Practice Exam Questions

citrix

1Y0-440

Architecting a Citrix Networking Solution

EXAMKILLER

Help Pass Your Exam At First Try

Citrix

Exam 1Y0-440

Architecting a Citrix Networking Solution

Version: 10.0

[Total Questions: 152]

Question No : 1

Scenario: More than 10,000 users will access a customer's environment. The current networking infrastructure is capable of supporting the entire workforce of users. However, the number of support staff is limited, and management needs to ensure that they are capable of supporting the full user base.

Which business driver is prioritized, based on the customer's requirements?

A. Simplify Management
B. Increase Scalability
C. Increase Flexibility
D. Reduce Costs
E. Enable Mobile Work Styles
F. Increase Security

Answer: A

Question No : 2

Which three steps should a Citrix Architect complete to configure session settings for different user accounts or groups? (Choose three.)

A. Bind a profile to the authentication virtual server that handles the traffic to which the architect wants to apply the policy.
B. Create policies to select the connections to which to apply particular profiles and bind the policies to users or groups.
C. Create a profile for each user account or group for which the architect wants to configure custom session settings.
D. Customize the default settings for sessions with the global session settings.
E. Bind a policy to the authentication virtual server that handles the traffic to which the architect wants to apply the profile.

Answer: B,C,E

Question No : 3

Scenario: A Citrix Architect has configured NetScaler Gateway integration with a XenApp environment to provide access to users from two domains: vendorlab.com and workslab.com. The Authentication method used is LDAP.

Which two steps are required to achieve Single Sign-on StoreFront using a single store? (Choose two.)

A. Configure Single sign-on domain in Session profile 'userPrincipalName'.
B. Do NOT configure SSO Name attribute in LDAP Profile.
C. Do NOT configure sign-on domain in Session Profile.
D. Configure SSO Name attribute to 'userPrincipalName' in LDAP Profile.

Answer: B,D

Question No : 4

Scenario: A Citrix Architect has met with a team of Workspacelab members for a design discussion They have captured the following requirements for the Citrix ADC design project:

The authentication must be deployed for the users from the workspacelab com and vendorlab com domains.

- The workspacelab users connecting from the internal (workspacelab) network should be authenticated using LDAP
- The workspacelab users connecting from the external network should be authenticated using LDAP and RADIUS.
- The vendorlab users should be authenticated using Active Directory Federation Service
- The user credentials must NOT be shared between workspacelab and vendorlab
- Single Sign-on must be performed between StoreFront and Citrix Gateway
- A domain drop down list must be provided if the user connects to the Citrix Gateway virtual server externally

Which method must the architect utilize for user management between the two domains?

A. Create a global catalog containing the objects of Vendorlab and Workspacelab domains.

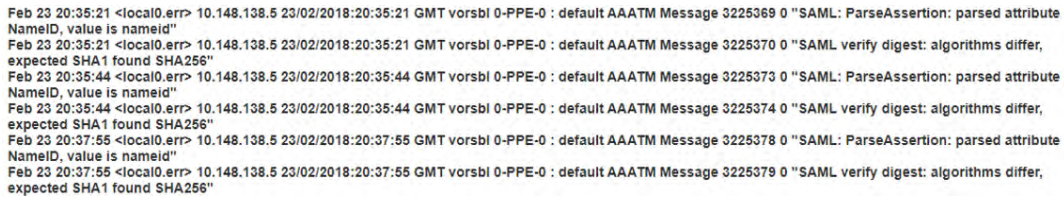
B. Create shadow accounts for the users of the Vendorlab domain in the Workspacelab domain C. Create a two-way trust between the Vendorlab and Workspacelab domains
C. Create shadow accounts for the users of the Workspacelab domain in the Vendorlab domain

Answer: B

Question No : 5

Scenario: A Citrix Architect has deployed an authentication setup with a ShareFile load-balancing virtual server. The NetScaler is configured as the Service Provider and Portalguard server is utilized as the SAML Identity Provider. While performing the functional testing, the architect finds that after the users enter their credentials on the logon page provided by Portalguard, they get redirected back to the Netscaler Gateway page at uri /cgi/samlauth/ and receive the following error.

