persistence Values	Member	Age (Seconds)
200.10.0.0	10.10.20.1:80	63
201.12.0.0	10.10.20.3:80	43
153.15.0.0	10.10.20.2:80	76
205.12.0.0	10.10.20.4:80	300
195.64.0.0	10.10.20.3:80	22
198.22.0.0	10.10.20.5:80	176
214.77.0.0	10.10.20.1:80	43

Web_PoolStatistics					
Member	Member Ratio	Member Priority	Outstanding Layer 7 Requests	Connection Count	Status
10.10.20.1:80	3	5	6	18	Available
10.10.20.2:80	3	5	6	12	Available
10.10.20.3:80	3	5	12	5	Disabled
10.10.20.4:80	1	1	8	19	Offline
10.10.20.5:80	1	1	4	9	Available

Virtual Server, Pool and Persistence Profile Settings					
VS_Web_Pool Settings		Web_Pool Settings		Source Persist Settings	
Destination	172.160.22.3:80	Load Balancing	Least Connections	Mode	Source Address
Profile(s)	TCP	Priority Activation	Less than 2	Netmask	255.255.0.0
Pool	Web_Pool	Monitor	Done	Timeout	360 seconds
iRules	None				
Persistence	Source_Persist				

- A. 10.10.20.1:80
 B. 10.10.20.2:80
 C. 10.10.20.3:80
 D. 10.10.20.4:80
 E. 10.10.20.5:80
 F. It cannot be determined with the information given.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 306

How is persistence configured?

- A. Persistence is an option within each pool's definition.
- B. Persistence is a profile type; an appropriate profile is created and associated with virtual server.
- C. Persistence is a global setting; once enabled, load-balancing choices are superseded by the persistence method that is specified.
- D. Persistence is an option for each pool member. When a pool is defined, each member's definition includes the option for persistence.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 307

Assume a virtual server has a ServerSSL profile. What SSL certificates are required on the BIG- IP?

- A. No SSL certificates are required on the BIG-IP.
- B. The BIG-IP's SSL certificates must only exist.
- C. The BIG-IP's SSL certificates must be issued from a certificate authority.
- D. The BIG-IP's SSL certificates must be created within the company hosting the BIG-IPs.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 308

Assume a virtual server is configured with a ClientSSL profile. What would the result be if the virtual server's destination port were not 443?

- A. SSL termination could not be performed if the virtual server's port was not port 443.

- B. Virtual servers with a ClientSSL profile are always configured with a destination port of 443.
- C. As long as client traffic was directed to the alternate port, the virtual server would work as intended.
- D. Since the virtual server is associated with a ClientSSL profile, it will always process traffic sent to port 443.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 309

Which statement is true concerning SSL termination?

- A. A virtual server that has both ClientSSL and ServerSSL profiles can still support cookie persistence.
- B. Decrypting traffic at the BIG-IP allows the use of iRules for traffic management, but increases the load on the pool member.
- C. When any virtual server uses a ClientSSL profile, all SSL traffic sent to the BIG-IP is decrypted before it is forwarded to servers.
- D. If a virtual server has both a ClientSSL and ServerSSL profile, the pool members have less SSL processing than if the virtual server had only a ClientSSL profile

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 310

Which event is always triggered when a client initially connects to a virtual server configured with an HTTPprofile?

- A. HTTP_DATA
- B. CLIENT_DATA
- C. HTTP_REQUEST
- D. CLIENT_ACCEPTED

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 311

A virtual server is listening at 10.10.1.100:any and has the following iRule associated with it:
when CLIENT_ACCEPTED { if {[TCP::local_port] equals 80 } { pool pool1 } elseif {[TCP::local_port] equals 443 } { pool pool2 } }
If a user connects to 10.10.1.100 and port 22, which pool will receive the request?

- A. pool1.
- B. pool2.
- C. None. The request will be dropped.
- D. Unknown. The pool cannot be determined from the information provided.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 312

Which statement is true about the synchronization process, as performed by the Configuration Utility or by typing `b config sync all`?

- A. The process should always be run from the standby system.
- B. The process should always be run from the system with the latest configuration.
- C. The two `/config/bigip.conf` configuration files are synchronized (made identical) each time the process is run.
- D. Multiple files, including `/config/bigip.conf` and `/config/bigip_base.conf`, are synchronized (made identical) each time the process is run.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 313

Which statement is true concerning the default communication between a redundant pair of BIG-IP devices?

- A. Communication between the systems cannot be effected by port lockdown settings.
- B. Data for both connection and persistence mirroring are shared through the same TCP connection.
- C. Regardless of the configuration, some data is communicated between the systems at regular intervals.

D. Connection mirroring data is shared through the serial fail-over cable unless network fail-over is enabled.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 314

When upgrading a BIG-IP redundant pair, what happens when one system has been updated but the other has not?

- A. Synching should not be performed.
- B. The first system to be updated will assume the Active role.
- C. This is not possible since both systems are updated simultaneously.
- D. The older system will issue SNMP traps indicating a communication error with the partner.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 315

When using the setup utility to configure a redundant pair, you are asked to provide a "Failover Peer IP".

Which address is this?

- A. an address of the other system in its management network
- B. an address of the other system in a redundant pair configuration
- C. an address on the current system used to listen for fail-over messages from the partner BIG-IP
- D. an address on the current system used to initiate mirroring and network fail-over heartbeat messages

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 316

Which two statements describe differences between the active and standby systems? (Choose two.)

- A. Monitors are performed only by the active system.
- B. Fail-over triggers only cause changes on the active system.
- C. Virtual server addresses are hosted only by the active system.
- D. Configuration changes can only be made on the active system.
- E. Floating self-IP addresses are hosted only by the active system.

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 317

Assuming other fail-over settings are at their default state, what would occur if the fail-over cable were to be disconnected for five seconds and then reconnected?

- A. As long as network communication is not lost, no change will occur.
- B. Nothing. Fail-over due to loss of voltage will not occur if the voltage is lost for less than ten seconds.
- C. When the cable is disconnected, both systems will become active. When the voltage is restored, unit two will revert to standby mode.
- D. When the cable is disconnected, both systems will become active. When the voltage is restored, both systems will maintain active mode.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 318

Where is persistence mirroring configured?

- A. It is always enabled.
- B. It is part of a pool definition.
- C. It is part of a profile definition.
- D. It is part of a virtual server definition.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

valuable

QUESTION 319

Given that VLAN fail-safe is enabled on the external VLAN and the network that the active BIG-IP's external VLAN is connected to has failed, which statement is always true about the results?

- A. The active system will note the failure in the HA table.
- B. The active system will reboot and the standby system will go into active mode.
- C. The active system will fail-over and the standby system will go into active mode.
- D. The active system will restart the traffic management module to eliminate the possibility that BIG-IP is the cause for the network failure.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 320

Where is connection mirroring configured?

- A. It is an option within a TCP profile.
- B. It is an optional feature of each pool.
- C. It is not configured; it is default behavior.
- D. It is an optional feature of each virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 321

Assuming there are open connections through an active system's virtual servers and a fail-over occurs, by default, what happens to the connections?

- A. All open connections are lost.
- B. All open connections are maintained.
- C. When persistence mirroring is enabled, open connections are maintained even if a fail-over occurs.
- D. Long-lived connections such as Telnet and FTP are maintained, but short-lived connections such as HTTP are lost.
- E. All open connections are lost, but new connections are initiated by the newly active BIG-IP, resulting in minimal client downtime.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 322

How is MAC masquerading configured?

- A. Specify the desired MAC address for each VLAN for which you want this feature enabled.
- B. Specify the desired MAC address for each self-IP address for which you want this feature enabled.
- C. Specify the desired MAC address for each VLAN on the active system and synchronize the systems.
- D. Specify the desired MAC address for each floating self-IP address for which you want this feature enabled.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 323

A new web application is hosted at www.example.net, but some clients are still pointing to the legacy web application at www.example.com.

Which iRule will allow clients referencing www.example.com to access the new application?

- A.

```
when HTTP_REQUEST {  
  if {[HTTP::host] equals "www.example.*"}{  
    HTTP::redirect "http://www.example.net" }  
}
```
- B.

```
when HTTP_REQUEST {  
  if {[HTTP::host] equals "www.example.com"}{  
    HTTP::redirect "http://www.example.net" }
```


- ```
}
C. when HTTP_DATA {
 if {[HTTP::host] equals "www.example.*"}{
 HTTP::redirect "http://www.example.net" }
 }
D. when HTTP_RESPONSE {
 if {[HTTP::host] equals "www.example.com"}{
 HTTP::redirect "http://www.example.net" }
 }
```

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 324**

Which iRule will instruct the client's browser to avoid caching HTML server responses?

- ```
A. when HTTP_REQUEST {
  if {[HTTP::header Content-Type] equals "html"} {
    HTTP::header insert Pragma "no-cache"
    HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT" HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate" }
  }
B. when HTTP_REQUEST {
  if {[HTTP::header Content-Type] contains "html"} {
    HTTP::header insert Pragma "no-cache"
    HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT" HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate" }
  }
C. when HTTP_RESPONSE {
  if {[HTTP::header Content-Type] contains "html"} {
    HTTP::header insert Pragma "no-cache"
    HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT" HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate" }
  }
D. when HTTP_RESPONSE {
  if {[HTTP::header Content-Type] equals "html"} {
    HTTP::header insert Pragma "no-cache"
    HTTP::header insert Expires "Fri, 01 Jan 1990 00:00:00 GMT" HTTP::header replace Cache-Control "no-cache,no-store,must-revalidate" }
  }
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 325

An IT administrator wants to log which server is being load balanced to by a user with IP address 10.10.10.25.

Which iRule should the LTM Specialist use to fulfill the request?

- A. when SERVER_CONNECTED {
if { [IP::addr [IP::remote_addr]] equals 10.10.10.25 } { log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" } }
- B. when CLIENT_ACCEPTED {
if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25 } { log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" } }
- C. when SERVER_CONNECTED {
if { [IP::addr [clientside [IP::remote_addr]] equals 10.10.10.25 } { log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" } }
- D. when CLIENT_ACCEPTED {
if { [IP::addr [IP::remote_addr]] equals 10.10.10.25 } { log local0. "client 10.10.10.25 connected to pool member [IP::addr [LB::server addr]]" } }

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 326

A customer needs to intercept all of the redirects its application is sending to clients. When a redirect is matched, the customer needs to log a message including the client IP address.

Which iRule should be used?

- A. when HTTP_RESPONSE {
if { [HTTP::is_3xx] } {
log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]" }
}
- B. when HTTP_REQUEST {
if { [HTTP::is_301] } {
log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]" }
}

```

}
C. when HTTP_REQUEST {
  if { [HTTP::is_redirect] } {
    log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]" }
  }
D. when HTTP_RESPONSE {
  if { [HTTP::is_redirect] } {
    log local0. "redirecting client ip address [IP::addr [IP::remote_addr]]" }
  }

```

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 327

A web application requires knowledge of the client's true IP address for logging and analysis purposes. Instances of the application that can decode X-Forwarded-For HTTP headers reside in pool_a, while pool_b instances assume the source IP is the true address of the client.

Which iRule provides the proper functionality?

```

A. when HTTP_DATA {
  if {[HTTP::header exists X-Forwarded-For]}{
    pool pool_a
  } else {
    pool pool_b
  }
}
B. when HTTP_RESPONSE {
  if {[HTTP::header exists X-Forwarded-For]}{
    pool pool_a
  } else {
    pool pool_b
  }
}
C. when HTTP_REQUEST {
  if {[HTTP::header exists X-Forwarded-For]}{
    pool pool_a
  } else {
    pool pool_b
  }
}

```

```

}
}
D. when HTTP_OPEN {
  if {[HTTP::header exists X-Forwarded-For]}{
    pool pool_a
  } else {
    pool pool_b
  }
}
}

```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 328

Which iRule will reject any connection originating from a 10.0.0.0/8 network?

- A. when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::remote_addr] mask 8]
 switch \$remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1}
 default { pool http_pool }
 }
 }
- B. when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::local_addr] mask 8]
 switch \$remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1}
 default { pool http_pool }
 }
 }
- C. when CLIENT_ACCEPTED {
 set remote_ip [IP::addr [IP::client_addr] mask 255.0.0.0] switch \$remote_ip {
 "10.0.0.0" { reject }
 "11.0.0.0" { pool pool_http1}
 default { pool http_pool }
 }
 }

```
}  
D. when CLIENT_ACCEPTED {  
    set remote_ip [IP::addr [IP::local_addr] mask 255.0.0.0] switch $remote_ip {  
        "10.0.0.0" { reject }  
        "11.0.0.0" { pool pool_http1 }  
        default { pool http_pool }  
    }  
}
```

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 329

There is a fault with an LTM device load balanced trading application that resides on directly connected VLAN vlan-301. The application virtual server is 10.0.0.1:80 with trading application backend servers on subnet 192.168.0.0/25. The LTM Specialist wants to save a packet capture with complete payload for external analysis.

Which command should the LTM Specialist execute on the LTM device command line interface?

- A. tcpdump -vvv -w /var/tmp/trace.cap 'net 192.168.0.0/25'
- B. tcpdump -vvv -s 0 -w /var/tmp/trace.cap 'net 192.168.0.0/25'
- C. tcpdump -vvv -nni vlan-301 -w /var/tmp/trace.cap 'net 192.168.0.0/25'
- D. tcpdump -vvv -s 0 -nni vlan-301 -w /var/tmp/trace.cap 'net 192.168.0.0/25'

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 330

An LTM Specialist has just captured trace /var/tmp/trace.cap for site www.example.com while listening on virtual address 10.0.0.1:443 configured on partition ApplicationA. The data payload being captured is SSL encrypted.

Which command should the LTM Specialist execute to decrypt the data payload?

- A. `ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/Common_d/certificate_d/Common:www.example.com.crt_1`
- B. `ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/Common_d/certificate_key_d/Common:www.example.com.key_1`
- C. `ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/ApplicationA_d/certificate_d/ApplicationA:www.example.com.crt_1`
- D. `ssldump -Aed -nr /var/tmp/trace.cap -k /config/filestore/files_d/ApplicationA_d/certificate_key_d/ApplicationA:www.example.com.key_1`

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 331

An LTM Specialist needs to rewrite text within an HTML response from a web server. A client is sending the following HTTP request:

GET / HTTP/1.1

Host: www.example.com

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Cache-Control: no-cache

Connection: keep-alive

Cookie: somecookie=1

HTTP/1.1 200 OK

Server: Apache/2.2.15 (Unix)

Last-Modified: Wed, 12 Aug 2009 00:00:30 GMT

Accept-Ranges: bytes

Content-Length: 1063

X-Connection: close

Content-Type: text/html; charset=UTF-8

Vary: Accept-Encoding

Content-Encoding: gzip

Connection: Keep-Alive

Although a stream profile has been added to the virtual server, the content within the HTTP response is NOT being matched and therefore NOT modified.

Which header field is contributing to the issue?

- A. HTTP Method
- B. Cookie content
- C. User-Agent Value
- D. Accept-Encoding header

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 332

An LTM Specialist needs to rewrite text within an HTML response from a web server. A client is sending the HTTP request below:

```
GET / HTTP/1.1
Host: www.f5.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language:en-US,en;q=0.5
Accept-Encoding:gzip, deflate
Cache-Control: no-cache
Connection: keep-alive
Cookie:somecookie=1
```

Although a stream profile has been added to the virtual server, the content within the HTTP response is NOT being matched, and therefore NOT modified.

Which HTTP header should the LTM Specialist remove from the request to ensure the content can be matched and modified?

- A. Connection
- B. Accept
- C. Cache-Control
- D. Accept-Encoding

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 333

An LTM Specialist configured a virtual server to load balance a custom application. The application works when it is tested from within the firewall but it fails when tested externally. The pool member address is 192.168.200.10:80. A capture from an external client shows:

```
GET /index.jsp HTTP/1.1
Host: 207.206.201.100
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:15.0) Gecko/20100101 Firefox/15.0.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Connection: keep-alive
HTTP/1.1 302 Found
Date: Wed, 17 Oct 2012 23:09:55 GMT
Server: Apache/2.2.15 (CentOS)
Location: http://192.168.200.10/user/home.jsp
Content-Length: 304
Connection: close
```

What is the solution to this issue?

- A. Assign a SNAT pool to the virtual server.
- B. Add a Web Acceleration Profile to the virtual server.
- C. Configure redirect rewrite option in the HTTP profile.
- D. Configure a content filter on the backend web server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 334

There are three servers in the pool: 172.16.20.1, 172.16.20.2, and 172.16.20.3, with the virtual IP address 10.0.20.88.

A user CANNOT connect to an HTTP application. To understand the problem and find a solution, the LTM Specialist runs two concurrent traces on the LTM device, with the following results:

Trace on client side:

