1Y0-241 Q&As

Deploy and Manage Citrix ADC with Traffic Management

Pass Citrix 1Y0-241 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/1y0-241.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Citrix Official Exam Center

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?

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

Correct Answer: A

Reference: https://support.citrix.com/article/CTX123782

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?

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

Correct Answer: D

Reference: https://www.citrix.com/blogs/2015/01/05/netscaler-best-practice-with-vmac-in-a-high-availabilityconfiguration/

QUESTION 3

Scenario: A Citrix Administrator configured a load-balancing vServer. The URL for this vServer is vpn.citrix.com. The backend server has the host name configured as server1.citrix.com.

The administrator needs to implement the policy to change the host name from vpn.citrix.com to server1.citrix.com, and vice versa.

Which does the administrator need to configure to meet this requirement?

A. set transform action "host change" -priority 10 -reqUrlFrom "https://vpn.citrix.com/*" -reqUrlInto "https://server1.citrix.com/*" -resUrlFrom "https://server1.citrix.com/*" -resUrlInto "https://vpn.citrix.com/*"

B. set transform action "host change" -priority 10 -reqUrlFrom "https://server1.citrix.com/*" -reqUrlInto "https://vpn.citrix.com/*" -resUrlFrom "https://server1.citrix.com/*" -resUrlInto "https://vpn.citrix.com/*"

C. set transform action "host change" -priority 10 -reqUrlFrom "https://server1.citrix.com/*" -reqUrlInto "https://vpn.citrix.com/*" -resUrlFrom "https://vpn.citrix.com/*" -resUrlInto "https://server1.citrix.com/*"

D. set transform action "host change" -priority 10 -reqUrlFrom "https://vpn.citrix.com/*" -reqUrlInto "https://server1.citrix.com/*" -resUrlFrom "https://vpn.citrix.com/*" -resUrlInto "https://server1.citrix.com/*"

Correct Answer: A

QUESTION 4

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.)

A. > add policy expression expr_hashdos_prevention "http.REQ.METHOD.EQ(\"POST\")andandhttp.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\")andandhttp.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

Correct Answer: AB

QUESTION 5

Which Citrix ADC feature can a Citrix Administrator employ to reuse existing TCP connections?

A. TCP buffering

B. Connection multiplexing

C. Keep-alive

D. Content switching

Correct Answer: B