The events in the /var/log/ns.log at the time of this issue are as follows:



What should the architect change in the SAML action to resolve this issue?

A. Signature Algorithm to SHA 256
B. The Digest Method to SHA 256
C. The Digest Method to SHA 1
D. Signature Algorithm to SHA 1

Answer: C

Question No : 6

Which parameter indicates the number of current users logged on to the Citrix gateway?

A. ICA connections
B. Total Connected Users

C. Active user session
D. Maximum User session

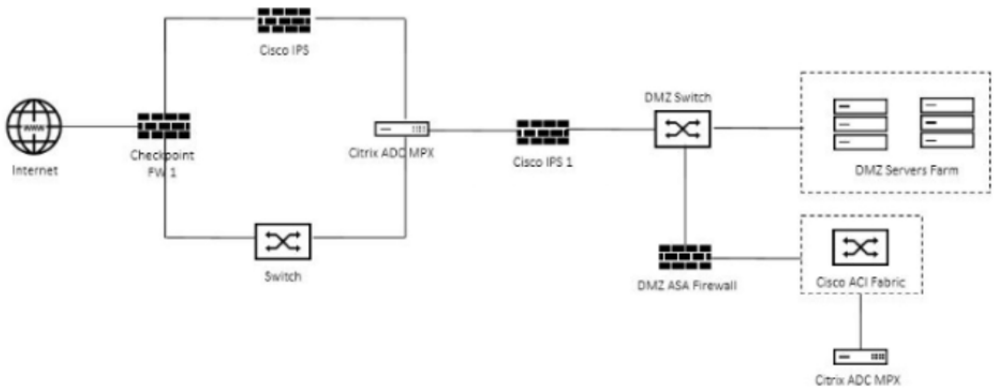
Answer: C

Question No : 7

Scenario: A Citrix Architect and a team of Workspacelab members met to discuss a Citrix ADC design project. They captured the following requirements from this design discussion:

- All three (3) Workspacelab sites (DC, NOR, and DR) will have similar Citrix ADC configurations and design.
- The external Citrix ADC MPX1 appliances will have Global Server Load Balancing (GSLB) configured and deployed in Active/Active mode.
- ADNS service should be configured on the Citrix ADC to make it authoritative for domain nsg.workspacelab.com • In GSLB deployment, the DNS resolution should be performed to connect the user to the site with least network latency.
- On the internal Citrix ADC, load balancing for StoreFront services, Citrix XML services, and Citrix Director services must be configured.
- On the external Citrix ADC, the Gateway virtual server must be configured in ICA proxy mode.

Click the Exhibit button to view the logical representation of the network.



On which firewall should the architect configure the access policy to permit the MEP communication between the sites?

A. CISCO IPS 1 and Checkpoint FW1
B. CISCO IPS and CISCO IPS1

C. CISCO IPS and Checkpoint FW1
D. Checkpoint FW1 and DMZ ASA Firewall

Answer: D

Question No : 8

A Citrix Architect needs to configure advanced features of Citrix ADC by using StyleBooks as a resource in the Heat service.

What is the correct sequence of tasks to be completed for configuring Citrix ADC using the Heat stack?

A.
1. Install Citrix ADC Bundle for OpenStack
2 Register OpenStack with Citrix Application Delivery Management
3. Add Citrix ADC instances (Optional)
4. Create service packages (Add OpenStack tenants)
5. Prepare the HOT by using the Citrix ADC Heat resources and Citrix ADC Network Resource
6. Deploy the Heat stack

B.
1. Install Citrix ADC Bundle for OpenStack
2 Add Citrix ADC instances (Optional)
3. Create service packages (Add OpenStack tenants)
4. Prepare the HOT by using the Citrix ADC Heat resources and Citrix ADC Network Resource
5. Register OpenStack with Citrix Application Delivery Management
6. Deploy the Heat stack