```
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on 0.0, link-type EN10MB (Ethernet), capture size 96 bytes
22:22:07.423759 IP 172.16.20.100.53875 > 10.0.20.88.80: S 998346084:998346084(0) win 5840 <mss 1460,sackOK,timestamp 67942058
0,nop,wscale 4>
22:22:07.424056 IP 10.0.20.88.80 > 172.16.20.100.53875: S 4671780:4671780(0) ack 998346085 win 4380 <mss 1460,nop,wscale
0,nop,nop,timestamp 2392362490 67942058,sackOK,eol>
22:22:07.424776 IP 172.16.20.100.53875 > 10.0.20.88.80: .ack 1 win 365 <nop,nop,timestamp 67942058 2392362490>
```



```
22:22:07.424790 IP 172.16.20.100.53875 > 10.0.20.88.80: P 1:149(148) ack 1 win 365 <nop,nop,timestamp 67942058 2392362490>
22:22:07.424891 IP 10.0.20.88.80 > 172.16.20.100.53875: .ack 149 win 4528 <nop,nop,timestamp 2392362491 67942058>
22:22:12.024850 IP 10.0.20.88.80 > 172.16.20.100.53875: R 1:1(0) ack 149 win 4528
```

6 packets captured
6 packets received by filter
0 packets dropped by kernel

Trace on server side:

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on internal, link-type EN10MB (Ethernet), capture size 96 bytes

```
22:22:07.424881 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2392362491 0,sackOK,eol>
```

```
22:22:08.424893 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2392363491 0,sackOK,eol>
```

```
22:22:09.625082 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,nop,wscale 0,nop,nop,timestamp 2392364691 0,sackOK,eol>
```

```
22:22:10.825194 IP 172.16.20.100.53875 > 172.16.20.2.80: S 51116678:51116678(0) win 4380 <mss 1460,sackOK,eol>
```

4 packets captured
4 packets received by filter
0 packets dropped by kernel

What should the LTM Specialist do to solve the problem?

- A. Edit the packet filter rules.
- B. Modify the monitor of the pool.
- C. Enable the virtual server.
- D. Configure the virtual server to use SNAT.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 335

An LTM Specialist is troubleshooting an HTTP monitor. The pool member is accessible directly through a browser, but the HTTP monitor is marking the pool member as down.

GET / HTTP/1.1
HTTP/1.1 400 Bad Request
Date: Tue, 23 Oct 2012 21:39:07 GMT

Server: Apache/2.2.22 (FreeBSD) PHP/5.4.4
mod_ssl/2.2.22 OpenSSL/0.9.8q DAV/2
Content-Length: 226
Connection: close
Content-Type: text/html; charset=iso-8859-1

How should the LTM Specialist resolve this issue?

- A. Add '200 OK' to the monitor's receive string.
- B. Add 'Connection: close\r\n' to the monitor's send string.
- C. Change the interval on the monitor from 5 seconds to 30 seconds.
- D. Change the HTTP version in the send string from HTTP/1.1 to HTTP/1.0.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 336

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "The connection was reset" in the browser, although connections directly to the pool member show the application is functioning correctly.

```
ltm pool srv1_https_pool {  
  members {  
    192.168.2.1:https {  
      address 192.168.2.1  
    }  
  }  
}  
  
ltm virtual https_example_vs {  
  destination 192.168.1.155:https  
  ip-protocol tcp  
  mask 255.255.255.255  
  pool srv1_https_pool  
  profiles {  
    http { }  
    tcp { }  
  }  
  snat automap  
  vlans-disabled  
}
```

How should the LTM Specialist resolve this issue?

- A. Enable HTTP monitoring on the pool.
- B. Add a ClientSSL profile to the virtual server.
- C. Disable SNAT Automap on the virtual server.
- D. Remove the HTTP profile from the virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 337

An LTM Specialist is troubleshooting an issue with a new virtual server. When connecting through the virtual server, clients receive the message "Unable to connect" in the browser, although connections directly to the pool member show the application is functioning correctly. The LTM configuration is:

```
ltm virtual /Common/vs_https {  
  destination /Common/10.10.1.110:443  
  ip-protocol udp  
  mask 255.255.255.255  
  pool /Common/pool_https  
  profiles {  
    /Common/udp { }  
  }  
  translate-address enabled  
  translate-port enabled  
  vlans-disabled  
}
```

```
ltm pool /Common/pool_https {  
  members {  
    /Common/172.16.20.1:443 {  
      address 172.16.20.1  
    }  
  }  
}
```

How should the LTM Specialist resolve this issue?

- A. Remove an HTTP monitor from the pool.
- B. Add an HTTP profile to the virtual server.
- C. Enable the pool member on the correct VLAN.
- D. Select the correct protocol for the virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 338

An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user's shopping cart is shown as empty. The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.

What is the issue?

- A. The port 80 pool member is deleting the user's session cookie.
- B. The port 443 pool member is deleting the user's session cookie.
- C. The port 80 and port 443 connections are balanced to the same node.
- D. The port 80 and port 443 connections are balanced to different nodes.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 339

An LTM Specialist is troubleshooting a problem on an eCommerce website. The user browses the online store using port 80, adding items to the shopping cart. The user then clicks the "Checkout" button on the site, which redirects the user to port 443 for the checkout process. Suddenly, the user's shopping cart is shown as empty. The shopping cart data is stored in memory on the server, and the default source address persistence profile is used on both virtual servers.

How should the LTM Specialist resolve this issue?

- A. Add an HTTP profile to both virtual servers.

- B. Enable SNAT Automap on both virtual servers.
- C. Create a custom persistence profile and enable "Map Proxies."
- D. Create a custom persistence profile and enable "Match Across Services."

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 340

An LTM device has been configured to log the reasons for generating TCP RST packets.

The following log entry occurs:

"01230140:3: RST sent from 192.168.1.100:80 to 192.168.1.124:39272, [0x112d82a:1721] {peer} TCP RST from remote system."

Which condition will trigger this log entry?

- A. A virtual server connection limit has been reached.
- B. The host at the other end terminated the TCP connection.
- C. The LTM device reset the connection because no pool members are available.
- D. The LTM device has reached the maximum number of allowed attempts to send the data segment to the affected TCP connection.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 341

An LTM device supports two power supplies. The value of the BigDB key "platform.powersupplymonitor" is equal to enable.

Where would the error message be visible if one of the power supplies fails or is NOT plugged in?

- A. visible only via the console
- B. in the /var/log/ltm log file
- C. in the /var/log/kern.log file

D. in the /var/log/tmm log file

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 342

An LTM Specialist loads a UCS file generated on a different LTM device and receives the following error message:

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

Which command should the LTM Specialist use to prevent the error?

- A. tmsh show /sys license
- B. tmsh show /sys hardware
- C. bigpipe config save /config.ucs
- D. tmsh load /sys /ucs rma <path/to/UCS>
- E. tmsh load /sys ucs<path/to/UCS> no-license

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

accurate answer

QUESTION 343

These log entries can have different root causes:

Jun 28 05:01:21 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: enabled Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071431:5: Attempting to connect to CMI peer 1.1.1.2 port 6699

Jun 28 05:01:21 LTM_A notice mcpd[27545]: 01071432:5: CMI peer connection established to 1.1.1.2 port 6699

Jun 28 05:01:26 LTM_A notice mcpd[27545]: 0107143a:5: CMI reconnect timer: disabled, all peers are connected

Which two commands should be used to obtain additional information on these entries? (Choose two.)

- A. tmsh show /sys mcpd
- B. bigstart status mcpd

- C. tmsh modify /sys db log.mcpd.level value debug
- D. tmsh modify /sys db log.cmi.level value debug

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 344

An LTM Specialist wants to allow access to the Always On Management (AOM) from the network.

Which two methods should the LTM Specialist use to configure the AOM interface? (Choose two.)

- A. Configure the AOM IP from the front panel buttons and LCD.
- B. Choose the network configurator in the AOM menu on the serial port.
- C. Configure the AOM network address in the GUI under System>Platform.
- D. Log in to the Host via ssh, "ssh aom", and modify the network configuration file.

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 345

An LTM Specialist troubleshooting an issue looks at the following /var/log/ltm entries:

```
Oct 2 04:52:42 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 05:37:16 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 05:57:32 slot1/tmm2 crit tmm2[21729]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 06:30:03 slot1/tmm7 crit tmm7[21734]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 06:37:44 slot1/tmm2 crit tmm2[21729]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
Oct 2 06:47:05 slot1/tmm5 crit tmm5[21732]: 01010201:2: Inet port exhaustion on 10.143.109.5 to 10.143.147.150:53 (proto 17)
```

Which configuration item should the LTM Specialist review to fix the issue?

- A. SNAT Pool
- B. Pool Member

- C. Port Lockdown
- D. Virtual Server Port Translation

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 346

An LTM Specialist with the Administrator role and terminal access of "tmsh" logs in via ssh and is in the Traffic Manager Shell. The LTM Specialist wants to enter the bash shell to review log files.

Which command does the LTM Specialist need to run to access the bash shell?

- A. exit
- B. quit
- C. run /cli bash
- D. run /util bash

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 347

Which command will identify the active LTM device currently handling client traffic?

- A. b ha table show
- B. tmsh list /sys ha-status
- C. tmsh show /cm traffic-group
- D. tmsh run /sys failover standby
- E. tmsh show /sys ha-status all-properties

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 348

Which command should an LTM Specialist use on the command line interface to show the health of RAID array hard drives?

- A. tmsh show /sys raid disk
- B. tmsh show /ltm raid disk
- C. tmsh show /sys raid status
- D. tmsh show /ltm disk status

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 349

Which command line interface command will check if the BIG-IP platform contains a packet velocity ASIC (PVA)?

- A. bigpipe platform show | grep -i pva
- B. tmsh show /sys hardware pva status
- C. tmsh show /sys hardware | grep -i pva
- D. tmsh show /ltm hardware | grep -i pva

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 350

Which two subsystems could the LTM Specialist utilize to access an LTM device with lost management interface connectivity? (Choose two.)

- A. AOM
- B. ILO
- C. SCCP

D. ALOM

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 351

A BIG-IP Operator has made a grave error and deleted a few virtual servers on the active LTM device fronting the web browsing proxies. The BIG-IP Operator has NOT yet performed a configuration sync.

Which command should the LTM Specialist execute on the active LTM device to force a failover to the standby node and restore web browsing?

- A. tmsh /sys failover standby
- B. tmsh run /sys failover standby
- C. tmsh /sys failover status standby
- D. tmsh run /sys failover status standby

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 352

The output of a tmsh command is:----- Net::Interface Name Status Bits Bits Errs Errs Drops Drops Colli In Out
In Out In Out sions ----- 1.1 down 0 0 0 0 0 0 0 1.2 up 191.4K 0 0 0 374 0 0 1.3 down 0 0 0 0 0 0 0 1.4 up
22.5K 0 0 0 44 0 0 2.1 miss 0 0 0 0 0 0 0 2.2 miss 0 0 0 0 0 0 0 mgmt up 43.2G 160.0G 0 0 0 0 0

Which command was executed on the LTM device to show the output?

- A. tmsh show /net interface
- B. tmsh /net show interface status
- C. tmsh /net show interface
- D. tmsh show /net interface status

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 353**

When configuring a pool member's monitor, which three association options are available? (Choose three.)

- A. inherit the pool's monitor
- B. inherit the node's monitor
- C. configure a default monitor
- D. assign a monitor to the specific member
- E. do not assign any monitor to the specific member

Correct Answer: ADE

Section: (none)

Explanation**Explanation/Reference:****QUESTION 354**

The current status of a given pool member is unknown - Which condition could explain that state?

- A. The member has no monitor assigned to it.
- B. The member has a monitor assigned to it and the most recent monitor was successful.
- C. The member has a monitor assigned to it and the monitor did not succeed during the most recent timeout period.
- D. The member's node has a monitor assigned to it and the monitor did not succeed during the most recent timeout period.

Correct Answer: A

Section: (none)

Explanation**Explanation/Reference:****QUESTION 355**

The ICMP monitor has been assigned to all nodes. In addition, all pools have been assigned custom monitors. The pool is marked available. In addition, all pools have been assigned custom monitors. If a pool is marked available (green) which situation is sufficient to cause this?

- A. All of the pool member nodes are responding to the ICMP monitor as expected.
- B. Less than 50% of the pool member nodes responded to the ICMP echo request.
- C. All of the members of the pool have had their content updated recently and their responses no longer match the monitor.
- D. Over 25% of the pool members have had their content updated and it no longer matches the receive rule of the custom monitor. The others respond as expected.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 356

Generally speaking, should the monitor templates be used as production monitors or should they be customized prior to use?

- A. Most templates, such as http and tcp, are as effective as customized monitors.
- B. Monitor template customization is only a matter of preference, not an issue of effectiveness or performance.
- C. Most templates, such as https, should have the receive rule customized to make the monitor more robust.
- D. While some templates, such as ftp, must be customized, those that can be used without modification are not improved by specific changes.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 357

You have a pool of servers that need to be tested. All of the servers but one should be tested every 10 seconds, but one is slower and should only be tested every 20 seconds. How do you proceed?

- A. It cannot be done. All monitors test every five seconds.
- B. It can be done, but will require assigning monitors to each pool member.
- C. It cannot be done. All of the members of a pool must be tested at the same frequency.
- D. It can be done by assigning one monitor to the pool and a different monitor to the slower pool member.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is accurated

QUESTION 358

When can a single virtual server be associated with multiple profiles?

- A. Never. Each virtual server has a maximum of one profile.
- B. Often. Profiles work on different layers and combining profiles is common.
- C. Rarely. One combination, using both the TCP and HTTP profile does occur, but it is the exception.
- D. Unlimited. Profiles can work together in any combination to ensure that all traffic types are supported in agiven virtual server.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 359

A site needs a virtual server that will use an iRule to parse HTTPS traffic based on HTTP header values.

Which two profile types must be associated with such a virtual server? (Choose two.)

- A. TCP
- B. HTTP
- C. HTTPS
- D. ServerSSL

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 360

You have created a custom profile named TEST2. The parent profile of TEST2 is named TEST1. If additionalchanges are made to TEST1, what is the effect on TEST2?

- A. All changes to TEST1 are propagated to TEST2.

- B. Some of the changes to TEST1 may propagate to TEST2.
- C. Changes to TEST1 cannot affect TEST2 once TEST2 is saved.
- D. When TEST1 is changed, the administrator is prompted and can choose whether to propagate changes to TEST2.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 361

If a client's browser does not accept cookies, what occurs when the client connects to a virtual server using cookie persistence?

- A. The connection request is not processed.
- B. The connection request is sent to a server.
- C. The connection request is load-balanced to an available pool member.
- D. The connection request is refused and the client is sent a "server not available" message.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 362

Which statement is true concerning cookie persistence?

- A. Cookie persistence allows persistence independent of IP addresses.
- B. Cookie persistence allows persistence even if the data are encrypted from client to pool member.
- C. Cookie persistence uses a cookie that stores the virtual server, pool name, and member IP address in cleartext.
- D. If a client's browser accepts cookies, cookie persistence will always cause a cookie to be written to the client's file system.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 363

Which three iRule events are likely to be seen in iRules designed to select a pool for load balancing? (Choose3)

- A. CLIENT_DATA
- B. SERVER_DATA
- C. HTTP_REQUEST
- D. HTTP_RESPONSE
- E. CLIENT_ACCEPTED
- F. SERVER_SELECTED
- G. SERVER_CONNECTED

Correct Answer: ACE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 364

Which action will take place when a failover trigger is detected by the active system?

- A. The active device will take the action specified for the failure.
- B. The standby device also detects the failure and assumes the active role.
- C. The active device will wait for all connections to terminate and then fail-over.
- D. The standby device will begin processing virtual servers that have failed, but the active device will continueservicing the functional virtual servers.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 365

Assuming that systems are synchronized, which action could take place if the fail-over cable is connectedcorrectly and working properly, but the systems cannot communicate over the network due to external networkproblems?

- A. If network fail-over is enabled, the standby system will assume the active mode.
- B. Whether or not network fail-over is enabled, the standby system will stay in standby mode.

- C. Whether or not network fail-over is enabled, the standby system will assume the active mode.
 D. If network fail-over is enabled, the standby system will go into active mode but only until the network recovers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 366

A virtual server is defined per the charts. The last five client connections were to members C, D, A, B, B. Given the conditions shown in the above graphic, if a client with IP address 205.12.45.52 opens a connection to the virtual server, which member will be used for the connection?

VS_Web_Pool Settings		Web_Pool Parameters	
Destination:	10.10.20.100:80	Load Balancing	Least Connections
Profiles:	TCP, HTTP	Priority Group	
iRules:	None	Activation:	Less Than 2
Default Pool:	Web_Pool	Monitor:	Custom_HTTP
Persistence:	None		

Web_Pool Member Statistics and Settings					
Member	Member Ratio	Member Priority	Outstanding Requests	Current Connections	Status
A: 172.16.20.1:80	3	5	4	56	Unavailable
B: 172.16.20.2:80	3	4	4	42	Available
C: 172.16.20.3:80	3	5	4	54	Unavailable
D: 172.16.20.4:80	1	3	1	22	Available
E: 172.16.20.5:80	1	1	1	18	Available

- A. 172.16.20.1:80
 B. 172.16.20.2:80
 C. 172.16.20.3:80
 D. 172.16.20.4:80
 E. 172.16.20.5:80

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 367

The following iRule is being used within a persistence profile on a virtual server.

Assuming the following HTTP requests are made within the same timeout window, what is the maximum number of persistence records that will be created iRule:

rulePersist_Universal { when HTTP_REQUEST { persist uie [findstr [HTTP ::uri] "?" 8 3] }Requests:

#1 http: l/www.test.com/input.html?testl 45ABR80
#2 http ://www.test.com/input .html?testl 35PDC72
#3 http://www.test.com/input.html?testl 25ABR76
#4 http ://www.test.com/input.html?testl 45MN088
#5 http ://www.test. com/input.html?testl 55ABR98
#6 http://www.test.com/input.html?testl 45PDC6O
#7 http ://www.test. com/input.html?testl 75ABC50
#8 http://www.test.com/input.html?testl 25MN055
#9 http://www.test.com/input.html?testl 45ABC70
#10 http://www.test.com/input.html?testl35 PDC42

- A. 4
- B. 3
- C. 10
- D. It cannot be determined from the given data.
- E. 5
- F. 1
- G. 0

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 368

Why would an administrator capture monitor traffic between a BIG-IP and servers?

- A. Viewing monitor traffic could help the administrator to define a more robust monitor.
- B. If a client were having difficulty logging into a load-balanced SSH server, viewing and analyzing the connection process would determine the reason.
- C. Only client traffic may be captured; monitor traffic may not be captured.
- D. If client traffic to servers was failing, viewing and analyzing monitor traffic would determine the reason.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 369

Which statement is true concerning packet filters?

- A. In addition to administrator-created filters, there always exists a "deny all" filter that processes traffic last.
- B. Filters cannot prevent access to the management port.
- C. The order of filters does not affect which traffic is accepted or denied.
- D. Filters cannot prevent the BIG-IP synching process from taking place.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 370

Which action CANNOT be performed by an iRule?

- A. Direct a connection request to a specific pool.
- B. Substitute a server's response with alternate data.
- C. Change the virtual server's default pool.
- D. Direct a client's request to a pool based on the client's browser's language.
- E. Limit a given client to a set amount of bandwidth.
- F. Discard a client before connecting to a server.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 371

Which persistence method will always recognize a client when the client returns to the same virtual server?

- A. SSL
- B. MSRD
- C. Expression [universal]
- D. No persistence method work in all situations.
- E. Source address

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 372

Which are immediate results of entering the following command: `b pool PoolA .{ lb method predictive member10.10.1 .1:80 member 10.10.1.2:80 }`

- A. Requests sent to this BIG-IP system with a destination port of 80 are load-balanced between the members of PoolA.
- B. No changes will take place since the command is missing the monitor component for PoolA.
- C. The `/config/bigip.cinf` file is updated to include a definition for the pool named PoolA.
- D. A new pool is available for association with any iRule or virtual server.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 373

Given the configuration shown below, if a connection request arrived on the BIG-IP with a source address of 200.10.10.10:1050 and a destination of 150.10.10.75:80, what would the source IP address of the associated packet be when it arrived on the chosen member of the web_pool?

