

100% Money Back
Guarantee

Vendor:Citrix

Exam Code:1Y0-241

Exam Name:Deploy and Manage Citrix ADC with
Traffic Management

Version:Demo

QUESTION 1

Scenario: A Citrix Administrator suspects an attack on a load-balancing vServer (IP address 192.168.100.25).

The administrator needs to restrict access to this vServer for 10 minutes.

Which Access Control List (ACL) will accomplish this?

- A. add simpleacl rule1 DENY -srcIP 192.168.100.25 -TTL 600000
- B. add simpleacl rule1 DENY -srcIP 192.168.100.25 -TTL 600
- C. add ns acl rule1 DENY -destIP 192.168.100.25 -TTL 600000
- D. add ns acl rule1 DENY -destIP 192.168.100.25 -TTL 600

Correct Answer: D

<https://docs.citrix.com/en-us/citrix-adc/current-release/networking/access-control-lists-acls/extended-acls-and-extended-acl6s.html>

By binding a multiple SAN certificate, we only need to adapt the DNS entries of the websites to point to the same IP (1 IP with 3 DNS) and we will be able to forward the requests to any backend server since all of them are serving the same content.

QUESTION 2

```
set gslb vServer-GSLB-1-MIR ENABLED
```

What will the Citrix ADC appliance send when the above command is executed?

- A. The Remote GSLB service as the first record in the response and adds the remaining active services as additional records
- B. The Local GSLB service as the first record in the response and adds the remaining active services as additional records
- C. Only the best GSLB service in the response
- D. The best global server load balancing (GSLB) service as the first record in the response, and the remaining active services as additional records

Correct Answer: D

<https://docs.citrix.com/en-us/citrix-adc/current-release/global-server-load-balancing/how-to/protect-setup-against-failure.html>

"if you enable multiple IP responses (MIR), the Citrix ADC appliance sends the best GSLB service as the first record in the response and adds the remaining active services as extra records. "

QUESTION 3

A Citrix Administrator needs to confirm that all client certificates presented to the authentication vServer are valid until the year 2023. Which expression can the administrator use to meet this requirement?

- A. CLIENT.SSL.CLIENT_CERT.VALID_NOT_AFTER.EQ(GMT2023)
- B. CLIENT.SSL.CLIENT_CERT.VALID_NOT_BEFORE.EQ(GMT2023)
- C. CLIENT.SSL.ORIGIN_SERVER_CERT.VALID_NOT_AFTER.EQ(GMT2023)
- D. CLIENT.SSL.CLIENT_CERT.DAYS_TO_EXPIRE.EQ(2023)

Correct Answer: A

<https://docs.citrix.com/en-us/citrix-adc/current-release/appexpert/policies-and-expressions/adv-policy-exp-working-with-dates-times-and-numbers/exp-for-ssl-certificate-date.html> <https://docs.citrix.com/en-us/citrix-adc/current-release/ssl/ssl-actions-and-policies/config-built-in-sslactions.html>

QUESTION 4

Scenario: A Citrix Administrator needs to configure persistence on a global server load balancing (GSLB) vServer to which a service is bound. Service must continue to handle requests from the client even after it is disabled manually ? accepting new requests or connections only to honor persistence. After a configured period of time, no new requests or connections are directed to the service and all existing connections are closed.

To achieve these requirements, which parameter can the administrator configure while disabling the service?

- A. Persistence threshold
- B. Persistence time-Out
- C. Wait time
- D. Request threshold

Correct Answer: C

<https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-advanced-settings/graceful-shutdown.html>

QUESTION 5

Scenario: A Citrix Administrator configured the rewrite policies below: bind lb vServer VIP1_http -policyName POL_14 -priority 120 -gotoPriorityExpression END - type REQUEST bind lb vServer VIP1_http -policyName POL_12 -priority 90 -gotoPriorityExpression NEXT - type REQUEST bind lb vServer VIP1_http -policyName POL_15 -priority 100 -gotoPriorityExpression END - type REQUEST bind lb vServer VIP1_http -policyName POL_13 -priority 101 -gotoPriorityExpression NEXT -type REQUEST Which policy will be evaluated last considering POL_12 is hit first?