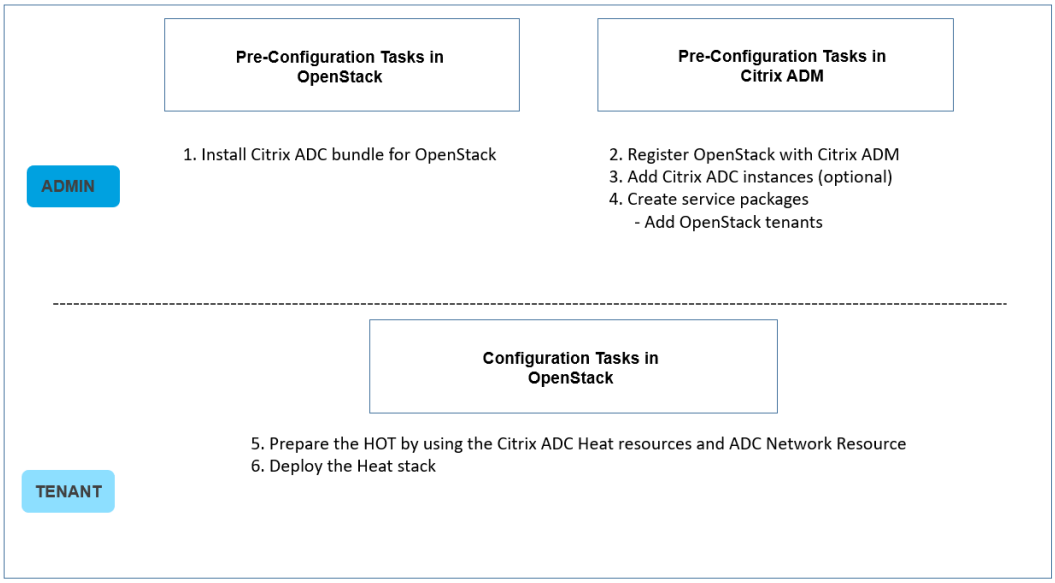
C.
1. Install Citrix ADC Bundle for OpenStack
2. Deploy the Heat stack
3. Register OpenStack with Citrix Application Delivery Management
4. Add Citrix ADC instances (Optional)
5. Prepare the HOT by using the Citrix ADC Heat resources and Citrix ADC Network Resource
6. Create service packages (Add OpenStack tenants)

D.
1. Install NetScaler Bundle for OpenStack
2. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource
3. Register OpenStack with NMAS
4. Deploy the Heat stack

