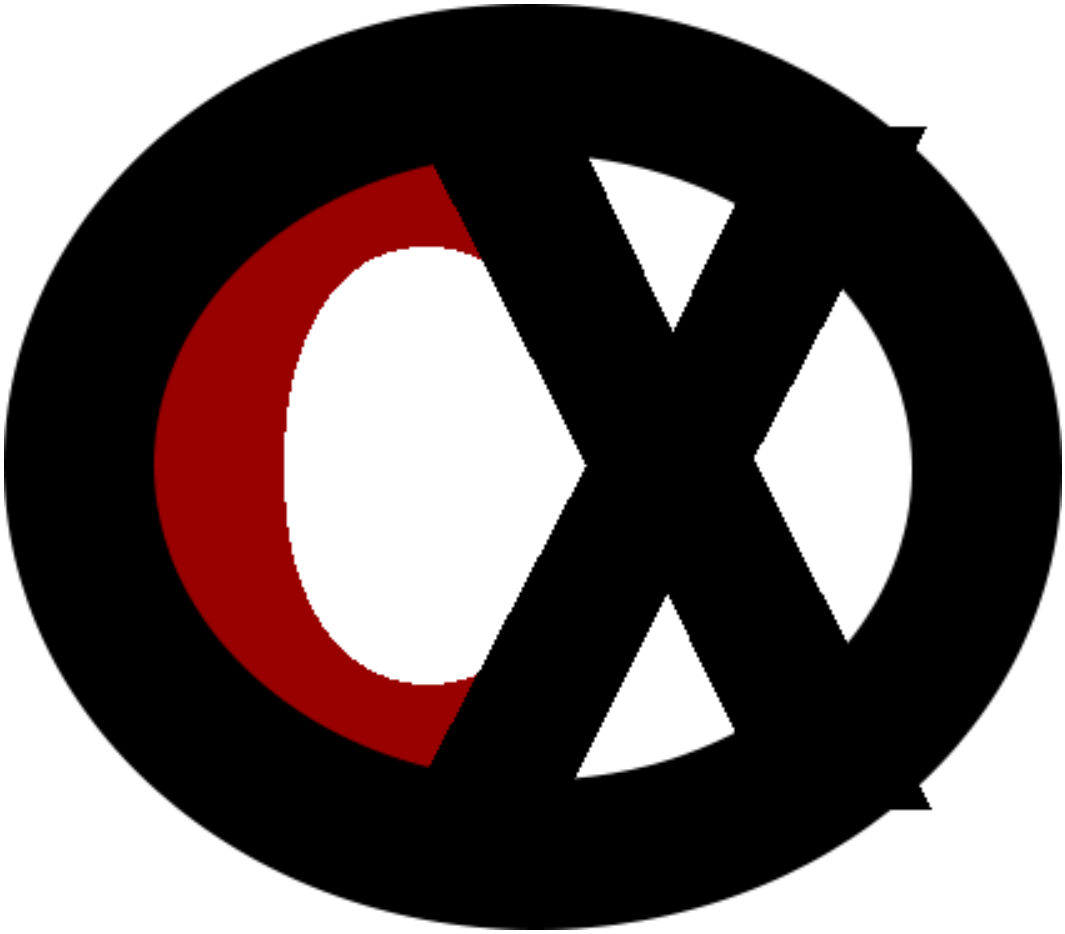
1Y0-240 Citrix ADC 12 Essentials and Traffic Management Practice Exam Demo



Citrixxperience.com

This Practice Exam was created by Jeffrey C Rohrer, owner of Citrixxperience.com.

1Y0-240 Citrix ADC 12 Essentials and Traffic Management Practice Exam Demo

Section 2: Basic Networking

2.01

Objective: Determine which networking topology to use with Citrix ADC based on given requirements.

1. In a high availability (HA) configuration, a Citrix Administrator wants to configure throughput (throughput parameter) based HA failover and link redundancy (lrMinThroughput parameter) on an LACP channel.

   Which configuration should the administrator perform to accomplish the goal?

   a. Set the throughput parameter to a value more than that of the lrMinThroughput parameter.
   b. Set the throughput parameter to a value less than that of the lrMinThroughput parameter.
   c. Set the throughput parameter to a value more than or equal to that of the lrMinThroughput parameter.
   d. Set the throughput parameter to a value less than or equal to that of the lrMinThroughput parameter.

   Answer: d.