- A. POL_12
- B. POL_13
- C. POL_14

D. POL_15

Correct Answer: D

QUESTION 6

Which Citrix ADC Access Control List (ACL) command can a Citrix Administrator use to bridge traffic originating from the IP address 192.168.10.200?

- A. add ns simpleacl6
- B. add ns simpleacl
- C. add ns acl
- D. add ns acl6

Correct Answer: C

<https://developer-docs.citrix.com/projects/citrix-adc-command-reference/en/latest/ns/ns-acl/>

QUESTION 7

Scenario: A Citrix Administrator is managing a Citrix Gateway with a standard Platform license and remote employees in the environment. The administrator wants to increase access by 3,000 users through the Citrix Gateway using VPN access.

Which license should the administrator recommend purchasing?

- A. Citrix ADC Burst Pack
- B. Citrix Gateway Express
- C. Citrix Gateway Universal
- D. Citrix ADC Upgrade

Correct Answer: C

Reference: <https://docs.citrix.com/en-us/citrix-gateway/current-release/citrix-gateway-licensing.html>

QUESTION 8

Scenario: A Citrix Administrator manages an environment that has a Citrix ADC high availability (HA) pair running on two MPX appliances. The administrator notices that the state of the secondary Citrix ADC is `Unknown`. What is causing the secondary state to be `Unknown`?

- A. The synchronization on the secondary appliance is disabled.
- B. TCP port 22 is disabled between the primary and secondary ADCs.

- C. The administrator made both Citrix ADCs primary.
- D. The remote procedure call (RPC) nodes are incorrectly configured.

Correct Answer: D

<https://docs.citrix.com/en-us/citrix-adc/current-release/system/high-availability-introduction/troubleshooting-high-availability.html>

QUESTION 9

Scenario: After deploying a Citrix ADC in production, a Citrix Administrator notices that client requests are NOT being evenly distributed among backend resources. The administrator wants to change from the default loadbalancing method to one that will help distribute the load more evenly.

Which load-balancing method would ensure that the server with the least amount of network utilization is receiving new connections?

- A. Least connection
- B. Least bandwidth
- C. Least response time
- D. Least packets

Correct Answer: B

<https://docs.citrix.com/en-us/citrix-adc/current-release/load-balancing/load-balancing-customizing-algorithms/leastbandwidth-method.html>

QUESTION 10

Scenario: While performing a disaster recovery test, a Citrix Administrator decides to failover the Citrix ADC high availability (HA) pair appliances. The administrator notices that the failover is NOT working as expected, and the secondary Citrix ADC is NOT taking over as primary. The administrator suspects that networking issues may be causing the failure.

What could be the cause of this issue?

- A. HA monitoring is enabled on an interface of the secondary node that shows as ENABLED, DOWN.
- B. The Independent Network Configuration (INC) mode is enabled on the primary node.
- C. HA monitoring is enabled on a disabled interface of the primary node.
- D. HA heartbeats are only seen on some enabled interfaces of the secondary node.

Correct Answer: C

QUESTION 11

A Citrix Administrator needs to use a client's IP address as the source IP address for Citrix ADC-to-server connections. Which Citrix ADC mode can the administrator use to meet this requirement?

- A. USNIP
- B. Layer 2
- C. Layer 3
- D. USIP

Correct Answer: D

When you enable the USIP address mode of a NetScaler appliance, the appliance forwards each packet to the appropriate back end server with the client IP address. <https://support.citrix.com/article/CTX121974>

QUESTION 12

Scenario: A Citrix Administrator is configuring a Citrix ADC high availability (HA) pair. The administrator needs to ensure that one Citrix ADC is UP and primary at all times to guarantee that business websites are always available. In the event that both nodes become unavailable or fail a health check, what does the administrator need to do to ensure that the Citrix ADCs still handle web traffic?

- A. Configure HA fail-safe mode on the primary Citrix ADC only.
- B. Disable HA fail-safe mode on each Citrix ADC independently.
- C. Configure HA fail-safe mode on each Citrix ADC independently.
- D. Disable HA fail-safe mode on the primary Citrix ADC only.

Correct Answer: C