5. Add NetScaler instances (Optional)
6. Create service packages (Add OpenStack tenants)

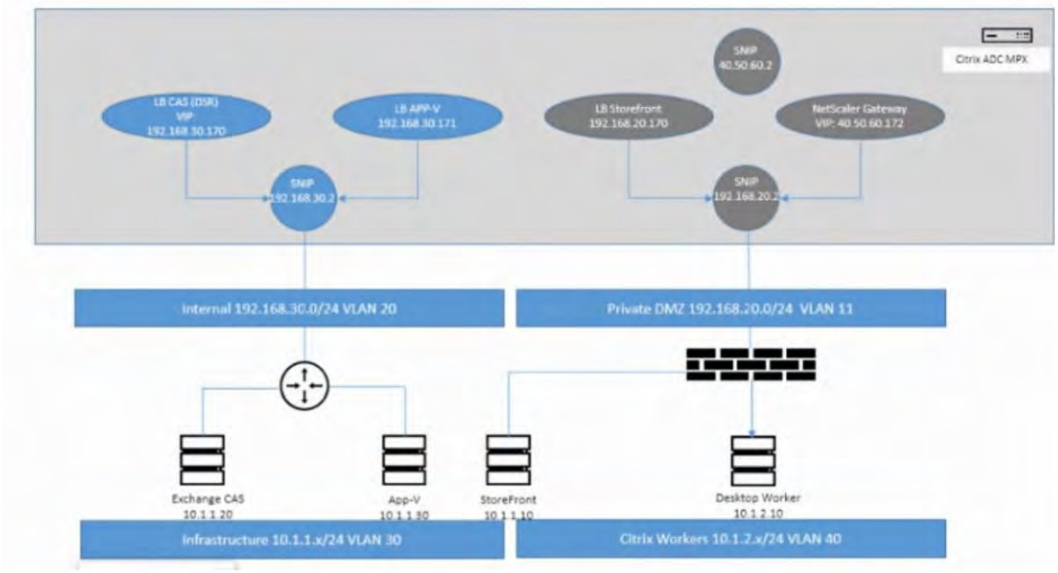
Answer: A

Explanation: -



Workflow to configure ADC instances using Heat

Question No : 9



Which IP address should be bound to VLAN 11?

A. 40.50.60.2
B. 192.168.30.2
C. 40.50.60.172
D. 192.168.20.170
E. 192.168.20.2
F. 192.168.30.171
G. 40.50.60.172

Answer: E

Question No : 10

_____ content type supports sending NITRO commands to NetScaler. (Choose the correct option to complete sentence.)

A. Application/sgml
B. Text/html
C. Application/json
D. Text/enriched

Answer: C

Question No : 11

Scenario: A Citrix Architect has deployed two MPX devices, 12.0.53.13 nc and MPX 11500 models, in a high availability (HA) pair for the Workspace labs team. The deployment method is two-arm. and the devices are installed behind a CISCO ASA 5585 firewall. The architect enables the following features on the Citrix ADC devices: Content Switching. SSL Offloading, Load Balancing, Citrix Gateway, Application Firewall in hybrid security, and Appflow. All are enabled to send monitoring information to Citrix Application Delivery Management 12.0.53.13 nc build. The architect is preparing to configure load balancing for Microsoft Exchange 2016 server.

The following requirements were discussed during the implementation:

- All traffic needs to be segregated based on applications, and the fewest number of IP addresses should be utilized during the configuration.
- All traffic should be secured, and any traffic coming into HTTP should be redirected to HTTPS.

- Single Sign-on should be created for Microsoft Outlook web access (OWA).
- Citrix ADC should recognize Uniform Resource Identifier (URI) and close the session to Citrix ADC, when users hit the Logoff button in Microsoft Outlook web access.
- Users should be able to authenticate using user principal name (UPN).
- The Layer 7 monitor should be configured to monitor the Microsoft Outlook web access servers, and the monitor probes must be sent on SSL.

Which Responder policy can be utilized to redirect the users from http://mail.citrix.com to https://mail.citrix.com/owa?

A. add responder action Act redirect ""https://mail.citrix.com/owa/"" -responseStatusCode 302 add responder policy pol "http.REQ.URL.PATH_AND_QUERY.EQ("/")" Act
B. add responder action Act redirect ""https://mail.citrix.com/owa/"" -responseStatusCode 307 add responder policy pol "HTTP.REQ.IS_NOTVALID Act
C. add responder action Act redirect ""http://mail.citrix.com/owa/"" -responseStatusCode 302 add responder policy pol "HTTP.REQ.IS_NOTVALID Act
D. add responder action Act redirect ""http://mail.citrix.com/owa/"" -responseStatusCode 302 add responder policy pol "http.REQ.URL.PATH_AND_QUERY.EQ("/")" Act

Answer: A

Question No : 12

Scenario: A Citrix Architect has set up NetScaler MPX devices in high availability mode with version 12.0.53.13 nc. These are placed behind a Cisco ASA 5505 Firewall. The Cisco ASA Firewall is configured to block traffic using access control lists. The network address translation (NAT) is also performed on the firewall.

