1Y0-440Q&As

Architecting a Citrix Networking Solution

Pass Citrix 1Y0-440 Exam with 100% Guarantee

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

https://www.passapply.com/1y0-440.html

100% Passing Guarantee
100% Money Back Assurance

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

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

Scenario: A Citrix Architect needs to design a new NetScaler Gateway deployment to provide secure RDP access to backend Windows machines.

Click the Exhibit button to view additional requirements collected by the architect during the design discussions.

Topic	Requirements
User experience	Once the user authenticates, they should be directed to a custom home page with the available RDP bookmarks. When a bookmark is clicked, an RDP connection to the backend machine will be established.
Additional considerations	Ensure that users can receive the most optimal RDP connection to backend machines located in different locations.

To meet the customer requirements, the architect should deploy the RDP proxy through _____ using a_____ solution. (Choose the correct option to complete the sentence.)

A. CVPN: single gateway

B. CVPN, stateless gateway

C. ICAProxy: single gateway

D. ICAProxy; stateless gateway

Correct Answer: C

QUESTION 2

Scenario: A Citrix Architect holds a design discussion with a team of Workspacelab members, and they capture the following requirements for the NetScaler design project.

1.

A pair of NetScaler MPX appliances will be deployed in the DMZ network and another pair in the internal network.

2.

High availability will be accessible between the pair of NetScaler MPX appliances in the DMZ network.

3.

Multi-factor authentication must be configured for the NetScaler Gateway virtual server.

4.

The NetScaler Gateway virtual server is integrated with the StoreFront server.

5.

Load balancing must be deployed for users from the workspacelab.com domain.

6.

The workspacelab users should be authenticated using Cert Policy and LDAP.

7.

All the client certificates must be SHA 256-signed, 2048 bits, and have UserPrincipalName as the subject.

8.

Single Sign-on must be performed between StoreFront and NetScaler Gateway.

After deployment, the architect observes that LDAP authentication is failing.

Click the Exhibit button to review the output of aaad debug and the configuration of the authentication policy.

Exhibit 1

```
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/ldap_common.
c[398]: ns_ldap_check_result 0-399: checking LDAP result. Expecting
101 (LDAP_RES_SEARCH_RESULT)
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/ldap_common.
c[436]: ns_ldap_check_result 0-399: ldap_result found expected result
LDAP_RES_SEARCH_RESULT
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/ldap_drv.
c[357]: receive_ldap_user_search_event 0-399: received LDAP_OK
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/naaad.c[4196]:
unregister_timer 0-399: releasing timer 175
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/ldap_drv.c[387]:
receive_ldap_user_search_event 0-399: Binding user… 0 entries
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/ldap_drv.c[388]:
receive_ldap_user_search_event 0-399: Admin authentication (Bind)
succeeded, now attempting to search the user hrl@workspacelab.com
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/ldap_drv.c[393]:
receive_ldap_user_search_event 0-399: ldap_first_entry returned null,
user hrl@workspacelab.com not found
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/naaad.c[3322]:
send_reject_with_code 0-399: Not trying cascade again
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/naaad.c[3324]:
send_reject_with_code 0-399: sending reject to kernel for :
hrl@workspacelab.com
Sun Feb 25 11:41:30 2018
  /home/ build/rs_120_53_3_RTM/usr.src/netscaler/aaad/naaad.c[3327]:
send_reject_with_code 0-399: Rejecting with error code 4009
```

Exhibit 2

```
add authentication ldapAction ldap-sam -serverName 192.168.10.11 -
serverPort 636 -ldapBase "DC=workspacelab, DC-com" -ldapBindDN
administrator@workspacelab.com -ldapBindDnPassword
54e394e320d69a5b3418746e4dc9e83ebf0a1c7ffd869abd3e040b42d38e4b2e -
encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
groupAttrName memberOf -subAttributeName cn -secType SSL -
ssoNameAttribute cn
add authentication ldapPolicy ldap-samaccount ns_true ldap-sam
add authentication certAction cert-upn -twoFactor ON -userNameField
Subject:CN
add authentication certPolicy cert ns_true cert-upn
```

What is causing this issue?

