# Question 1

Scenario: A Citrix Administrator needs to integrate LDAP for Citrix ADC system administration using current active directory (AD) groups. The administrator created the group on the Citrix ADC, exactly matching the group name in LDAP.

What can the administrator bind to specify the permission level and complete the LDAP configuration?

## Options:

**A-** A command policy to the group

**B-** A nested group to the new group

**C-** Users to the group on the Citrix ADC

**D-** An authentication, authorization, and auditing (AAA) action to the group

## Answer:

A

# Question 2

When a Citrix ADC high availability (HA) pair failover occurs, by what method does the Citrix ADC communicate to the network switches and routers that IP-to-MAC address bindings have changed?

## Options:

**A-** Reverse ARP (RARP) to update the network devices

**B-** MAC-based forwarding (MBF) to update the routers

**C-** Proxy ARP to update the network devices

**D-** Gratuitous ARPs (GARPs) to update the network devices

## Answer:

D

# Question 3

**Question Type:** **MultipleChoice**

Scenario: The primary content switching vServer has gone down. To troubleshoot, a Citrix Administrator has issued the following command:

> show csvserver CSV

CSV (10.1.100.100:443) -- HTTPS Type: CONTENT

State: UP

Last state change was at Mon Jun 29 15:20:43 2020

Time since last state change: 1 day, 06:47:58 610

Client Idle Timeout: 180 sec

Down state flush: ENABLED

Disable Primary vServer On Down: DISABLED

Appflow logging: ENABLED

Port Rewrite: DISABLED

State Update: DISABLED

Default: Content Precedence: URL

vServer IP and Port insertion: OFF

Persistence: NONE redirect: http://www.site1.com/mysite1/maintenance

Backup: vServer--LB--2

Listen Policy: NONE

IcmpResponse: PASSIVE

RHIstate: PASSIVE

Traffic Domain: 0

Based on this output, where will the subsequent request be redirected?

## Options:

**A-** http://www.site1.com/mysite1/maintenance

**B-** vServer--LB-2

**C-** Backup content switching vServer

**D-** 10.1.100.100:443

## Answer:

A

# Question 4

Scenario: A Citrix Administrator manages an environment that has three SSL websites, all serving the same content.

www.company.com

www.company.net

www.company.org

The administrator would like to consolidate the websites into a single, load-balanced SSL vServer.

What can the administrator bind to use a single SSL vServer?

## Options:

**A-** A wildcard certificate to a single SSL vServer

**B-** A wildcard certificate to a content-switching vServer

**C-** The certificate of each website to a single SSL vServer

**D-** A multiple SAN certificate to a single SSL vServer

## Answer:

C

# Question 5

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?

## Options:

**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

## Answer:

D

# Question 6

To protect an environment against Hash DoS attacks, which two configurations can a Citrix Administrator use to block all post requests that are larger than 10,000 bytes? (Choose two.)

## Options:

**A-** > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\")&&
http.REQ.CONTENT_LENGTH.GT(10000)"
> add rewrite policy drop_rewrite expr_hashdos_prevention DROP
> bind rewrite global drop_rewrite 100 END --type REQ_OVERRIDE

**B-** > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\")&&
http.REQ.CONTENT_LENGTH.GT(10000)"
> add responder policy pol_resp_hashdos_prevention expr_hashdos_prevention DROP NOOP
> bind responder global pol_resp_hashdos_prevention 70 END --type REQ_OVERRIDE

**C-** > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\") ||
http.REQ.CONTENT_LENGTH.GT(10000)"
> add responder policy pol_resp_hashdos_prevention expr_hashdos_prevention DROP NOOP
> bind responder global pol_resp_hashdos_prevention 70 END --type REQ_OVERRIDE

**D-** > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\") ||
http.REQ.CONTENT_LENGTH.GT(10000)"

> add rewrite policy drop_rewrite expr_hashdos_prevention DROP

> bind rewrite global drop_rewrite 70 END --type REQ_OVERRIDE

**E-** > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\") ||
http.REQ.CONTENT_LENGTH.GT(10000)"

> add responder policy pol_resp_hashdos_prevention expr_hashdos_prevention DROP NOOP

> bind responder global pol_resp_hashdos_prevention 100 END --type REQ_OVERRIDE

**F-** > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\") ||
http.REQ.CONTENT_LENGTH.GT(10000)"

> add rewrite policy drop_rewrite expr_hashdos_prevention DROP

> bind rewrite global drop_rewrite 100 END --type REQ_OVERRIDE

## Answer:

B, E

# Question 7

**Question Type:** **MultipleChoice**

Scenario: A Citrix Administrator configured SNMP to send traps to an external SNMP system. When reviewing the messages, the administrator notices several entity UP and entity DOWN messages.

To what are these messages related?

## Options:

**A-** Load-balancing vServers

**B-** Network interface

**C-** High availability nodes

**D-** SSL profile

## Answer:

A

# Question 8

**Question Type: MultipleChoice**

Scenario: A Citrix Administrator would like to grant access to a Junior Citrix Administrator on the Citrix ADC.

The administrator would like to grant full access to everything except the following:

Shell User configuration

Partition configuration

Which preexisting command policy would meet the needs of this scenario?

## Options:
**A-** Sysadmin

**B-** Operator

**C-** Network

**D-** Superuser

## Answer:
A