```
self 150.10.10.1 { netmask 255.255.255.0 unit 1 floating enable vlan external allow tcp https } self 10.10.1.1 { netmask 255.255.255.0 unit 1 floating enable vlan internal allow default } pool web_pool { member 10.10.1.11:80 member 10.10.1.12:80 member 10.10.1.13:80 } snat pool client_pool { member 10.10.1.100 }
```

```
member 150.10.10.15 }virtual VS_web { destination 150.10.10.10:80 ip protocol tcp snat automap pool web_pool } virtual VS_network { destination 150.10.10.0: any mask 255.255.255.0 snat pool client_pool ip protocol tcp pool web_pool } virtual VS_network { destination 150.10.10.0: any mask 255.255.255.0 snat pool client_pool ip protocol tcp pool web_pool } virtual VS_network { destination 150.10.10.0: any mask 255.255.255.0 snat pool client_pool ip protocol tcp pool web_pool }
```

- A. 10.10.1.1 A. 10.10.1.1
- B. 200.10.10.10 D. 200.10.10.10
- C. 10.10.1.100 B. 10.10.1.100
- D. 150.10.10.15 C. 150.10.10.15

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

specified answer

QUESTION 374

What occurs when a load config command is issued?

- A. The running configuration is replaced by the any portion of the configuration files that are syntactically correct.
- B. The running configuration is loaded into files for storage
- C. The running configuration is compared to the configuration in files and, when changes are noted, the version in the files is loaded over what is in memory.
- D. The running configuration is replaced by the configuration in the files, but only if they are syntactically correct.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 375

By default, BIG-IP ASM allows which of the following HTTP methods in a client request? (Choose 3)

- A. PUT
- B. GET
- C. POST
- D. HEAD

E. TRACE

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

updated answers

QUESTION 376

The Flow Login feature prevents which web vulnerability from occurring?

- A. Buffer overflow
- B. Cookie poisoning
- C. Forceful browsing
- D. Cross site scripting

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 377

When initially configuring the BIG-IP system using the config utility, which two parameters can be set? (Choose two.)

- A. the netmask of the SCCP
- B. the IP address of the SCCP
- C. the port lockdown settings for the SCCP
- D. the netmask of the host via the management port
- E. the IP address of the host via the management port
- F. the port lockdown settings for the host via the management port

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 378

A site has six members in a pool. All of the servers have been designed, built, and configured with the same applications. It is known that each client's interactions vary significantly and can affect the performance of the servers. If traffic should be sent to all members on a regular basis, which load-balancing mode is most effective if the goal is to maintain a relatively even load across all servers?

- A. Ratio
- B. Priority
- C. Observed
- D. Round Robin

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 379

The incoming client IP address is 205.12.45.52. The last five connections have been sent to members C, D, A, B, B. The incoming client? IP address is 205.12.45.52. The last five connections have been sent to members C, D, A, B, B. Given the virtual server and pool definitions and the statistics shown in the graphic, which member will be used for the next connection?

VS_Web_Pool Settings		Web_Pool Parameters	
Destination:	172.160.22.3:80	Load Balancing:	Least Connections
Profiles:	TCP	Priority Group Activation:	Less Than 2
iRules:	None	Monitor:	None
Default Pool:	Web_Pool		
Persistence:	None		

Web_Pool Member Statistics and Settings					
Member	Member Ratio	Member Priority	Outstanding Requests	Current Connections	Status
A: 10.10.20.1:80	3	5	4	56	Unknown
B: 10.10.20.2:80	3	4	4	57	Unknown
C: 10.10.20.3:80	3	5	4	54	Offline
D: 10.10.20.4:80	1	3	1	2	Unknown
E: 10.10.20.5:80	1	1	1	1	Unknown

- A. 10.10.20.1:80
- B. 10.10.20.2:80
- C. 10.10.20.3:80
- D. 10.10.20.4:80
- E. 10.10.20.5:80

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 380

A site has six members in a pool. Three of the servers are new and have more memory and a faster processor than the others. Assuming all other factors are equal and traffic should be sent to all members, which two load-balancing methods are most appropriate? (Choose two.)

- A. Ratio
- B. Priority
- C. Observed

D. Round Robin

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 381

Which two can be a part of a pool's definition? (Choose two.)

- A. rule(s)
- B. profile(s)
- C. monitor(s)
- D. persistence type
- E. load-balancing mode

Correct Answer: CE

Section: (none)

Explanation

Explanation/Reference:

modified options

QUESTION 382

What is required for a virtual server to support clients whose traffic arrives on the internal VLAN and pool members whose traffic arrives on the external VLAN?

- A. That support is never available.
- B. The virtual server must be enabled for both VLANs.
- C. The virtual server must be enabled on the internal VLAN.
- D. The virtual server must be enabled on the external VLAN.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 383

A standard virtual server has been associated with a pool with multiple members. Assuming all other settings are left at their defaults, which statement is always true concerning traffic processed by the virtual server?

- A. The client IP address is unchanged between the client-side connection and the server-side connection.
- B. The server IP address is unchanged between the client-side connection and the server-side connection.
- C. The TCP ports used in the client-side connection are the same as the TCP ports server-side connection.
- D. The IP addresses used in the client-side connection are the same as the IP addresses used in the server-side connection.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 384

Monitors can be assigned to which three resources? (Choose three.)

- A. NATs
- B. pools
- C. iRules
- D. nodes
- E. SNATs
- F. pool members
- G. virtual servers

Correct Answer: BDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 385

A site has assigned the ICMP monitor to all nodes and a custom monitor, based on the HTTP template, to a pool of web servers. The HTTP-based monitor is working in all cases. The ICMP monitor is failing for 2 of the pool member 5 nodes. All other settings are default. What is the status of the monitor is working in all cases. The ICMP monitor is failing for 2 of the pool member? 5 nodes. All other settings are default. What is the status of the pool members?

- A. All pool members are up since the HTTP-based monitor is successful.
- B. All pool members are down since the ICMP-based monitor is failing in some cases.
- C. The pool members whose nodes are failing the ICMP-based monitor will be marked disabled.
- D. The pool members whose nodes are failing the ICMP-based monitor will be marked unavailable.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 386

A site would like to ensure that a given web server's default page is being served correctly prior to sending it client traffic. They assigned the default HTTP monitor to the pool. What would the member status be if it sent an unexpected response to the GET request?

- A. The pool member would be marked offline (red).
- B. The pool member would be marked online (green).
- C. The pool member would be marked unknown (blue).
- D. The pool member would alternate between red and green.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 387

A site is load balancing to a pool of web servers. Which statement is true concerning BIG-IP's ability to verify whether the web servers are functioning properly or not?

- A. Web server monitors can test the content of any page on the server.
- B. Web server monitors always verify the contents of the index.html page.
- C. Web server monitors can test whether the server's address is reachable, but cannot test a page's content.
- D. Web server monitors can test the content of static web pages, but cannot test pages that would require the web server to dynamically build content.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 388

The current status of a given pool is fflne?(red). Which condition could explain that state? Assume the descriptions below include all monitorsThe current status of a given pool is ?ffline?(red). Which condition could explain that state? Assume the descriptions below include all monitors assigned for each scenario.

- A. No monitors are currently assigned to any pool, member or node.
- B. The pool has a monitor assigned to it, and none of the pool members passed the test.The pool has a monitor assigned to it, and none of the pool? members passed the test.
- C. The pool has a monitor assigned to it, and only some of the pool's members passed the test.
- D. A monitor is assigned to all nodes and all nodes have passed the test. The pool's members have no specific monitor assigned to them.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 389

You need to terminate client SSL traffic at the BIG-IP and also to persist client traffic to the same pool member based on a BIG-IP supplied cookie. Which four are profiles that would normally be included in the virtual server's definition? (Choose four.)

- A. TCP
- B. HTTP
- C. HTTPS
- D. ClientSSL
- E. ServerSSL
- F. Cookie-Based Persistence

Correct Answer: ABDF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 390

A site needs to terminate client HTTPS traffic at the BIG-IP and forward that traffic unencrypted. Which two are profile types that must be associated with such a virtual server? (Choose two.)

- A. TCP
- B. HTTP
- C. HTTPS
- D. ClientSSL
- E. ServerSSL

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 391

Which statement is true concerning SSL termination?

- A. A virtual server that has both ClientSSL and ServerSSL profiles can still support cookie persistence.
- B. Decrypting traffic at the BIG-IP allows the use of iRules for traffic management, but increases the load on the pool member.
- C. When any virtual server uses a ClientSSL profile, all SSL traffic sent to the BIG-IP is decrypted before it is forwarded to servers.
- D. If a virtual server has both a ClientSSL and ServerSSL profile, the pool members have less SSL processing than if the virtual server had only a ClientSSL profile.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 392

A site wishes to perform source address translation on packets from some clients but not others.

The determination is not based on the client's IP address, but on the virtual servers their packets arrive on. What could best accomplish this goal?

- A. A SNAT for all addresses could be defined, and then disable the SNAT processing for select VLANs.
- B. Some virtual servers could be associated with SNAT pools and others not associated with SNAT pools.
- C. The decision to perform source address translation is always based on VLAN. Thus, the goal cannot be achieved.
- D. The decision to perform source address translation is always based on a client's address (or network). Thus, this goal cannot be achieved.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 393

Assume a client's traffic is being processed only by a NAT; no SNAT or virtual server processing takes place. Also assume that the NAT definition specifies a NAT address and an origin address while all other settings are left at their defaults. If a client were to initiate traffic to the NAT address, what changes, if any, would take place when the BIG-IP processes such packets?

- A. The source address would not change, but the destination address would be translated to the origin address.
- B. The destination address would not change, but the source address would be translated to the origin address.
- C. The source address would not change, but the destination address would be translated to the NAT's address.
- D. The destination address would not change, but the source address would be translated to the NAT's address.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 394

A standard virtual server is defined with a pool and a SNAT using automap. All other settings for the virtual server are at defaults. When client traffic is processed by the BIG-IP, what will occur to the IP addresses?

- A. Traffic initiated by the pool members will have the source address translated to a self-IP address but the destination address will not be changed.
- B. Traffic initiated to the virtual server will have the destination address translated to a pool member address and the source address translated to a self-IP address. Traffic initiated to the virtual server will have the destination address translated to a pool member address and the source address translated to a self-IP address.
- C. Traffic initiated by selected clients, based on their IP address, will have the source address translated to a self-IP address but the destination will only be translated if the traffic is destined to the virtual server.
- D. Traffic initiated to the virtual server will have the destination address translated to a pool member address and the source address translated to a self-

IP address. Traffic arriving destined to other destinations will have the source translated to a self-IP address only.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

right answer

QUESTION 395

A standard virtual server is defined with a pool and a SNAT using automap. All other settings for the virtual server are at defaults. When client traffic is processed by the BIG-IP, what will occur to the IP addresses?

- A. Traffic initiated by the pool members will have the source address translated to a self-IP address but the destination address will not be changed.
- B. Traffic initiated to the virtual server will have the destination address translated to a pool member address and the source address translated to a self-IP address.
- C. Traffic initiated by selected clients, based on their IP address, will have the source address translated to a self-IP address but the destination will only be translated if the traffic is destined to the virtual server.
- D. Traffic initiated to the virtual server will have the destination address translated to a pool member address and the source address translated to a self-IP address. Traffic arriving destined to other destinations will have the source translated to a self-IP address only.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 396

Which VLANs must be enabled for a SNAT to perform as desired (translating only desired packets)?

- A. The SNAT must be enabled for all VLANs.
- B. The SNAT must be enabled for the VLANs where desired packets leave the BIG-IP.
- C. The SNAT must be enabled for the VLANs where desired packets arrive on the BIG-IP.
- D. The SNAT must be enabled for the VLANs where desired packets arrive and leave the BIG-IP.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 397

Which two alerting capabilities can be enabled from within an application visibility reporting (AVR) analytics profile? (Choose two.)

- A. sFlow
- B. SNMP
- C. e-mail
- D. LCD panel alert
- E. high speed logging (HSL)

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 398

What is a benefit provided by F5 Enterprise Manager?

- A. Enterprise Manager allows administrators to analyze traffic flow and create custom application IPS signatures.
- B. Enterprise Manager allows administrators to establish baseline application usage and generate an alert if an administratively set threshold for the application is exceeded.
- C. Enterprise Manager allows administrators to identify application vulnerabilities. Virtual patches are then automatically generated and applied to remediate the detected application vulnerability.
- D. Enterprise Manager allows administrators to monitor all application traffic. Configuration optimization suggestions based on the observed traffic patterns are then generated for the administrator to review and apply.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 399

Which two items can be logged by the Application Visibility Reporting analytics profile? (Choose two.)

- A. User Agent
- B. HTTP version
- C. HTTP Response Codes
- D. Per Virtual Server CPU Utilization

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

correct answers

QUESTION 400

Which file should be modified to create custom SNMP alerts?

- A. /config/alert.conf
- B. /etc/alertd/alert.conf
- C. /config/user_alert.conf
- D. /etc/alertd/user_alert.conf

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 401

An LTM Specialist has set up a custom SNMP alert.

Which command line tool should the LTM Specialist use to test the alert?

- A. logger
- B. logtest
- C. testlog
- D. snmptest

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 402

An LTM Specialist is customizing local traffic logging. Which traffic management OS alert level provides the most detail?

- A. Alert
- B. Notice
- C. Critical
- D. Emergency
- E. Informational

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 403

An LTM Specialist must perform a packet capture on a virtual server with an applied standard FastL4 profile. The virtual server 10.0.0.1:443 resides on vlan301.

Which steps should the LTM Specialist take to capture the data payload successfully while ensuring no other virtual servers are affected?

- A. The standard FastL4 profile should have PVA acceleration disabled. Then the packet capture tcpdump -ni vlan301 should be executed on the command line interface.
- B. The packet capture tcpdump -ni vlan301 should be executed on the command line interface.
There is no need to change profiles or PVA acceleration.
- C. A new FastL4 profile should be created and applied to the virtual server with PVA acceleration disabled. Then the packet capture tcpdump -ni vlan301 should be executed on the command line interface.
- D. The LTM device is under light load. The traffic should be mirrored to a dedicated sniffing device. On the sniffing device, the packet capture tcpdump -ni vlan301 should be executed.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 404

A new VLAN vlan301 has been configured on a highly available LTM device in partition ApplicationA. A new directly connected backend server has been placed on vlan301. However, there are connectivity issues pinging the default gateway. The VLAN self IPs configured on the LTM devices are 192.168.0.251 and 192.168.0.252 with floating IP 192.168.0.253. The LTM Specialist needs to perform a packet capture to assist with troubleshooting the connectivity.

Which command should the LTM Specialist execute on the LTM device command line interface to capture the attempted pings to the LTM device default gateway on VLAN vlan301?

- A. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.253'
- B. tcpdump -ni vlan301 'host 192.168.0.253'
- C. tcpdump -ni /ApplicationA/vlan301 'host 192.168.0.251 or host 192.168.0.252'
- D. tcpdump -ni vlan301 'host 192.168.0.251 or host 192.168.0.252'

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 405

An LTM device pool has suddenly been marked down by a monitor. The pool consists of members 10.0.1.1:443 and 10.0.1.2:443 and are verified to be listening. The affected virtual server is 10.0.0.1:80.

Which two tools should the LTM Specialist use to troubleshoot the associated HTTPS pool monitor via the command line interface? (Choose two.)

- A. curl
- B. telnet
- C. ssldump
- D. tcpdump

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 406

An LTM Specialist needs to modify the logging level for tcpdump execution events. Checking the BigDB Key, the following is currently configured:

```
sys db log.tcpdump.level {  
value "Notice"  
}
```

Which command should the LTM Specialist execute on the LTM device to change the logging level to informational?

- A. tmsh set /sys db log.tcpdump.level value informational
- B. tmsh set /sys db log.tcpdump.level status informational
- C. tmsh modify /sys db log.tcpdump.level value informational
- D. tmsh modify /sys db log.tcpdump.level status informational

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 407

An application is configured on an LTM device:

Virtual server: 10.0.0.1:80 (VLAN vlan301)

SNAT IP: 10.0.0.1

Pool members: 10.0.1.1:8080, 10.0.1.2:8080, 10.0.1.3:8080 (VLAN vlan302)

Which packet capture should the LTM Specialist perform on the LTM device command line interface to capture only client traffic specifically for this virtual server?

- A. tcpdump -ni 0.0:nnn -s 0 'host 10.0.0.1' -w /var/tmp/trace.cap
- B. tcpdump -ni vlan301 -s 0 'port 80 and host 10.0.0.1' -w /var/tmp/trace.cap
- C. tcpdump -ni vlan301 -s 0 'port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3' -w /var/tmp/trace.cap
- D. tcpdump -ni vlan302 -s 0 'port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3' -w /var/tmp/trace.cap
- E. tcpdump -ni 0.0:nnn -s 0 '(port 80 and host 10.0.0.1) or (port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 408

Given:

```
Filesystem Size Used Avail Use% Mounted on
/dev/md11 248M 248M 0 100% /
/dev/md13 3.0G 76M 2.8G 3% /config
/dev/md12 1.7G 1.1G 476M 71% /usr
/dev/md14 3.0G 214M 2.6G 8% /var
/dev/md0 30G 2.2G 26G 8% /shared
/dev/md1 6.9G 288M 6.3G 5% /var/log
none 3.9G 452K 3.9G 1% /dev/shm
none 3.9G 19M 3.9G 1% /var/tmstat
none 3.9G 1.2M 3.9G 1% /var/run
prompt 4.0M 12K 4.0M 1% /var/prompt
/dev/md15 12G 8.3G 3.1G 74% /var/lib/mysql
```

Which command is used to produce this output?

- A. df
- B. du
- C. lsof
- D. ps
- E. vmstat

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 409

An LTM Specialist realizes that a datacenter engineer has changed the console baud rate.

Which command determines the current baud rate via the command line interface?

- A. tmsh show /ltm console
- B. tmsh show /sys console
- C. tmsh list /sys baud-rate

D. tmsh list /net baud-rate

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 410

The LTM device is configured for RADIUS authentication. Remote logins are failing and the LTM Specialist must verify the RADIUS configuration.

How should the LTM Specialist check the RADIUS server and shared secret configured on the LTM device?

- A. tmsh show running-config /auth radius
- B. tmsh show running-config /sys auth radius
- C. tmsh show running-config /auth configuration
- D. tmsh show running-config /sys auth radius-server

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 411

An F5 LTM Specialist needs to perform an LTM device configuration backup prior to RMA swap.

Which command should be executed on the command line interface to create a backup?

- A. bigpipe config save /var/tmp/backup.ucs
- B. tmsh save /sys ucs /var/tmp/backup.ucs
- C. tmsh save /sys config /var/tmp/backup.ucs
- D. tmsh save /sys config ucs /var/tmp/backup.ucs

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 412

An LTM Specialist notices the following error on the stdout console:

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

Which command should be executed to verify the LTM device license?

- A. bigpipe version
- B. tmsh show /sys license
- C. tmsh /util bigpipe version
- D. tmsh show /sys license status

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 413

Given the log entry:

```
011f0005:3: HTTP header (32800) exceeded maximum allowed size of 32768 (Client sidE. vip=/Common/VS_web profile=http pool=/Common/POOL_web client_ip=10.0.0.1)
```

Which HTTP profile setting can be modified temporarily to resolve the issue?

- A. Increase Maximum Requests
- B. Decrease Maximum Requests
- C. Increase Maximum Header Count
- D. Decrease Maximum Header Count
- E. Increase Maximum Header size
- F. Decrease Maximum Header size

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

QUESTION 414

Which command should the LTM Specialist use to determine the current system time?

- A. date
- B. time
- C. uname -a
- D. ntpq -p

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 415

An LTM Specialist connects to an LTM device via the serial console cable and receives unreadable output. The LTM Specialist is using the appropriate cable and connecting it to the correct serial port.

Which command should the LTM Specialist run through ssh to verify that the baud rate settings for the serial port are correct on the LTM device?

- A. tmsh list /sys console
- B. tmsh edit /sys console
- C. tmsh show /sys console
- D. tmsh show /ltm console

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 416

Which two can be a part of a virtual server's definition? (Choose two.)

- A. rule(s)
- B. pool(s)

- C. monitor(s)
- D. node address(es)
- E. load-balancing method(s)

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 417

Assume a BIG-IP has no NATs or SNATs configured. Which two scenarios are possible when client traffic arrives on a BIG-IP that is NOT destined to a self-IP? (Choose two.)

- A. If the destination of the traffic does not match a virtual server, the traffic will be discarded.
- B. If the destination of the traffic does not match a virtual server, the traffic will be forwarded based on routing tables.
- C. If the destination of the traffic matches a virtual server, the traffic will be processed per the virtual server definition.
- D. If the destination of the traffic matches a virtual server, the traffic will be forwarded, but it cannot be load balanced since no SNAT has been configured.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 418

The active LTM device in a high-availability (HA) pair performs a failover at the same time the network team reports an outage of a switch on the network.

Which two items could have caused the failover event? (Choose two.)

- A. a VLAN fail-safe setting
- B. a monitor on a pool in an HA group
- C. the standby LTM that was rebooted
- D. an Auditor role that has access to the GUI
- E. the standby LTM that lost connectivity on the failover VLAN

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 419

An active/standby pair of LTM devices deployed with network failover are working as desired. After external personnel perform maintenance on the network, the LTM devices are active/active rather than active/standby. No changes were made on the LTM devices during the network maintenance.

Which two actions would help determine the cause of the malfunction? (Choose two.)

- A. checking that the configurations are synchronized
- B. checking the configuration of the VLAN used for failover
- C. checking the configuration of the VLAN used for mirroring
- D. checking the open ports in firewalls between the LTM devices
- E. checking synchronization of system clocks among the network devices

Correct Answer: BD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 420

Given LTM device ltm log:

```
Sep 26 20:51:08 local/lb-d-1 notice promptstatusd[3695]: 01460006:5: semaphore mcpd.running(1) held
Sep 26 20:51:08 local/lb-d-1 notice promptstatusd[3695]: 01460006:5:
Sep 26 20:51:08 local/lb-d-1 warning promptstatusd[3695]: 01460005:4: mcpd.running(1) held, wait for mcpd
Sep 26 20:51:08 local/lb-d-1 info sod[3925]: 010c0009:6: Lost connection to mcpd - reestablishing.
Sep 26 20:51:08 local/lb-d-1 err bcm56xxd[3847]: 012c0004:3: Lost connection with MCP:
16908291 ... Exiting bsx_connect.cpp(174)
Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0012:6: MCP Exit Status Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0012:6: Info:
LACP stats (time now:1348717868) : no traffic
Sep 26 20:51:08 local/lb-d-1 info bcm56xxd[3847]: 012c0014:6: Exiting... Sep 26 20:51:08 local/lb-d-1 err lind[3842]: 013c0004:3: IO error on recv from
mcpd - connection lost
Sep 26 20:51:08 local/lb-d-1 notice bigd[3837]: 01060110:5: Lost connection to mcpd with error 16908291, will reinit connection.
Sep 26 20:51:08 local/lb-d-1 err statsd[3857]: 011b0004:3: Initial subscription for system configuration failed with error "
Sep 26 20:51:08 local/lb-d-1 err statsd[3857]: 011b0001:3: Connection to mcpd failed with error '011b0004:3: Initial subscription for system configuration
```

failed with error "" Sep 26 20:51:08 local/lb-d-1 err csyncd[3851]: 013b0004:3: IO error on recv from mcpd - connection lost
.....skipping more logs.....
Sep 26 20:51:30 local/lb-d-1 notice sod[3925]: 01140030:5: HA proc_running bcm56xxd is now responding.
Sep 26 20:51:34 local/lb-d-1 notice sod[3925]: 01140030:5: HA proc_running mcpd is now responding.
Sep 26 20:51:34 local/lb-d-1 notice sod[3925]: 010c0018:5: Standby

Which daemon failed?

- A. promptstatusd
- B. mcpd
- C. sod
- D. bcm56xxd
- E. lind

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 421

In preparation for a maintenance task, an LTM Specialist performs a "Force to Standby" on LTM device Unit 1. LTM device Unit 2 becomes active as expected. The maintenance task requires the reboot of Unit 1. Shortly after the reboot is complete, the LTM Specialist discovers that Unit 1 has become active and Unit 2 has returned to standby.

What would cause this behavior?

- A. Unit 1 is set with the redundancy state preference of active in devices groups.
- B. Unit 1 is set with the redundancy state preference of active in high availability.
- C. A traffic group is configured with Auto Failback, and Unit 1 is the default device.
- D. A device group is configured with Auto Failback, and Unit 1 is the default device.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 422

A high-availability (HA) pair configuration uses only the hardwire serial cable connection to determine device state. A power outage occurs to the PDU powering the active unit. The standby unit takes over the active role as expected.

How is the peer unit able to determine the active unit is unavailable?

- A. voltage loss on serial cable
- B. no data stream received on serial port
- C. no response on management interface
- D. no heartbeat packets received on self IPs

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 423

-- Exhibit

```

ltm node /test/10.1.1.1 {
    address 10.1.1.1
}
ltm node /test/10.1.1.2 {
    address 10.1.1.2
}
ltm node /test/10.1.1.3 {
    address 10.1.1.3
}
ltm pool /test/test1_pool {
    members {
        /test/10.1.1.1:80 {
            address 10.1.1.1
        }
        /test/10.1.1.2:8080 {
            address 10.1.1.2
        }
    }
}
ltm pool /test/test2_pool {
    members {
        /test/10.1.1.1:8080 {
            address 10.1.1.1
        }
        /test/10.1.1.3:8080 {
            address 10.1.1.3
        }
    }
}
ltm virtual /test/test1_vs {
    destination /test/172.16.20.1:80
    ip-protocol tcp
    mask 255.255.255.255
    pool /test/test2_pool
    profiles {
        /Common/http { }
        /Common/tcp { }
    }
    translate-address enabled
    translate-port enabled
    vlans-disabled
}
ltm virtual-address /test/172.16.20.1 {
    address 172.16.20.1
    mask 255.255.255.255
    traffic-group /Common/traffic-group-1
}

```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is reviewing the 'test' partition.

Which objects, in order, can be removed from the partition?

- A. delete pool test1_pool, delete node 10.1.1.2
- B. delete node 10.1.1.2, delete pool test2_pool
- C. delete pool test1_pool, delete node 10.1.1.2, delete node 10.1.1.1
- D. delete virtual test1_vs, delete pool test2_pool, delete node 10.1.1.1
- E. delete pool test1_pool, delete pool test2_pool, delete node 10.1.1.3

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 424

-- Exhibit