The following requirements were captured by the architect during the discussion held as part of the NetScaler security implementation project with the customer's security team:

The NetScaler MPX device:

- should monitor the rate of traffic either on a specific virtual entity or on the device. It should be able to mitigate the attacks from a hostile client sending a flood of requests. The NetScaler device should be able to stop the HTTP, TCP, and DNS based requests.
- needs to protect backend servers from overloading.
- needs to queue all the incoming requests on the virtual server level instead of the service level.
- should provide protection against well-known Windows exploits, virus-infected personal computers, centrally managed automated botnets, compromised

webservers, known spammers/hackers, and phishing proxies.
- should provide flexibility to enforce the decided level of security check inspections for the requests originating from a specific geolocation database.
- should block the traffic based on a pre-determined header length, URL length, and cookie length. The device should ensure that characters such as a single straight quote (“); backslash (\); and semicolon (;) are either blocked, transformed, or dropped while being sent to the backend server.

Which security feature should the architect configure to meet these requirements?

A. Global Server Load balancing with Dynamic RTT
B. Global Server Load Balancing with DNS views
C. Geolocation-based blocking using Application Firewall
D. geolocation-based blocking using Responder policies
E. Global Server Load Balancing with Mac Based Forwarding

Answer: C

Question No : 13

A Citrix Architect can execute a configuration job using a DeployMasterConfiguration template on a Citrix ADC____deployed_____. (Choose the correct option to complete sentence:

A. MPX; In high availability
B. CPX: without partitions
C. CPX; In high availability
D. MPX; as a cluster Instance
E. SDX; with more than 6 partitions

Answer: A

Question No : 14

A Citrix Architect needs to make sure that maximum concurrent AAA user sessions are limited to 4000 as a security restriction.

Which authentication setting can the architect utilize to view the current configuration?

A. Global Session Settings
B. AAA Parameters
C. Active User Session
D. AAA Virtual Server

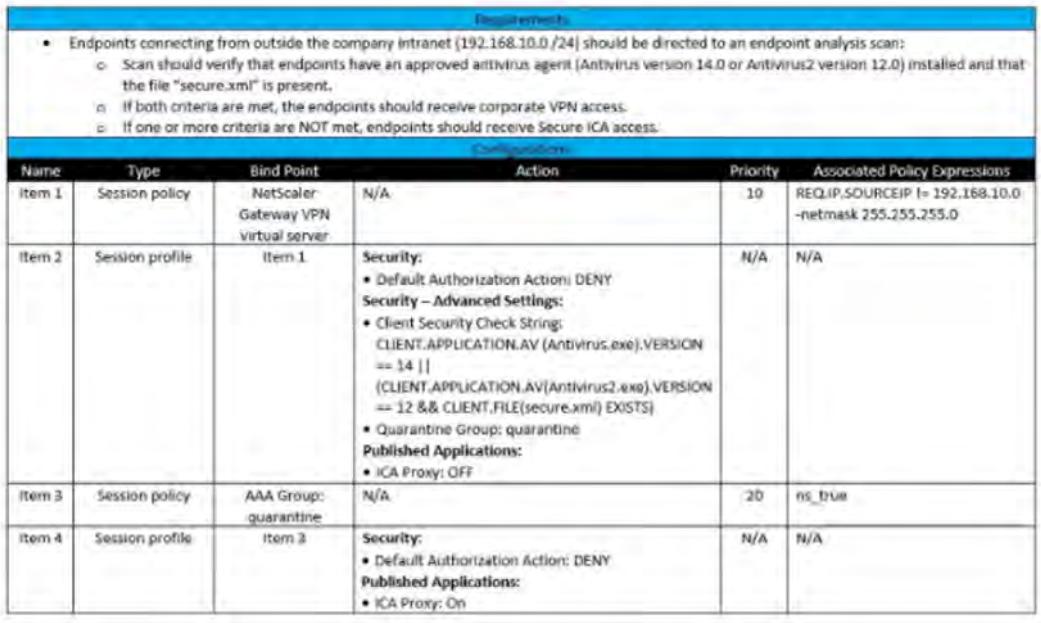
Answer: A

Question No : 15

Scenario: A Citrix Architect needs to assess an existing on-premises NetScaler deployment which includes Advanced Endpoint Analysis scans. During a previous security audit, the team discovered that certain endpoint devices were able to perform unauthorized actions despite NOT meeting pre-established criteria.