A. UserNamefield is set as subjection

B. Password used is incorrect

C. User does NOT exist in database

D. IdapLoginName is set as sAMAccountName

Correct Answer: A

QUESTION 3

A Citrix Architect has deployed NetScaler Management and Analytics System (NMAS) to monitor a high availability pair of NetScaler VPX devices.

The architect needs to deploy automated configuration backup to meet the following requirements:

1.

The configuration backup file must be protected using a password.

2.

The configuration backup must be performed each day at 8:00 AM GMT.

3.

The configuration backup must also be performed if any changes are made in the ns.conf file.

4.

Once the transfer is successful, auto-delete the configuration file from the NMAS.

Which SNMP trap will trigger the configuration file backup?

A. netScalerConfigSave

B. sysTotSaveConfigs

C. netScalerConfigChange

D. sysconfigSave

Correct Answer: A

Reference: https://docs.citrix.com/en-us/netscaler-mas/12/instance-management/how-to-backup-andrestore-using-mas.html#configuring-instance-backup-settings

QUESTION 4

Scenario: A Citrix Architect needs to assess an existing NetScaler configuration. The customer recently found that members of certain administrator groups were receiving permissions on the production NetScaler appliances that do NOT align with the designed security requirements.

Click the Exhibit button to view the configured command policies for the production NetScaler 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	Commands 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+ns\s+config) (?!\S+\s+ns\s+partitition).*	1
Item 2	Command Policy	"NetScaler" group	DENY	.*	2
Item 3	Command Policy	"Level2Support" group	ALLOW	(^main.*)(^show\s+ (?!system)(?!configstatus) (?!nsns\.conf) (?!ns savedconfig) (?!ns runningConfig) (?!gslbrunningConfig) (?!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	(^main.*) | (^show\s+ (?!system) (?!configstatus) (?!nsns\.conf) (?!ns savedconfig) (?!ns runningConfig) (?!gslbrunningConfig) (?!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 3

B. priority; Item 5

C. action; Item 1

D. priority; Item 2

E. action; Item 4

F. command spec; Item 6

Correct Answer: D

QUESTION 5

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 should be scanned to determine whether they are connecting from within the company intranet (192.168.10.0/24) and belong to the company Windows domain (workspacelab.com).
  - Endpoints meeting both of these criteria are permitted to continue to the authentication page.
  - Endpoints NOT meeting 1 or more of these criteria should NOT be permitted to authenticate.
- All endpoints should also be scanned to confirm that an approved antiVirus client ("Antivirus") is running.
  - Endpoints that have an antivirus client running can access intranet resources.
  - Endpoints that do NOT have an antivirus client running should be added to quarantine group that can only access the XenApp and XenDesktop environment.

Configurations

Name	Type	Bind Point	Action	Priority	Associated Policy Expressions
Item 1	Preauthentication setting	Global-NetScaler Gateway	Allow	N/A	ns_true
Item 2	Preauthentication policy	NetScaler Gateway VPN virtual server	N/A	10	REQ.IPSOURCEIP == 192.168.10.0 -netmask 255.255.255.0 && CLIENT.SYSTEM (DOMAIN_SUFFIX_ anyof_workspacelab EXISTS
Item 3	Preauthentication profile	Item 2	Allow	N/A	N/A
Item 4	Session policy	NetScaler Gateway VPN virtual server	N/A	20	ns_true
Item 5	Session profile	Item 4	**Security:** - Default Authorization Action: DENY **Security-Advanced Settings:** - Client Security Check String: CLIENT.APPLICATION. PROCESS (antivirus.exe) EXISTS - Quarantine Group: quarantine **Published Applications:** - ICA Proxy: OFF	N/A	N/A
Item 6	Session policy	AAA Group: quarantine	N/A	30	ns_true
Item 7	Session profile	Item 6	**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 6

B. Item 7

C. Item 1

D. Item 3

E. Item 5

F. Item 2

G. Item 4

Correct Answer: F

Latest 1Y0-440 Dumps 1Y0-440 PDF Dumps 1Y0-440 VCE Dumps