```

itm rule /Common/vs1-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs1") && not ([HTTP::uri] starts_with "/app") } {
HTTP::redirect "https://vs1/app/"
return
}
}
}

itm rule /Common/vs2-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs2") && not ([HTTP::uri] starts_with "/app4") } {
HTTP::redirect "https://vs2/app4/"
return
}
}
}

itm rule /Common/vs3-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs3") && not ([HTTP::uri] starts_with "/app2") } {
HTTP::redirect "https://vs3/app2/"
return
}
}
}

itm rule /Common/vs4-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs4") && not ([HTTP::uri] starts_with "/app") } {
HTTP::redirect "https://vs4/app/"
return
}
}
}

itm rule /Common/vs5-https-redirect {
when HTTP_REQUEST {
if { not ([HTTP::host] eq "vs5") && not ([HTTP::uri] starts_with "/app3") } {
HTTP::redirect "https://vs5/app3/"
return
}
}
}

```

-- Exhibit --

Refer to the exhibit.

Which two items can be consolidated to simplify the LTM configuration? (Choose two.)

- A. /Common/vs1-https-redirect
- B. /Common/vs2-https-redirect
- C. /Common/vs3-https-redirect
- D. /Common/vs4-https-redirect
- E. /Common/vs5-https-redirect

Correct Answer: AD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 425

-- Exhibit

Data Format		Normalized												
Auto Refresh		Disabled												
		Refresh												
		Search												
				Bits		Packets		Connections			Requests		Request Queue	
<input checked="" type="checkbox"/>	Status	Pool/Member	Partition / Path	In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum	
<input type="checkbox"/>		DNS_pool	Common	0	0	0	0	0	0	0		0	0	
<input type="checkbox"/>		-- 172.16.20.1:53	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		-- 172.16.20.2:53	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		-- 172.16.20.3:53	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		ecomm_pool	Common	21.6K	60.2K	20	16	0	1	2		0	0	
<input type="checkbox"/>		-- ecomm_server:80	Common	21.6K	60.2K	20	16	0	1	2	5	0	0	
<input type="checkbox"/>		ftp_pool	Common	10.9K	8.9K	24	15	1	1	1		0	0	
<input type="checkbox"/>		-- 172.16.20.1:21	Common	10.9K	8.9K	24	15	1	1	1	0	0	0	
<input type="checkbox"/>		-- 172.16.20.2:21	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		-- 172.16.20.3:21	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		hello_world_pool	Common	0	0	0	0	0	0	0		0	0	
<input type="checkbox"/>		-- ecomm_server:81	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		http_pool	Common	142.2K	1.5M	137	173	0	6	10		0	0	
<input type="checkbox"/>		-- 172.16.20.1:80	Common	43.6K	639.1K	48	66	0	2	3	6	0	0	
<input type="checkbox"/>		-- 172.16.20.2:80	Common	30.7K	369.8K	34	44	0	2	3	4	0	0	
<input type="checkbox"/>		-- 172.16.20.3:80	Common	67.8K	537.2K	55	63	0	2	4	11	0	0	
<input type="checkbox"/>		iOS_pool	Common	0	0	0	0	0	0	0		0	0	
<input type="checkbox"/>		-- ecomm_server:82	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		server1_80	Common	24.9M	190.0M	56.4K	56.3K	0	1	9.5K		0	0	
<input type="checkbox"/>		-- 172.16.20.1:80	Common	24.9M	190.0M	56.4K	56.3K	0	1	9.5K	0	0	0	
<input type="checkbox"/>		server2_80_pool	Common	24.0M	190.1M	56.3K	56.6K	0	1	9.3K		0	0	
<input type="checkbox"/>		-- 172.16.20.2:80	Common	24.8M	190.1M	56.3K	56.6K	0	1	9.5K	0	0	0	
<input type="checkbox"/>		server_pool	Common	0	0	0	0	0	0	0		0	0	
<input type="checkbox"/>		-- 172.16.20.1:0	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		-- 172.16.20.2:0	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		-- 172.16.20.3:0	Common	0	0	0	0	0	0	0	0	0	0	
<input type="checkbox"/>		webgoat_pool	Common	0	0	0	0	0	0	0		0	0	
<input type="checkbox"/>		-- webgoat_8080:8080	Common	0	0	0	0	0	0	0	0	0	0	

-- Exhibit --
Refer to the exhibit.

Which pool can be removed without affecting client traffic?

- A. ftp_pool
- B. http_pool
- C. server1_80
- D. server_pool

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 426

-- Exhibit --

The exhibit consists of four screenshots from a Cisco ASA configuration interface, showing various profile settings.

Profile: http

Class Profile Statistics

Current Rate

Queue	Count
Accepted	693
Not Accepted	0
Discarded	40
Full	0
HTTP	0
Adaptive	0

Miscellaneous

Receive: Rate	Count
Not Accepted	0
Discarded	0
Full	0
HTTP	0
Adaptive	0

Configuration (Advanced)

Profile: http

Protocol Profile: http

Class Profile Statistics

Current Rate

Queue	Count
Accepted	693
Not Accepted	0
Discarded	40
Full	0
HTTP	0
Adaptive	0

Miscellaneous

Receive: Rate	Count
Not Accepted	0
Discarded	0
Full	0
HTTP	0
Adaptive	0

Profile: https

Class Profile Statistics

Current Rate

Queue	Count
Accepted	693
Not Accepted	0
Discarded	40
Full	0
HTTP	0
Adaptive	0

Miscellaneous

Receive: Rate	Count
Not Accepted	0
Discarded	0
Full	0
HTTP	0
Adaptive	0

Profile: ftp

Class Profile Statistics

Current Rate

Queue	Count
Accepted	693
Not Accepted	0
Discarded	40
Full	0
HTTP	0
Adaptive	0

Miscellaneous

Receive: Rate	Count
Not Accepted	0
Discarded	0
Full	0
HTTP	0
Adaptive	0

-- Exhibit --

Refer to the exhibit.

Which profile could be removed or changed on this virtual server to reduce CPU load on the LTM device without increasing server side bandwidth usage?

- A. tcp
- B. http
- C. httpcompression
- D. optimized-caching

Correct Answer: C

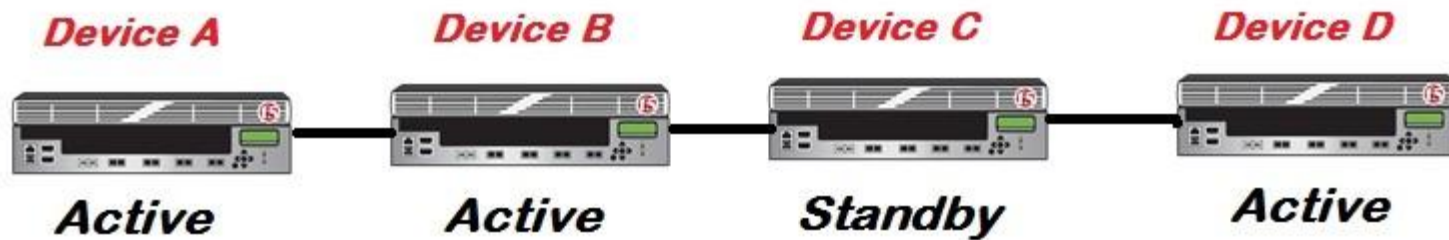
Section: (none)

Explanation

Explanation/Reference:

QUESTION 427

-- Exhibit



-- Exhibit --

Refer to the exhibit.

An LTM Specialist is upgrading the LTM devices.

Which device should be upgraded first?

- A. Device A
- B. Device B
- C. Device C
- D. Device D

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 428

-- Exhibit

An SSH configuration error exposes a potential vulnerability - CVE-2012-1493

Recommended upgrade version
10.2.4 11.0.0.HF2 11.1.0.HF3 11.2.0

Solution Links
[SOL13600](#)

Heuristic Name
H386652

Was this helpful?
👍 Yes 👎 No

[Details](#)

Related Changes
ID 379600

Description
An SSH configuration error in the default SSH configuration may allow unauthorized remote users to gain privileged access to the system.

Recommendation resolution
Upgrade to an unaffected version. For workaround information, refer to the linked Solution.

Additional Information
The current configuration appears to be vulnerable.

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is working on an LTM 11.0.0 installation and has identified a security vulnerability as shown in the exhibit. The LTM Specialist is tasked with applying the latest available hotfix to resolve the problem.

Which procedure resolves the problem?

- A. Browse to System > Software Management > Hotfix List.
Import TMOS 11.2.0 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.
- B. Browse to System > Software Management > Hotfix List.
Import 11.1.0.HF3 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.
- C. Browse to System > Software Management > Image List.
Import TMOS 11.2.0 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.
- D. Browse to System > Software Management > Image List.
Import 11.1.0.HF3 to the available hotfix images.
Select the imported hotfix image and installation location and click Install.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 429

-- Exhibit

Hostname: VTI-UEH-A-001 Date: Oct 17, 2012 User: admin
 IP Address: 10.0.0.201 Time: 1:12 PM (EST) Role: Administrator Partition: Common Log out

f5 1100 MB (All) (N/A)
 Not All Devices Synced

Main Help About

Statistics
 App
 Wizards
 Global Traffic
 Local Traffic
 Access Policy
 Device Management
 Network
 System

System >> Software Management: Image List

Image List Hosts List Antivirus Check Updated Boot Locations

Installed Images

Product	Version	Build	Disk	Boot Location	Active	Media	Install Status
B-G-P	11.2.1	797.0	HD1	HD1.1	Yes	hd	complete
U-G-P	11.1.0	2260.0	HD1	HD1.2	No	hd	complete
D-G-P	11.2.1	797.0	HD1	HD1.3	No	hd	complete

Available Images Import

Status	Software Image	Version	Last Modified	Image Size	MD5 Verified	Available
<input checked="" type="checkbox"/>	BIGIP-11.1.0-1943.0.iso	11.1.0	Tue Oct 2 10:37:31 2012	1012 MB	Yes	Yes
<input checked="" type="checkbox"/>	BIGIP-11.2.1-797.0.iso	11.2.1	Wed Sep 26 13:19:27 2012	1213 MB	Yes	Yes

Delete Install

Configuration
 Device Configuration
 File Management
 Disk Management
Software Management
 License
 Resource Provisioning
 Platform
 High Availability
 Archives
 Services
 Preferences
 Performance
 SNMP

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has uploaded a qkview to F5 iHealth.

Within the GUI, what is the correct procedure to comply with the recommendation shown in the exhibit?

- A. Obtain product version image from release.f5.com.
Overwrite existing image with new product version image.
Select product version image and click Install.
Select the available disk and volume set name.
- B. Obtain product version image from images.f5.com.
Overwrite existing image with new product version image.
Select product version image and click Install.
Select the available disk and volume set name.
- C. Obtain product version image from downloads.f5.com.
Import product version image.
Install image onto BIG-IP platform.
Select product version image and click Install.
Select the available disk and volume set name.
- D. Log a call requesting the product version image via websupport.f5.com Import product version image.
Install image onto BIG-IP platform.
Select product version image and click Install.
Select the available disk and volume set name.

Correct Answer: C








Section: (none)

Explanation

Explanation/Reference:

QUESTION 430

-- Exhibit

Status	
Diagnostics	
Results	 3 High  1 Medium  2 Low
Recommendation	 Upgrade to version: 11.2.0 or higher
Status	 No new potential issues identified since last update.
Errors	
Extraction	 No errors during QKView extraction.
Diagnostics	 No errors during diagnostics run.

-- Exhibit --

Refer to the exhibit.

Which step should an LTM Specialist take next to finish upgrading to HD1.3?

- A. Install image to HD1.3
- B. Install hotfix to HD1.3
- C. Activate HD1.3
- D. Relicense HD1.3

Correct Answer: C

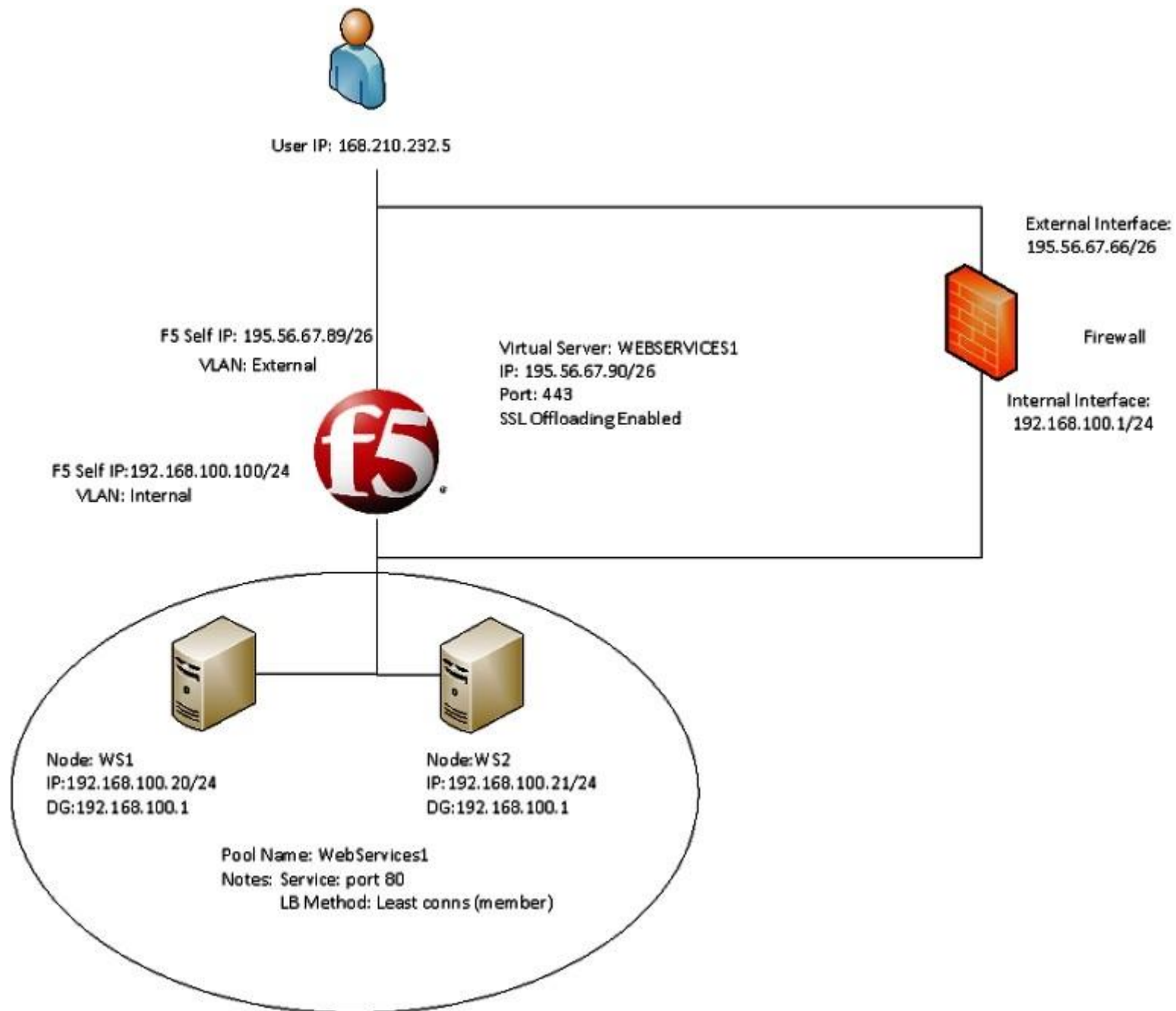
Section: (none)

Explanation

Explanation/Reference:

QUESTION 431

-- Exhibit



-- Exhibit --

Refer to the exhibit.

Users receive an error when attempting to connect to the website <https://website.com>. The website has a DNS record of 195.56.67.90. The upstream ISP has confirmed that there is nothing wrong with the routing between the user and the LTM device.

The following tcpdump outputs have been captured:

External Vlan, filtered on IP 168.210.232.5

00:25:07.598519 IP 168.210.232.5.33159 > 195.56.67.90.https: S 1920647964:1920647964(0) win 8192 <mss 1450,nop,nop,sackOK>

00:25:07.598537 IP 195.56.67.90.https > 168.210.232.5.33159: S 2690691360:2690691360(0) ack 1920647965 win 4350 <mss 1460,sackOK,eol>

00:25:07.598851 IP 168.210.232.5.33160 > 195.56.67.90.https: S 2763858764:2763858764(0) win 8192 <mss 1450,nop,nop,sackOK>

00:25:07.598858 IP 195.56.67.90.https > 168.210.232.5.33160: S 1905576176:1905576176(0) ack 2763858765 win 4350 <mss 1460,sackOK,eol>

Internal Vlan, filtered on IP 168.210.232.5

00:31:46.171124 IP 168.210.232.5.33202 > 192.168.100.20.http: S 2389057240:2389057240(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>

What is the problem?

- A. The filters on the tcpdumps are incorrect.
- B. The DNS entry for website.com is incorrect.
- C. The virtual server 'WEBSERVICES1' is listening on the incorrect port.
- D. The firewall is dropping the connection coming from the pool members returned to the client.
- E. The subnet masks of the pool members of pool WebServices1 and the f5 'Internal' Vlan are incorrect.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 432

-- Exhibit