   Explanation: In an HA configuration, if an administrator wants to configure throughput (throughput parameter) based HA failover and link redundancy (lrMinThroughput parameter) on an LACP channel, the admin must set the throughput parameter to a value less than or equal to that of the lrMinThroughput parameter. The maximum supported throughput of an LACP channel is calculated as the maximum supported throughput of the active subchannel. If the throughput parameter value is equal to or less than the lrminthroughput parameter value, HA failover occurs when both

of the following conditions exist at the same time: None of the subchannels' maximum supported throughput meets the lrMinThroughput parameter value and the maximum supported throughput of the LACP channel does not meet the throughput parameter value.

Source: Configuring Link Aggregation
https://docs.citrix.com/en-us/netscaler/12/networking/interfaces/configuring-link-aggregation.html#link-redundancy-using-lacp-channels

Section 3: Citrix ADC Platforms

3.02

Objective: Identify the pieces of the multi-tenant structure for Citrix ADC SDX.

2. **Scenario:** A Citrix Administrator has configured several instances on an SDX ADC appliance. The administrator has enabled L2 mode to allow the instances to receive and forward packets for MAC addresses other than their own MAC addresses. The administrator plans to enable two interfaces on one of the instances.

   Which action should the administrator take to allow the plan to work correctly?

   a. Enable L3 mode.
   b. Disable L2 mode.
   c. Configure MAC-based forwarding.
   d. Tag one of the instances on the interface.

   Answer: d.

   Explanation: In Layer 2 (L2) mode, a Citrix ADC instance acts as a learning bridge and forwards all packets for which it is not the destination. With L2

mode enabled, the instance can receive and forward packets for MAC addresses other than its own MAC address. However, if an administrator wants to enable L2 mode on a Citrix ADC instance running on an SDX ADC appliance, the administrator must first allow L2 mode on that instance. On a given 1/x interface, untagged packets must be allowed on only one instance. For all other instances enabled on the same interface, the administrator must select Tagged.

Source: Allowing L2 Mode on a Citrix NetScaler instance
https://docs.citrix.com/en-us/sdx/12/configuring-managing-netscaler-instance/configuring-l2-mode-on-netscaler-instance.html

Section 5: Load Balancing

5.01

Objective: Identify the Citrix ADC load-balancing role of entities.

3. **Scenario:** A Citrix Administrator has configured Least Response Time load balancing on an HTTP virtual server. Soon, the administrator notices that the virtual server appears to be using the Round Robin method of load balancing.

   Which configuration can the administrator perform to fix this issue?

   a. Add another HTTP virtual server.
   b. Reconfigure as an HTTPS virtual server.
   c. Assign weights to the back end services.
   d. Bind monitors to the back end services.

   Answer: c.

   Explanation: When the load balancing virtual server is configured to use the least response time method, it selects the service with the fewest active

connections and the lowest average response time. An administrator can configure this method for HTTP and Secure Sockets Layer (SSL) load balancing virtual servers only. The response time (also called Time to First Byte, or TTFB) is the time interval between sending a request packet to a service and receiving the first response packet from the service. The NetScaler appliance uses response code 200 to calculate TTFB. If weights ARE NOT assigned to the services, services will get overloaded and switch to Round Robin mode.

Source: Least response time method
https://docs.citrix.com/en-us/netscaler/12/load-balancing/load-balancing-customizing-algorithms/leastresponsetime-method.html

Section 6: SSL Offload
6.03

Objective: Determine which SSL deployment to use for a given environment.

4. **Scenario:** A Citrix Administrator must install the SSL certificates necessary to encrypt the connections among components in a double-hop DMZ deployment. StoreFront in the second DMZ connects to the XML Service hosted on a server in the internal network. The XML Service is a standard Windows service on the server.

   Which two configurations must the administrator make in this scenario? (Choose two.)

   a. A server certificate must be installed on the Internet Information Services server in the internal network.
   b. A server certificate must be installed within the SSL Relay on the server hosting the XML Service in the internal network.
   c. StoreFront must have a root certificate installed that is signed by the same CA as the server certificate installed on the SSL Relay.

d. StoreFront must have a root certificate installed that is signed by the same CA as the server certificate installed on the Internet Information server.

Answer: b.c.

Explanation: When StoreFront in the second DMZ connects to the XML Service hosted on a server in the internal network, if the XML Service runs on a Microsoft Internet Information Services (IIS) server on the XenApp server, an SSL server certificate must be installed on the IIS server. If the XML Service is a standard Windows service (does not reside in IIS), an SSL server certificate must be installed within the SSL Relay on the server. StoreFront must have a root certificate installed that is signed by the same CA as the server certificate installed on either the Microsoft IIS server or the SSL Relay.