The issue was isolated to several endpoint analysis (EPA) scan settings.

Click the Exhibit button to view the endpoint security requirements and configured EPA policy settings.



Requirements

- Endpoints connecting from outside the company intranet (192.168.10.0 /24) should be directed to an endpoint analysis scan:
  - Scan should verify that endpoints have an approved antivirus agent (Antivirus version 14.0 or Antivirus2 version 12.0) installed and that the file "secure.xml" is present.
  - If both criteria are met, the endpoints should receive corporate VPN access.
  - If one or more criteria are NOT met, endpoints should receive Secure ICA access.

Configuration

Name	Type	Bind Point	Action	Priority	Associated Policy Expressions
Item 1	Session policy	NetScaler Gateway VPN virtual server	N/A	10	REQ.IP.SOURCEIP != 192.168.10.0 -netmask 255.255.255.0
Item 2	Session profile	Item 1	**Security:** • Default Authorization Action: DENY **Security – Advanced Settings:** • Client Security Check String: CLIENT.APPLICATION.AV (Antivirus.exe).VERSION == 14 || (CLIENT.APPLICATION.AV(Antivirus2.exe).VERSION == 12 && CLIENT.FILE(secure.xml) EXISTS) • Quarantine Group: quarantine **Published Applications:** • ICA Proxy: OFF	N/A	N/A
Item 3	Session policy	AAA Group: quarantine	N/A	20	ns_true
Item 4	Session profile	Item 3	**Security:** • Default Authorization Action: DENY **Published Applications:** • ICA Proxy: On	N/A	N/A

Which setting is preventing the security requirements of the organization from being met?

A. Item 3
B. Item 4
C. Item 2
D. Item 6

Answer: D

Question No : 16

Which four settings can a Citrix Architect use to create a configuration job using Citrix Application Delivery Management? (Choose four.)

A. Action
B. File
C. Configuration Template
D. StyleBooks
E. Event Manager
F. Instance
G. Record and Play

Answer: B,C,F,G

Question No : 17

Which response is returned by the Citrix ADC, if a negative response is present in the local cache?

A. NXDOMAIN
B. NXDATA
C. NODOMAIN
D. NO DATA

Answer: A

Question No : 18

Which two NetScaler cookies indicate the validity of the Authentication, Authorization and Accounting (AAA) session for users? (Choose two.)

A. NSC_WT
B. NSC_TMAS

C. NSC_AAAC
D. NSC_TMAA

Answer: B,D

Question No : 19

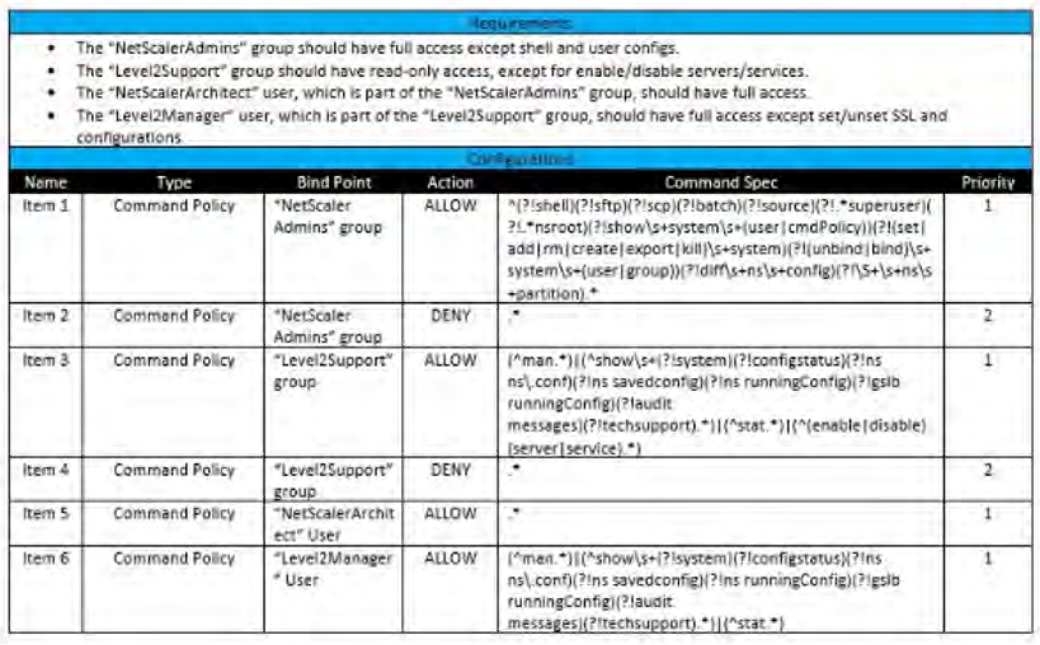
Which three methods can a Citrix Architect use to assess the capabilities of a network infrastructure? (Choose three.)