```

1 1 0.2423 (0.2423) C>S Handshake
    ClientHello
        Version 3.2
        cipher suites
            TLS_DHE_RSA_WITH_AES_256_CBC_SHA
            TLS_DHE_DSS_WITH_AES_256_CBC_SHA
            TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
            TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
            NULL
Unknown SSL content type 72
1 2 0.2432 (0.0008) S>CShort record
1 0.2432 (0.0000) S>C TCP FIN
New TCP connection #2: 168.210.232.5(24782) <->
193.33.229.103(443)
2 1 0.2393 (0.2393) C>S Handshake
    ClientHello
        Version 3.2
        cipher suites
            TLS_DHE_RSA_WITH_AES_256_CBC_SHA
            TLS_DHE_DSS_WITH_AES_256_CBC_SHA
            TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
            TLS_RSA_WITH_3DES_EDE_CBC_SHA
        compression methods
            NULL
Unknown SSL content type 72
2 2 0.2404 (0.0010) S>CShort record
2 0.2404 (0.0000) S>C TCP FIN
2 3 0.4738 (0.2333) C>S Alert
    level          fatal
    value          unexpected_message
2 0.4742 (0.0003) C>S TCP FIN
1 3 0.4857 (0.2425) C>S Alert
    level          fatal
    value          unexpected_message
1 0.4857 (0.0000) C>S TCP FIN

```

-- Exhibit --

Refer to the exhibit.

A client attempts to connect from a Google Chrome browser to a virtual server on a BIG-IP LTM. The virtual server is SSL Offloaded. When the client connects, the client receives an SSL error. After trying Mozilla Firefox and Internet Explorer browsers, the client still receives the same errors.

The LTM Specialist does an ssldump on the virtual server and receives the results as per the exhibit.
What is the problem?

- A. The SSL key length is incorrect.
- B. The BIG-IP LTM is NOT serving a certificate.
- C. The BIG-IP LTM is NOT listening on port 443.
- D. The client needs to be upgraded to the appropriate cipher-suite.

Correct Answer: B

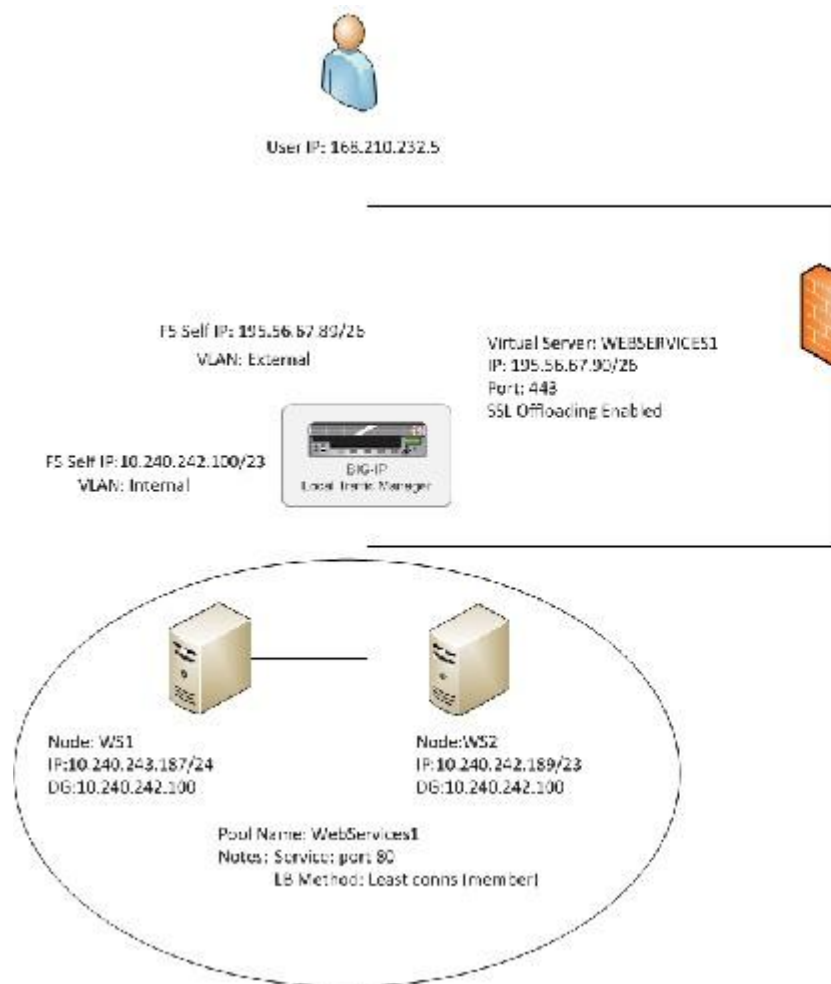
Section: (none)

Explanation

Explanation/Reference:

QUESTION 433

-- Exhibit



External Vlan tcpdump

```
22:28:27.689421 IP 168.210.232.5.27820 > 195.56.67.90.https: S 4159851702:4159851702(0) win 5192 <msg 1450,nop,nop,sackOK>
22:28:27.689433 IP 195.56.67.90.https > 168.210.232.5.27820: S 876741540:876741540(0) ack 4159851703 win 4350 <msg 1460,sackOK,e
22:28:27.819524 IP 168.210.232.5.27820 > 195.56.67.90.https: .ack 1 win 1450
22:28:27.921141 IP 168.210.232.5.27820 > 195.56.67.90.https: P 1:104(103) ack 1 win 65250
22:28:27.922822 IP 195.56.67.90.https > 168.210.232.5.27820: P 1:506(505) ack 104 win 4453
22:28:27.922899 IP 195.56.67.90.https > 168.210.232.5.27820: F 506:506(0) ack 104 win 4453
```

Internal Vlan tcpdump

```
22:35:17.858896 IP 168.210.232.5.27820 > 10.240.242.189.http: S 3302554564:3302554564(0) win 4380 <msg 1460,nop,wscale 0,sackOK,eol
22:35:17.862769 IP 10.240.242.189.http > 168.210.232.5.27820: S 4222809244:4222809244(0) ack 3302554565 win 65535 <msg 1310,nop,w
0,nop,nop,sackOK>
22:35:17.862786 IP 168.210.232.5.27820 > 10.240.242.189.http: .ack 1 win 4380
22:35:36.836155 IP 168.210.232.5.33202 > 10.240.243.187.http: S 2389057240:2389057240(0) win 4380 <msg 1460,nop,wscale 0,sackOK,eol
```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist has a virtual server set up on the LTM device as per the exhibit. The LTM Specialist receives reports of intermittent issues. Some clients are connecting fine while others are failing to connect.

The LTM Specialist does a tcpdump on the relevant interfaces, with the following results extracted:
What is causing the intermittent issues?

- A. The firewall is dropping the packets from WS1.
- B. The default gateway is inaccessible from WS1.
- C. The load balancing (LB) method is inappropriate.
- D. The pool members have been set up as an active/standby pair, with WS1 as the standby.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 434

-- Exhibit

External Vlan tcpdump:

```
16:38:10.184240 IP 168.210.232.5.59156 > 66.212.246.58.1990: S 1208467898:1208467898(0) win 8192 <mss 1380,nop,wscale 8,ncp,nop,sackOK>
16:38:10.184249 IP 66.212.246.58.1990 > 168.210.232.5.59156: S 2009182511:2009182511(0) ack 1208467899 win 4140 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:10.454030 IP 168.210.232.5.59156 > 66.212.246.58.1990: . ack 1 win 5
16:38:52.809723 IP 168.210.232.5.31084 > 66.212.246.58.1991: S 2991752264:2991752264(0) win 8192 <mss 1380,nop,wscale 8,ncp,nop,sackOK>
16:38:52.809734 IP 66.212.246.58.1991 > 168.210.232.5.31084: S 2217364875:2217364875(0) ack 2991752265 win 4140 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:52.737749 IP 168.210.232.5.59172 > 66.212.246.58.2002: S 3158709238:3158709238(0) win 8192 <mss 1380,nop,wscale 8,ncp,nop,sackOK>
16:38:52.737766 IP 66.212.246.58.2002 > 168.210.232.5.59172: S 7716150:7716150(0) ack 3158709239 win 4140 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.007421 IP 168.210.232.5.59172 > 66.212.246.58.2002: . ack 1 win 5
16:38:53.078216 IP 168.210.232.5.31084 > 66.212.246.58.1991: . ack 1 win 5
16:43:21.434766 IP 168.210.232.5.59156 > 66.212.246.58.1990: R 830:830(0) ack 94934 win 0
```

Internal Vlan tcpdump:

```
16:38:11.007217 IP 168.210.232.5.10033 > 10.240.243.65.1989: S 2408612037:2408612037(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:11.887559 IP 10.240.243.65.1989 > 168.210.232.5.10033: S 165435577:165435577(0) ack 2408612038 win 8192 <mss 1310,nop,nop,sackOK>
16:38:11.887566 IP 168.210.232.5.10033 > 10.240.243.65.1989: . ack 1 win 4380
16:38:53.007459 IP 168.210.232.5.59172 > 10.240.243.66.2002: S 26149351:26149351(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.007908 IP 10.240.243.66.2002 > 168.210.232.5.59172: S 3880985485:3880985485(0) ack 26149352 win 8192 <mss 1310,nop,nop,sackOK>
16:38:53.007916 IP 168.210.232.5.59172 > 10.240.243.66.2002: . ack 1 win 4380
16:38:53.078499 IP 168.210.232.5.31084 > 10.240.242.197.1991: S 2788170026:2788170026(0) win 4380 <mss 1460,nop,wscale 0,sackOK,eol>
16:38:53.078861 IP 10.240.242.197.1991 > 168.210.232.5.31084: S 2169754248:2169754248(0) ack 2788170027 win 8192 <mss 1310,nop,wscale 8,nop,nop,sackOK>
16:38:53.078871 IP 168.210.232.5.31084 > 10.240.242.197.1991: . ack 1 win 4380
16:43:29.434782 IP 168.210.232.5.10033 > 10.240.243.65.1989: R 181:181(0) ack 88278 win 53535
```

-- Exhibit --

Refer to the exhibit.

A company uses a complex piece of client software that connects to one or more virtual servers (VS) hosted on an LTM device. The client software is experiencing issues. An LTM Specialist is tasked with finding the cause of the problem.

The LTM Specialist has the tcpdump extract and knows the client software has at least one connection to a VS on port 1990. However, when a tcpdump runs on the internal VLAN, there is no record of port 1990 in the tcpdump.

Why is there no record of port 1990 in the tcpdump?

- A. The LTM device drops the connection.
- B. Port 1990 is a well-known port, so its use is restricted.
- C. The LTM device performs a Port Address Translation (PAT).
- D. The LTM device performs a Network Address Translation (NAT).

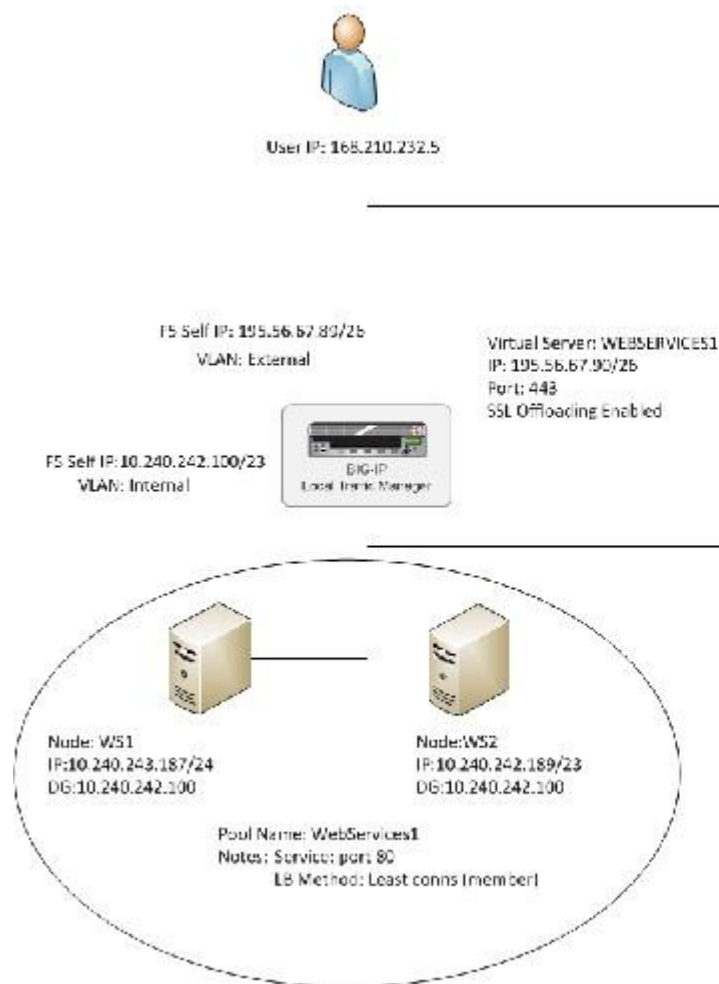
Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

-- Exhibit --



External Vlan tcpdump

```
22:28:27.689421 IP 168.210.232.5.27820 > 195.56.67.90.https: S 4159851702:4159851702(0) win 5192 <msg 1450,nop,nop,sackOK>
22:28:27.689433 IP 195.56.67.90.https > 168.210.232.5.27820: S 876741540:876741540(0) ack 4159851703 win 4350 <msg 1460,sackOK,e
22:28:27.819524 IP 168.210.232.5.27820 > 195.56.67.90.https: .ack 1 win 1450
22:28:27.921141 IP 168.210.232.5.27820 > 195.56.67.90.https: P 1:104(103) ack 1 win 65250
22:28:27.922822 IP 195.56.67.90.https > 168.210.232.5.27820: P 1:506(505) ack 104 win 4453
22:28:27.922899 IP 195.56.67.90.https > 168.210.232.5.27820: F 506:506(0) ack 104 win 4453
```

Internal Vlan tcpdump