Source: Managing SSL Certificates in a Double-Hop DMZ Deployment https://docs.citrix.com/en-us/citrix-gateway/12-1/double-hop-dmz/ng-double-dmz-install-con/ng-double-dmz-install-ssl-certificates-tsk.html

Section 8: Troubleshooting

8.01

Objective: Determine how to resolve Citrix ADC log issues.

5. **Scenario:** A Citrix Administrator is planning to consolidate all Citrix ADC logging into one log file. The administrator must ensure there is a filter definition for each log transaction that occurs.

   Which step should the administrator take to meet the requirement?

   a. Define the default filter.
   b. Apply the filter to all IP addresses.

c. Ensure all ADC appliances are on the same subnet.
d. Specify each NSIP address in the consolidated log file.

Answer: a.

Explanation: For consolidated logging, if a log transaction occurs for which there is no filter definition, the default filter is used (if it is enabled.) The only way to configure consolidated logging of all the ADC appliances is by defining the default filter.

Source: Customize logging on the NSLOG server
https://docs.citrix.com/en-us/netscaler/12/system/audit-logging/customize-logging-on-nslog-server.html

Section 9: Classic and Default Policies

9.01

Objective: Determine how to use the Citrix ADC classic policy engine to create policies.

6. A classic Citrix ADC policy can be used _____ and _____. (Choose the two correct options to complete the sentence.)

a. determine whether HTTP responses are cacheable
b. configure the behavior of the Responder function
c. determine how to perform DNS resolution for requests
d. configure LDAP and certificate-based authentication schemes
e. configure the behavior of the Filter, SureConnect, and Priority Queuing functions

Answer: d.e.

Explanation: The Citrix ADC supports a variety of features that rely on policies for operation. Some operations can only be performed with classic

policies. A couple of operations only used with classic policies are to configure LDAP and certificate-based authentication schemes and to configure the behavior of the Filter, SureConnect, and Priority Queuing functions.

Source: Classic and advanced policies
https://docs.citrix.com/en-us/citrix-adc/13/appexpert/policies-and-expressions/introduction-to-policies-and-exp/classic-and-advanced-policy.html#how-different-citrix-adc-features-use-policies

Section 11: Content Switching

11.01

Objective: Determine how to utilize Content Switching components.

7. **Scenario:** A Citrix Administrator is required to configure Citrix ADC to present content that is relevant to users in the Paris, France area. The administrator also must present content in French to the Paris users.

   Which ADC feature should the administrator use to meet the requirements?

   a. Load Balancing
   b. Unified Gateway
   c. Cache Redirection
   d. Content Switching

   Answer: d.

   Explanation: An administrator may want to present different content to different users. For example, the administrator may want to allow users from the IP range of a customer or partner to have access to a special Web portal, or present content relevant to a specific geographical area to users

from that area, or present content in different languages to the speakers of those languages, or present content tailored to specific devices, such as smartphones, to those who use the devices. The ADC content switching feature enables the appliance to distribute client requests across multiple servers on the basis of specific content that an administrator wishes to present to those users.

Source: Content Switching
https://docs.citrix.com/en-us/netscaler/12/content-switching.html

Section 13: Global Server Load Balancing

13.02

Objective: Determine how to Implement GSLB in a Citrix ADC environment.

8. Which command can a Citrix Administrator execute to prevent clients from attempting to connect to GSLB sites that are down?

    a. set gslb vserver<name> MIR ENABLED
    b. set gslb vserver<name> EDR ENABLED
    c. set gslb vserver<name> MIR DISABLED
    d. set gslb vserver<name> EDR DISABLED

    Answer: b.

    Explanation: When a GSLB virtual server is disabled or in a DOWN state, the response to a DNS query for the GSLB domain bound to that virtual server contains the IP addresses of all the services bound to the virtual server. However, you can configure the GSLB virtual server to in this case send an empty down response (EDR). When this option is set, a DNS response from a GSLB virtual server that is in a DOWN state does not contain IP address records, but the response code is successful. This prevents clients from attempting to connect to GSLB sites that are down.

Source: Protect the GSLB setup against failure
https://docs.citrix.com/en-us/netscaler/12/global-server-load-balancing/how-to/protect-setup-against-failure.html#configuring-a-gslb-virtual-server-to-respond-with-an-empty-address-record-when-down