A. Review existing monitoring solutions for periods of latency, lost packets, and insufficient bandwidth.
B. Map the location of the users against the existing network topology.
C. Alter firewall rules of existing network to fit into the new NetScaler Deployment.
D. Examine the topology for single points of failure and potential bottlenecks.
E. Ensure that users and computers are in the correct organizational units (OUs).

Answer: A,B,D

Question No : 20

Scenario: A Citrix Architect needs to assess an existing Citrix ADC configuration. The customer recently found that members of certain administrator groups were receiving permissions on the production Citrix ADC appliances that do NOT align with the designed security requirements. Click the Exhibit button to view the configured command policies for the production Citrix ADC deployment.



Requirements

- The "NetScalerAdmins" group should have full access except shell and user configs.
- The "Level2Support" group should have read-only access, except for enable/disable servers/services.
- The "NetScalerArchitect" user, which is part of the "NetScalerAdmins" group, should have full access.
- The "Level2Manager" user, which is part of the "Level2Support" group, should have full access except set/unset SSL and configurations.

Configurations

Name	Type	Bind Point	Action	Command Spec	Priority
Item 1	Command Policy	"NetScaler Admins" group	ALLOW	^(?!shell)(?!sftp)(?!scp)(?!batch)(?!source)(?!.*superuser)(?!.*nsroot)(?!show\s+system\s+(user|cmdPolicy))(?!(set|add|rm|create|export|kill)\s+system)(?!(unbind|bind)\s+system\s+(user|group))(?!diff\s+ns\s+config)(?!\S+\s+ns\s+partition).*	1
Item 2	Command Policy	"NetScaler Admins" group	DENY	.*	2
Item 3	Command Policy	"Level2Support" group	ALLOW	(^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*)|(^stat.*)|(^(enable|disable) (server|service).*)	1
Item 4	Command Policy	"Level2Support" group	DENY	.*	2
Item 5	Command Policy	"NetScalerArchitect" User	ALLOW	.*	1
Item 6	Command Policy	"Level2Manager" User	ALLOW	(^man.*)|(^show\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!audit messages)(?!techsupport).*)|(^stat.*)	1

To align the command policy configuration with the security requirements of the organization, the_____for_____should change. (Choose the correct option to complete the sentence.)

A. command spec; Item 6
B. priority; Item 5
C. command spec; Item 3
D. action; Item 4
E. priority; Item 2
F. action; Item 1

Answer: E

Question No : 21

Which two settings must a Citrix Architect enable to deploy a shared VLAN on Citrix ADC VPX instance on an ESX platform? (Choose two.)

A. VLAN tagging on the VLAN
B. Port based VLAN tagging must be enabled
C. Promiscuous mode for shared VLANs
D. VLAN sharing on the VLAN

Answer: C,D