```
22:35:17.858896 IP 168.210.232.5.27820 > 10.240.242.189.http: S 3302554564:3302554564(0) win 4380 <msg 1460,nop,wscale 0,sackOK,eol
22:35:17.862769 IP 10.240.242.189.http > 168.210.232.5.27820: S 4222909244:4222909244(0) ack 3302554565 win 65535 <msg 1310,nop,w
0,nop,nop,sackOK>
22:35:17.862786 IP 168.210.232.5.27820 > 10.240.242.189.http: .ack 1 win 4380
22:35:36.836255 IP 168.210.232.5.33202 > 10.240.242.187.http: S 2389057240:2389057240(0) win 4380 <msg 1460,nop,wscale 0,sackOK,eol
```

-- Exhibit --

Refer to the exhibit.

A company uses a complex piece of client software that connects to one or more virtual servers hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem.

The LTM Specialist has the tcpdump extract and knows the client source IP is 168.210.232.5.

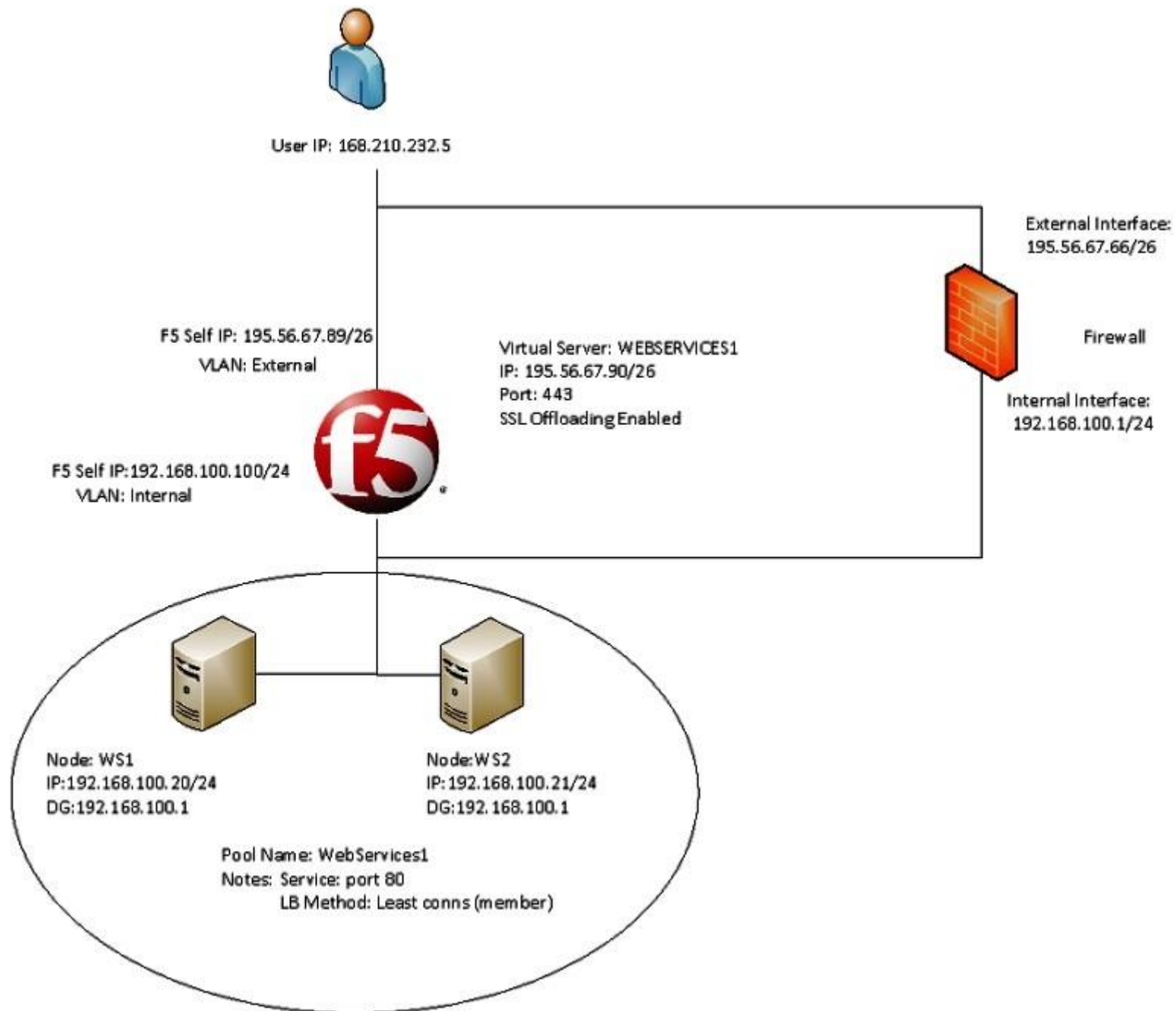
Assuming no wildcard virtual servers, how many distinct virtual servers does the client connect to on the LTM device?

- A. 2
- B. 3
- C. 4
- D. 6

Answer: B

QUESTION 435

-- Exhibit --



-- Exhibit --

Refer to the exhibit.

A company uses a complex piece of client software that connects to one or more virtual servers (VS) hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem.

The LTM Specialist is seeing a client source IP of 168.210.232.5 in the tcpdump. However, the client source IP is actually 10.123.17.12.

Why does the IP address of 10.123.17.12 fail to appear in the tcpdump?

- A. The LTM device performed NAT on the individual's IP address.
- B. The Secure Network Address Translation (SNAT) pool on the virtual server is activated.
- C. Network Address Translation (NAT) has occurred in the path between the client and the LTM device.
- D. The individual's data stream is being routed to the LTM device by a means other than the default route.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 436

-- Exhibit --

New TCP connection #3: 172.16.1.20(49379) <-> 172.16.20.1(443)

3 1 0.0006 (0.0006) C>S Handshake

ClientHello

Version 3.1

cipher suites

TLS_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

Unknown value 0x3c

Unknown value 0x3d

Unknown value 0xff

compression methods

NULL

3 2 0.0009 (0.0002) S>C Handshake

ServerHello

Version 3.1

session_id[32]=

ed 15 16 5f c2 9d bf 5e e6 70 0e a4 86 59 bf 27

e7 b5 fa 49 38 fd 24 d7 c3 1e c1 9f d2 67 e4 f7

cipherSuite TLS_RSA_WITH_RC4_128_SHA

compressionMethod NULL

3 3 0.0009 (0.0000) S>C Handshake

Certificate

3 4 0.0009 (0.0000) S>C Handshake

ServerHelloDone

New TCP connection #4: 172.16.1.20(49380) <-> 172.16.20.1(443)

4 1 0.0004 (0.0004) C>S Handshake

ClientHello

Version 3.1

cipher suites

TLS_RSA_WITH_RC4_128_SHA

TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_3DES_EDE_CBC_SHA

Unknown value 0x3c

Unknown value 0x3d

Unknown value 0xff

compression methods

NULL

4 2 0.0007 (0.0002) S>C Handshake

ServerHello

Version 3.1

session_id[32]=

f5 eb fe e9 8e fc e9 7f c5 13 1b 40 69 15 08 72

-- Exhibit --

Refer to the exhibit.

A company uses a complex piece of client software that connects to one or more virtual servers (VS) hosted on an LTM device. The client software is experiencing issues. An LTM Specialist must determine the cause of the problem. The LTM Specialist has the tcpdump extract. The client loses connection with the LTM device.

Where is the reset originating?

- A. the local switch
- B. the application server
- C. the device initiating the connection
- D. the destination device of the initial connection

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 437

-- Exhibit

Virtual Server details

Type	Standard
Protocol	TCP
Protocol Profile (Client)	tcp-wan-optimised
Protocol Profile (Server)	tcp-lan-optimised
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	None
FTP Profile	None
Stream Profile	None
XML Profile	None
SSL Profile (Client)	None
SSL Profile (Server)	None
Authentication Profiles	None
RTSP Profile	None
SMTP Profile	None
Diameter Profile	None
SIP Profile	None
Statistics Profile	None
SNAT Pool	None
Rate Class	None
Traffic Class	None
Connection Limit	None
Connection Mirroring	None
Address Translation	Enabled
Port Translation	Enabled
Source Port	Preserve
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None

Pool details:

10.40.242.12: 443
10.40.242.13: 443

-- Exhibit --

Refer to the exhibit.

An LTM device is used to load balance web content over a secure channel.

The developers of the web content have done a trace using an HTTP profiler application. They believe that allowing the LTM device to compress traffic to the client will improve performance. The client can utilize GZIP or deflate compression algorithms.

An LTM Specialist must implement the compression.

The LTM Specialist has completed the following actions:

1. Create the relevant profile.
2. Apply the relevant profile to the virtual server (VS).

After applying the relevant profile, the LTM device is failing to compress the traffic. Instead, the traffic is being served with an error.

What is the problem?

- A. The incorrect compression algorithm is applied to the compression profile.
- B. The LTM device CANNOT SSL offload the traffic in order to read and compress it.
- C. The Protocol Profile (Client) option of "Allow Compression" needs to be enabled.
- D. The Protocol Profile (Server) option of "Allow Compression" needs to be enabled.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 438

Which three files/data items are included in a BIG-IP UCS backup file? (Choose three.)

- A. The BIG-IP administrative addresses.
- B. The BIG-IP license.
- C. The BIG-IP log files.
- D. The BIG-IP default traps.
- E. The BIG-IP host name.

Correct Answer: ABE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 439

Could an iRule perform persistence based on a cookie?

- A. Yes AniRule could be designed to persist based on the contents of a cookie.
- B. No. iRules cannot affect persistence.
- C. Yes. An iRule could be designed to persist based on the contents of a cookie.
- D. No. Cookie persistence is only based on a cookie persistence profile.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 440

How is traffic flow through transparent virtual servers different from typical virtual servers?

- A. Traffic flow through transparent virtual servers must be forwarded through a single routing device.
- B. Traffic flow through transparent virtual servers does not have IP address translation performed.
- C. Traffic flow through transparent virtual servers is not load balanced.
- D. Traffic flow through transparent virtual servers is bridged (leave IP and IMAC addresses intact) rather than routed (leave IP address intact but change the MAC addresses).

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 441

Adivinar (?)

- A. Any text string within a cookie.

- B. Any bytes within the initial client request packet.
- C. An IP address.
- D. The value in the tcp acknowledgement field.

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 442

A monitor has been defined with an alias port of 443. All other options are left at their defaults. The administrator wishes to assign it to a pool of members where the members' ports vary.

Which is the result?

- A. For each member, if the member port is not 443, the member will be marked down.
- B. For each member, the monitor will test member node at port 443.
- C. For each member, if it is running an SSL service at the member port, the monitor may work. Otherwise, the monitor will fail and the member will be marked down.
- D. This assignment is not allowed since the port do not match.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

answer is modified

QUESTION 443

A site wishes to delegate the name www.mysite.com to a GTM System. Which entry would be appropriate in their current DNS servers?

- A. www.mysite.com. IN A 132.26.33.15
- B. 15.33.addr-in.arpa.com IN PTR .wip.mysite.com.
- C. www.mysite.com. IN CNAME wip.mysite.com.
- D. www.mysite.com. IN DEL www.GTM.mysite.com.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 444

Which statement about root DNS servers is true?

- A. Root servers have databases of all registered DNS servers.
- B. Root servers have databases of the DNS servers for top-level domains.
- C. Root servers have databases of DNS servers for each geographical area. They direct requests to appropriate LDNS servers.
- D. Root servers have databases of commonly accessed sites. They also cache entries for additional servers as requests are made.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 445

What is the advantage of specifying three load balancing methods when load balancing within pools?

- A. Specifying three methods allows the GTM System to use all three methods simultaneously.
- B. Specifying three methods allows the GTM System to choose the optimal method for each name resolution.
- C. Specifying three methods allows the GTM System alternate methods if insufficient data is available for other methods.
- D. Specifying three methods allows the GTM System to rotate between the three methods so that no one method is used too often.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 446

Specifying three methods allows the GTM System to rotate between the three methods so that no one method is used too often.

- A. The IP address of the server must be added to the wideip.conf file.
- B. The IP address of the server must be added to the syslog-ng.conf file.

- C. The IP address of the server and valid userid/password combination must be added to the hosts.allow file.
- D. The IP address of the server and valid userid/password combination must be added to the syslog-ng.conf file.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 447

What are two advantages of the Quality of Service (QoS) load balancing method? (Choose two.)

- A. It resolves requests to the site with the highest QoS value in the IP header.
- B. It combines multiple load balancing metric values in a single load balancing method.
- C. It allows the GTM administrator to place relative values on each metric used to determine the optimum site.
- D. It allows the GTM System to select the optimum virtual server based on all available path and server metrics.

Correct Answer: BC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 448

When is a Virtual Server hosted by an LTM System defined with two IP addresses?

- A. Two addresses are used to define the Virtual Server when it is managed by redundant LTM Systems.
- B. Two addresses are used to define some Virtual Servers so that the GTM System can choose the better address when resolving the name.
- C. Two addresses are used to define Virtual Servers when the LTM System hosting it is behind a firewall that is translating the Virtual Server address.
- D. Two addresses are used to define a Virtual Server when the WideIP should resolve to a different address depending on which LTM System is active.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 449

What is a characteristic of iQuery?

- A. It uses SSH.
- B. It uses SSL.
- C. It uses SCP.
- D. It uses HTTPS.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 450

Listeners that correspond to non-floating self IP addresses are stored in which configuration file?

- A. /config/bigip.conf
- B. /config/bigip_base.conf
- C. /config/gtm/wideip.conf
- D. /config/bigip_local.conf

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

answer is modified

QUESTION 451

What is the primary benefit of associating Servers with Data Centers?

- A. The primary benefit is in assigning a single IP address to identify a Data Center.
- B. The primary benefit is in combining probing metrics. Load balancing decisions can be made more intelligently.
- C. The primary benefit is administrative. It is easier to remember to add servers when they are categorized by a physical location.
- D. The primary benefit is in load balancing. Clients will not be directed to Data Centers that are separated from them by great distances.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 452

Which two are events that can be used to trigger GTM iRule data processing? (Choose two.)

- A. LB_FAILED
- B. DNS_REQUEST
- C. HTTP_REQUEST
- D. CLIENT_ACCEPTED

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 453

Which statement is correct if a TOP-based monitor is assigned to an LTM System and an HTTP-based monitor is assigned to one of that LTM System's Virtual Servers?

- A. The Virtual Server status is based on the TCP monitor only.
- B. The Virtual Server status is based on the HTTP monitor only.
- C. GTM Systems do not allow monitors on both an LTM System and one of its Virtual Servers.
- D. The Virtual Server status is based on both the TOP and HTTP monitor; if either fails, the Virtual Server is unavailable.
- E. The Virtual Server status is based on both the TOP and HTTP monitor; if either succeeds, the Virtual Server is available.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 454

With standard DNS, assuming no DNS request failures, which process describes the normal resolution process on a "first time" DNS request?

- A. Client requests address from root server, root server returns IP address to Authoritative DNS, Authoritative DNS returns requested IP address, LDNS returns requested IP address to client.
- B. Client requests address from LDNS, LDNS requests from GTM, GTM requests from Authoritative DNS, Authoritative DNS returns requested IP address, LDNS returns requested IP address to client.
- C. Client requests address from LDNS, Authoritative DNS receives request from root server, root server returns LDNS address, LDNS returns client address, Authoritative DNS returns requested IP address, LDNS returns requested IP address to client.
- D. Client requests address from LDNS, LDNS requests from root server, root server returns Authoritative DNS address, LDNS requests from Authoritative DNS, Authoritative DNS returns requested IP address, LDNS returns requested IP address to client.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 455

Which statement is true regarding fail-over?

- A. Hardware fail-over is disabled by default.
- B. Hardware fail-over can be used in conjunction with network failover.
- C. If the hardware fail-over cable is disconnected, both BIG-IP devices will always assume the active role.
- D. By default, hardware fail-over detects voltage across the fail-over cable and monitors traffic across the internal VLAN.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 456

Where is persistence mirroring configured?

- A. It is always enabled.
- B. It is part of a pool definition.
- C. It is part of a profile definition.
- D. It is part of a virtual server definition.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 457

Assume the bigd daemon fails on the active system. Which three are possible results? (Choose three.)

- A. The active system will restart the bigd daemon and continue in active mode.
- B. The active system will restart the tmm daemon and continue in active mode.
- C. The active system will reboot and the standby system will go into active mode.
- D. The active system will fail-over and the standby system will go into active mode.
- E. The active system will continue in active mode but gather member and node state information from the standby system.

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 458

What is the purpose of MAC masquerading?

- A. to prevent ARP cache errors
- B. to minimize ARP entries on routers
- C. to minimize connection loss due to ARP cache refresh delays
- D. to allow both BIG-IP devices to simultaneously use the same MAC address

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 459

Which process or system can be monitored by the BIG-IP system and used as a fail-over trigger in a redundant pair configuration?

- A. bandwidth utilization
- B. duplicate IP address
- C. CPU utilization percentage
- D. VLAN communication ability

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 460

Assuming there are open connections through an active system's NAT and a fail-over occurs, by default, what happens to those connections?

- A. All open connections will be lost.
- B. All open connections will be maintained.
- C. The "Mirror" option must be chosen on the NAT and the setting synchronized prior to the connection establishment.
- D. Long-lived connections such as Telnet and FTP will be maintained while short-lived connections such as HTTP will be lost.
- E. All open connections are lost, but new connections are initiated by the newly active BIG-IP, resulting in minimal client downtime.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 461

A virtual server is defined per the charts. The last five client connections were to members C, D, A, B, B. Given the conditions shown in the above graphic, if a client with IP address 205.12.45.52 opens a connection to the virtual server, which member will be used for the connection?

VS_Web_Pool Settings		Web_Pool Parameters	
Destination:	10.10.20.100:80	Load Balancing	Least Connections
Profiles:	TCP, HTTP	Priority Group	
iRules:	None	Activation:	Less Than 2
Default Pool:	Web_Pool	Monitor:	Custom_HTTP
Persistence:	None		

Web_Pool Member Statistics and Settings					
Member	Member Ratio	Member Priority	Outstanding Requests	Current Connections	Status
A: 172.16.20.1:80	3	5	4	56	Unavailable
B: 172.16.20.2:80	3	4	4	42	Available
C: 172.16.20.3:80	3	5	4	54	Unavailable
D: 172.16.20.4:80	1	3	1	22	Available
E: 172.16.20.5:80	1	1	1	18	Available

- A. 172.16.20.1:80
- B. 172.16.20.2:80
- C. 172.16.20.3:80
- D. 172.16.20.4:80
- E. 172.16.20.5:80

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 462

Under what condition must an appliance license be reactivated?

- A. Licenses only have to be reactivated for RMAs - no other situations.
- B. Licenses generally have to be reactivated during system software upgrades.
- C. Licenses only have to be reactivated when new features are added (IPv6, Routing Modules, etc) - no other situations.

D. Never. Licenses are permanent for the platform regardless the version of software installed.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

valuable answer

QUESTION 463

Which three methods can be used for initial access to a BIG-IP system? (Choose three.)

- A. CLI access to the serial console port
- B. SSH access to the management port
- C. SSH access to any of the switch ports
- D. HTTP access to the management port
- E. HTTP access to any of the switch ports
- F. HTTPS access to the management port
- G. HTTPS access to any of the switch ports

Correct Answer: ABF

Section: (none)

Explanation

Explanation/Reference:

QUESTION 464

What is the purpose of provisioning?

- A. Provisioning allows modules that are not licensed to be fully tested.
- B. Provisioning allows modules that are licensed be granted appropriate resource levels.
- C. Provisioning allows the administrator to activate modules in non-standard combinations.
- D. Provisioning allows the administrator to see what modules are licensed, but no user action is ever required.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 465

Which three properties can be assigned to nodes? (Choose three.)

- A. ratio values
- B. priority values
- C. health monitors
- D. connection limits
- E. load-balancing mode

Correct Answer: ACD

Section: (none)

Explanation

Explanation/Reference:

QUESTION 466

Where is the load-balancing mode specified?

- A. within the pool definition
- B. within the node definition
- C. within the virtual server definition
- D. within the pool member definition

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 467

An LTM Specialist is running the following packet capture on an LTM device:

```
ssldump -Aed -ni vlan301 'port 443'
```

Which two SSL record message details will the ssldump utility display by default? (Choose two.)

- A. HTTP Version

- B. User-Agent
- C. ClientHello
- D. ServerHello
- E. Issuer

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference:

valid answers

QUESTION 468

Given this as the first packet displayed of an ssldump:

```
2 2 1296947622.6313 (0.0001) S>CV3.1(74) Handshake
ServerHello
Version 3.1
random[32]=
19 21 d7 55 c1 14 65 63 54 23 62 b7 c4 30 a2 f0
b8 c4 20 06 86 ed 9c 1f 9e 46 0f 42 79 45 8a 29
session_id[32]=
c4 44 ea 86 e2 ba f5 40 4b 44 b4 c2 3a d8 b4 ad
4c dc 13 0d 6c 48 f2 70 19 c3 05 f4 06 e5 ab a9
cipherSuite TLS_RSA_WITH_RC4_128_SHA
compressionMethod NULL
```

In reviewing the rest of the ssldump, the application data is NOT being decrypted.

Why is ssldump failing to decrypt the application data?

- A. The application data is encrypted with SSLv3.
- B. The application data is encrypted with TLSv1.
- C. The data is contained within a resumed TLS session.
- D. The BigDB Key Log.Tcpdump.Level needs to be adjusted.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 469

An LTM Specialist is troubleshooting virtual server 10.0.0.1:443 residing on VLAN vlan301. The web application is accessed via www.example.com. The LTM Specialist wants to save a packet capture with complete decrypted payload for external analysis.

Which command should the LTM Specialist execute on the LTM device command line interface?

- A. tcpdump -vvv -s 0 'host 10.0.0.1 and port 443' -w /var/tmp/trace.cap
- B. tcpdump -vvv -s 0 -ni vlan301 'host 10.0.0.1 and port 443' -w /var/tmp/trace.cap
- C. ssldump -Aed -k
/config/filestore/files_d/Common_d/certificate_key_d/Common:www.example.com.key_1 > /var/tmp/trace.cap
- D. ssldump -Aed -ni vlan301 -k
/config/filestore/files_d/Common_d/certificate_key_d/Common:www.example.com.key_1 > /var/tmp/trace.cap

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 470

An application is configured on an LTM device:

Virtual server: 10.0.0.1:80 (VLAN vlan301)

SNAT IP: 10.0.0.1

Pool members: 10.0.1.1:8080, 10.0.1.2:8080, 10.0.1.3:8080 (VLAN vlan302)

Which packet capture should the LTM Specialist perform on the LTM device command line interface to capture only server traffic specifically for this application?

- A. tcpdump -ni 0.0:nnn -s 0 'host 10.0.0.1' -w /var/tmp/trace.cap
- B. tcpdump -ni vlan301 -s 0 'port 80 and host 10.0.0.1' -w /var/tmp/trace.cap
- C. tcpdump -ni vlan302 -s 0 'port 8080 and (host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap
- D. tcpdump -ni 0.0:nnn -s 0 '(port 80 and host 10.0.0.1) or (port 8080 and host 10.0.1.1 or host 10.0.1.2 or host 10.0.1.3)' -w /var/tmp/trace.cap

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 471

An LTM Specialist sees these entries in /var/log/ltm:

```
Oct 25 03:34:31 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443
Oct 25 03:34:32 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443
Oct 25 03:34:33 tmm warning tmm[7150]: 01260017:4: Connection attempt to insecure SSL server (see RFC5746) aborted. 172.16.20.1:443
```

Assume 172.16.20.0/24 is attached to the VLAN "internal."

What should the LTM Specialist use to troubleshoot this issue?

- A. curl -d - -k https://172.16.20.1
- B. ssldump -i internal host 172.16.20.1
- C. tcpdump -i internal host 172.16.20.1 > /shared/ssl.pcap ssldump < /shared/ssl.pcap
- D. tcpdump -s 64 -i internal -w /shared/ssl.pcap host 172.16.20.1 ssldump -r /shared/ssl.pcap

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 472

A virtual server for a set of web services is constructed on an LTM device. The LTM Specialist has created an iRule and applied this iRule to the virtual server:

```
when HTTP_REQUEST {
  switch [HTTP::uri] {
    "/WS1/ws.jsp" {
      log local0. "[HTTP::uri]-Redirected to JSP Pool"
      pool JSP
    }
    default { log local0. "[HTTP::uri]-Redirected to Non-JSP Pool" pool NonJSP
  }
}
```

```
}
```

However, the iRule is NOT behaving as expected. Below is a snapshot of the log:

```
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/WS1/WS.jsp-Redirected to Non-JSP Pool  
/ws1/WS.jsp-Redirected to Non-JSP Pool  
/WS1/ws.jsp-Redirected to JSP Pool  
/ws1/ws.jsp-Redirected to Non-JSP Pool
```

What is the problem?

- A. The condition in the iRule is case sensitive.
- B. The 'switch' command in the iRule has been used incorrectly.
- C. The pool members of both pools need to be set up as case-insensitive members.
- D. The "Process Case-Insensitivity" option for the virtual server needs to be selected.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 473

An LTM Specialist is tasked with ensuring that the syslogs for the LTM device are sent to a remote syslog server. The following is an extract from the config file detailing the node and monitor that the LTM device is using for the remote syslog server:

```
monitor  
Syslog_15002 {  
defaults from udp  
dest *:15002  
}  
  
node 91.223.45.231 {  
monitor Syslog_15002  
screen RemoteSYSLOG  
}
```

There seem to be problems communicating with the remote syslog server. However, the pool monitor shows that the remote server is up.

The network department has confirmed that there are no firewall rules or networking issues preventing the LTM device from communicating with the syslog server. The department responsible for the remote syslog server indicates that there may be problems with the syslog server. The LTM Specialist checks the BIG-IP LTM logs for errors relating to the remote syslog server. None are found. The LTM Specialist does a tcpdump:

tcpdump -nn port 15002, with the following results:

```
21:28:36.395543 IP 192.168.100.100.44772 > 91.223.45.231.15002: UDP, length 19
21:28:36.429073 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 169
21:28:36.430714 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 181
21:28:36.840524 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 169
21:28:36.846547 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 181
21:28:39.886343 IP 192.168.100.100.39499 > 91.223.45.231.15002: UDP, length 144
```

Note. 192.168.100.100 is the self IP of the LTM device.

Why are there no errors for the remote syslog server in the log files?

- A. The -log option for tcpdump needs to be used.
- B. The monitor type used is inappropriate.
- C. The "verbose" logging option needs to be enabled for the pool.
- D. When the remote syslog sever fails, it returns to service before the timeout for the monitor has expired.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 474

Given a tcpdump on an LTM device from both sides of a connection on the External and Internal VLANs, how should an LTM Specialist determine if SNAT is enabled for a particular pool?

- A. by checking to see if the Source IP is carried through from the External Vlan to the Internal Vlan
- B. by checking to see if the Destination port is carried through from the External Vlan to the Internal Vlan
- C. by checking to see if the Source port is carried through from the External Vlan to the Internal Vlan
- D. by checking to see if the Destination IP is carried through from the External Vlan to the Internal Vlan

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 475

An LTM Specialist has a OneConnect profile and HTTP profile configured on a virtual server to load balance an HTTP application.

The following HTTP headers are seen in a network trace when a client connects to the virtual server:

Clientside:

GET / HTTP/1.1

Host: 192.168.136.100

User-Agent: Mozilla/5.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate

Connection: keep-alive

Serverside:

HTTP/1.1 200 OK

Date: 5 Jun 1989 17:06:55 GMT

Server: Apache/2.2.14 (Ubuntu)

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Length: 3729

X-Connection: close

Content-Type: text/html

The LTM Specialist notices the OneConnect feature is working incorrectly.

Why is OneConnect functioning incorrectly?

- A. Client must support HTTP/1.0.
- B. Client must support HTTP keep-alive.
- C. Server must support HTTP/0.9.
- D. Server must support HTTP keep-alive.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 476

While investigating the cause of a device failover, an LTM Specialist discovers the following events in /var/log/ltm:

01010029:5: Clock advanced by 518 ticks
01010029:5: Clock advanced by 505 ticks
01010029:5: Clock advanced by 590 ticks
01010029:5: Clock advanced by 568 ticks
01010029:5: Clock advanced by 1681 ticks
01010029:5: Clock advanced by 6584 ticks
01140029:5: HA daemon_heartbeat tmm fails action is failover and restart. 010c0026:5: Failover condition, active attempting to go standby.

Which issue caused the failover?

- A. NTP being out of sync
- B. TMM being descheduled
- C. VLAN Fail-safe heartbeats
- D. HA missing heartbeat packets

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 477

A failover event is recorded in the log messages:

Jan 01 00:00:50 BIG-IP notice sod[5855]: 01140029:5: HA proc_running tmm fails action is go offline and down links.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c0050:5: Sod requests links down. Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c0054:5: Offline for traffic group /Common/traffic-group-1.
Jan 01 00:00:50 BIG-IP notice sod[5855]: 010c003e:5: Offline Jan 01 00:00:50 BIG-IP notice logger: /usr/bin/tmipsecd --tmmcount 4 ==> /usr/bin/bigstart stop racoon
Jan 01 00:00:50 BIG-IP info lacpd[5502]: 01160016:6: Failover event detected. (Switchboard failsafe disabled while offline)
Jan 01 00:00:51 BIG-IP err bcm56xxd[5296]: 012c0010:3: Failover event detected. Marking external interfaces down.bsx.c(3633)
Jan 01 00:00:51 BIG-IP info bcm56xxd[5296]: 012c0015:6: Link: 1.1 is DOWN Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 0107143c:5: Connection to CMI peer 10.0.0.3 has been removed
Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 0107143a:5: CMI reconnect timer: enabled Jan 01 00:00:56 BIG-IP notice mcpd[5318]: 01071431:5: Attempting to connect to CMI peer 10.0.0.3 port 6699

What is the cause of the failover?

- A. TMM failed, and VLAN fail-safe initiated the failover.
- B. TMM failed, and system fail-safe initiated the failover.

- C. Loss of connection to CMI peer 10.0.0.3 initiated the failover.
- D. A switchboard failure caused system fail-safe to initiate the failover.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 478

An LTM Specialist has just manually failed the active LTM device over to the standby LTM device. The LTM Specialist notices the newly active LTM device is NOT currently receiving traffic. The LTM Specialist verifies the newly active device is responding to ARP but still no traffic is hitting the virtual servers. The LTM Specialist also notices that the virtual servers eventually start responding.

What should be added to the configuration to resolve the problem?

- A. vlan failsafe
- B. floating self IP
- C. network failover
- D. MAC masquerading
- E. connection mirroring

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 479

An LTM Specialist is troubleshooting an issue where one LTM device in a three LTM device group is failing to synchronize after a synchronize to group command is issued. The LTM Specialist verifies there are no packet filters, port lock down, or network issues preventing the connection.

What are two reasons the synchronization group is having issues? (Choose two.)

- A. Certificates expired on all of the peer LTM devices.
- B. Certificates stored for the device trusts on all of the peer LTM devices are corrupted.
- C. Admin passwords changed on one of the peer LTM devices that are able to synchronize.
- D. Admin password changed on the LTM device NOT receiving the synchronized configurations.

E. Certificates stored for the device trusts on the LTM device NOT receiving the configuration are corrupted.

Correct Answer: DE

Section: (none)

Explanation

Explanation/Reference:

QUESTION 480

An LTM Specialist configures two LTM devices in a high-availability pair with trusts established and device groups configured properly using network failover. After several months, the LTM Specialist notices that changes made to one LTM device do NOT cause the synchronization status to update to "changes pending," and this device does NOT synchronize with the device group.

Which two steps should the LTM Specialist take to identify the issue? (Choose two.)

- A. Verify that NTP is synchronized.
- B. Verify the network connectivity between the devices.
- C. Verify that the devices are not using self-signed certificates.
- D. Verify that ConfigSync is using the management IP address.
- E. Verify that port lockdown on the ConfigSync interface is set to allow port 1026.

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

QUESTION 481

An HA pair of LTM devices configured in Active-Standby mode stops responding to traffic and causes an outage. The Active device becomes Standby, but the partner device stays in Standby mode instead of taking over as Active. A reboot and restart of the services brings the LTM device to Active mode for a short time, but then it goes into Standby mode again.

Which two configuration components caused this condition? (Choose two.)

- A. VLAN Fail-safe
- B. System Fail-safe
- C. Gateway Fail-safe
- D. Switch Board Failure

E. Link down on Failover

Correct Answer: AC

Section: (none)

Explanation

Explanation/Reference:

QUESTION 482

A device group is made up of four members: LTM-A, LTM-B, LTM-C, and LTM-D. An LTM Specialist makes a configuration change on LTM-B. Later, a different LTM Specialist notices a "changes pending" message on all devices. When logged into LTM-D, the LTM Specialist attempts to config-sync to the device group. The sync operation fails.

Why is the LTM Specialist on LTM-D unable to synchronize the configuration to the group?

- A. The changes made on LTM-B are invalid.
- B. LTM-D has the lowest commit-id of the group.
- C. NTP is NOT configured on the devices in the group.
- D. LTM-B is the device eligible to initiate a config-sync.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

QUESTION 483

A failover event is recorded in the following log messages:

Jan 01 00:56:56 BIG-IP notice mcpd[5318]: 01070727:5: Pool /Common/my-pool member /Common/10.0.0.10:80 monitor status down.

Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0045:5: Leaving active, group score 10 peer group score 20.

Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0052:5: Standby for traffic group /Common/traffic-group-1.

Jan 01 00:56:56 BIG-IP notice sod[5855]: 010c0018:5: Standby Jan 01 00:57:06 BIG-IP notice logger: /usr/bin/tmipsecd --tmcount 4 ==> /usr/bin/bigstart stop racoon

What is the cause of the failover?

- A. The HA group score changed.
- B. No traffic is seen on traffic-group-1.
- C. The peer device left the traffic group.

D. The racoon service stopped responding.

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

QUESTION 484

An LTM device pair is configured for failover and connection mirroring. The LTM devices are configured with virtual servers for HTTP, HTTPS with SSL offload, and SSH. An event occurs that causes a failover. HTTP and SSH sessions active at the time of failover remain active, but HTTPS sessions are dropped.

What is the root cause of this problem?

- A. The SSL certificates on the LTM devices do NOT match.
- B. Connection mirroring is incompatible with clientssl profiles.
- C. SNAT automap was NOT enabled for the HTTPS virtual servers.
- D. Connection mirroring was NOT enabled for the HTTPS virtual servers.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 485

-- Exhibit

```

ltm profile httpclass acct_class {
    app-service none
    defaults-from httpclass
    paths { glob:/accounting }
    pool srv1_http_pool
    redirect none
}
ltm profile httpclass marketing_class {
    app-service none
    defaults-from httpclass
    paths { glob:/marketing }
    pool srv1_http_pool
    redirect none
}
ltm profile httpclass default_class {
    app-service none
    defaults-from httpclass
    pool srv2_http_pool
    redirect none
}
ltm virtual http_vs {
    destination 192.168.1.155:http
    http-class {
        acct_class
        marketing_class
        default_class
    }
    ip-protocol tcp
    mask 255.255.255.255
    pool srv2_http_pool
    profiles {
        http { }
        tcp { }
    }
    snat automap
    vlans-disabled
}

```

-- Exhibit --

Refer to the exhibit.

An LTM Specialist is reviewing the virtual server configuration on an LTM device.

Which two actions should the LTM Specialist perform to minimize the virtual server configuration? (Choose two.)

- A. Remove 'snat automap' from the virtual server.
- B. Remove the 'http' profile from the virtual server.
- C. Remove the 'default_class' from the virtual server.
- D. Combine 'acct_class' and 'marketing_class' into one class and update associations on the virtual server.
- E. Combine 'marketing_class' and 'default_class' into one class and update associations on the virtual server.

Correct Answer: CD

Section: (none)

Explanation

Explanation/Reference: