

# 1Y0-440<sup>Q&As</sup>

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.pass2lead.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: Based on a discussion between a Citrix Architect and team of Workspacelab has been created across three (3) sites.

They captured the following requirements during the design discussion held for NetScaler design projects:

1.

All three (3) Workspacelab sites (DC, NDR, and DR) will have similar NetScaler configuration and design.

2.

Both external and internal NetScaler MPX appliances will have Global Server Load balancing (GSLB) configured and deployed in Active/Passive mode.

3.

GSLB should resolve both A and AAA DNS queries.

4.

In the GSLB deployment, the NDR site will act as backup for the DC site. whereas the DR site will act as backup for the NDR site.

5.

When the external NetScaler replies to DNS traffic coming in through Cisco Firepower IPS, the replies should be sent back through the same path.

6.

On the internal NetScaler, both front-end VIP and back-end SNIP will be part of the same subnet.

7.

USIP is configured on the DMZ NetScaler appliances.

8.

The external NetScaler will act default gateway for back-end servers.

9.

All three (3) sites (DC, NDR, and DR) will have two (2) links to the Internet from different service providers configured in Active/Standby mode.

Which design decision must the architect make to meet the design requirements above?

A. Interface 0/1 must be used for DNS traffic.

B. The SNIP of the external NetScaler must be configured as default gateway on the back-end servers.

C. ADNS service must be used with IPv6 address.

D. Policy-Based Route with next hop as CISCO IPS must be configured on the external NetScaler.

Correct Answer: C

## QUESTION 2

Which parameter must a Citrix Architect configure to ensure that HDX Proxy Connection terminates upon AAA Session TimeOut?

- A. ICA session timeout in VPN parameters
- B. Session timeout(mins) in NetScaler gateway Session Profile.
- C. Session timeout(mins) in VPN Parameters
- D. ICA session timeout in netScaler Gateway Session Profile.

Correct Answer: D

Reference: [https://www.citrix.com/content/dam/citrix/en\\_us/citrix-developer/documents/Netscaler/how-do-ica-session-timeout-with-aaa.pdf](https://www.citrix.com/content/dam/citrix/en_us/citrix-developer/documents/Netscaler/how-do-ica-session-timeout-with-aaa.pdf)

## QUESTION 3

Scenario: A Citrix Architect needs to design a NetScaler deployment in Microsoft Azure. An Active-Passive NetScaler VPX pair will provide load balancing for three distinct web applications. The architect has identified the following requirements:

1.

Minimize deployment costs where possible.

2.

Provide dedicated bandwidth for each web application.

3.

Provide a different public IP address for each web application.

For this deployment, the architect should configure each NetScaler VPX machine to have \_\_\_\_\_ network interface(s) and configure IP address by using \_\_\_\_\_. (Choose the correct option to complete the sentence).

- A. 4; Port Address Translation
- B. 1; Network Address Translation
- C. 1; Port Address Translation
- D. 2; Network Address Translation
- E. 4; Network Address Translation

F. 2; Port Address Translation

Correct Answer: C

---

#### QUESTION 4

\_\_\_\_\_ 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

Correct Answer: B

---

#### QUESTION 5

Scenario: A Citrix Architect needs to deploy a NetScaler appliance for Workspacelab, which will provide application load balancing services to Partnerlab and Vendorlab.

The setup requirements are as follows:

1.

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

2.

High availability will be accessible on the NetScaler MPX in the DMZ Network.

3.

Load balancing should be performed for the mail servers for Partnerlab and Vendorlab.

4.

The traffic for both of the organizations must be isolated.

5.

Separate Management accounts must be available for each client.

6.

The load-balancing IP addresses must be identical.

7.

A separate VLAN must be utilized for communication for each client.

Which solution can the architect utilize to meet the requirements?

- A. Traffic Domain
- B. Admin Partition
- C. VLAN Filtering
- D. VPX or MPX

Correct Answer: D

#### QUESTION 6

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

1.

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

2.

The workspacelab users connecting from the internal (workspacelab) network should be authenticated using LDAP.

3.

The workspacelab users connecting from the external network should be authenticated using LDAP and RADIUS.

4.

The vendorlab users should be authenticated using Active Directory Federation Service.

5.

The user credentials must NOT be shared between workspacelab and vendorlab.

6.

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

7.

A domain drop down list must be provided if the user connects to the NetScaler gateway virtual server externally.

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

- A. Create shadow accounts for the users of the Workspacelab domain in the Vendorlab domain.
- B. Create a global catalog containing the objects of Vendorlab and Workspacelab domains.
- C. Create shadow accounts for the Vendorlab domain in the Workspacelab domain.
- D. Create a two-way trust between the Vendorlab and Workspacelab domains.

Correct Answer: B

---

#### QUESTION 7

Scenario: A Citrix Architect needs to plan for a customer environment in which more than 10,000 users will need access. The networking infrastructure needs to be able to handle the expected usage.

Which business driver should be prioritized based on the customer's requirement?

- A. Increase flexibility
- B. Enable mobile work styles
- C. Simplify management
- D. Increase Scalability
- E. Reduce Costs
- F. Increase Security

Correct Answer: D

---

#### QUESTION 8

Scenario: The following NetScaler environment requirements were discussed during a design meeting between a Citrix Architect and the Workspacelab team:

1.

All traffic should be secured, and any traffic coming into HTTP should be redirected to HTTPS.

2.

Single Sign-on should be created for Microsoft Outlook web access (OWA).

3.

NetScaler should recognize Uniform Resource Identifier (URI) and close the session to NetScaler when users hit the Logoff button in Microsoft Outlook web access.

4.

Users should be able to authenticate using user principal name (UPN).

5.

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 method can the architect use to redirect the user accessing <https://mail.citrix.com> to [https:// mail.citrix.com](https://mail.citrix.com)?

A. add responder action act redirect "https://mail.citrix.com" -responseStatusCode 302 add responder policy pol HTTP.REQ.IS\_VALID act

B. add lb server test SSL 10.107.149.243.80 -persistenceType NONE -cltTimeout 180 -redirectFromPort 80 -httpsRedirectUrl https://mail.citrix.com

C. add lb server test SSL 10.107.149.243.443 -persistenceType NONE -cltTimeout 180 -redirectFromPort 80 -httpsRedirectUrl https://mail.citrix.com

D. add responder action act redirect "\https://\ + HTTP REQ.HOSTNAME.HTTP\_URL\_SAFE + HTTP.REQ.URL\_PATH\_AND\_QUERY.HTTP\_URL\_SAFE\n\n" -responseStatusCode 302 add responder policy pol HTTP.REQ.IS\_VALID act

Correct Answer: C

---

### QUESTION 9

Scenario: A Citrix Architect needs to configure a full VPN session profile to meet the following requirements:

1.

Users should be able to send the traffic only for the allowed networks through the VPN tunnel.

2.

Only the DNS requests ending with the configured DNS suffix workspacelab.com must be sent to NetScaler Gateway.

3.

If the DNS query does NOT contain a domain name, then DNS requests must be sent to NetScaler gateway.

Which settings will meet these requirements?

A. Split Tunnel to OFF, Split DNS Both

B. Split Tunnel to ON, Split DNS Local

C. Split Tunnel to OFF, Split DNS Remote

D. Split Tunnel to ON, Split DNS Remote

Correct Answer: B

---

### QUESTION 10

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.

Correct Answer: BD

Reference: <https://docs.citrix.com/en-us/storefront/3-12/plan/user-authentication.html>

---

#### QUESTION 11

Scenario: A Citrix Architect needs to assess an existing NetScaler configuration. The customer recently found that certain user groups were receiving access to an internal web server with an authorization configuration that does NOT align with the designed security requirements.

Click the Exhibit button view the configured authorization settings for the web server.



| Requirements  |                       |   |        |          |   |
|---|-----------------------|---|--------|----------|---|
| <ul style="list-style-type: none"> <li>By default, no connection should have access to network resources unless authorized based on the other requirements.</li> <li>By default, only connections coming from the internal network (192.168.10.0/24) should be permitted to access the web server.</li> <li>The Accountants group is authorized to access URLs with a “.zip” extension; all other users must NOT be authorized for this.</li> <li>The Executives group is authorized to access the web server from inside OR outside the internal network.</li> </ul> |                       |   |        |          |   |
| Configurations  |                       |   |        |          |   |
| Name  | Type                  | Bind Point                                  | Action | Priority | Associated Policy Expressions             |
| Item 1  | Authorization setting | Global                                      | DENY   | N/A      | N/A                                       |
| Item 2  | Authorization Policy  | NetScaler traffic management virtual server | ALLOW  | 1        | Client.IP.SRC.IN_SUBNET (192.168.10.0/24) |
| Item 3  | Authorization Policy  | NetScaler traffic management virtual server | DENY   | 2        | HTTP.REQ.URL.SUFFIX.EQ (“zip”)            |
| Item 4  | Authorization Policy  | Accountants Group                           | ALLOW  | 1        | HTTP.REQ.URL.SUFFIX.EQ (“zip”)            |
| Item 5  | Authorization Policy  | Executives Group                            | ALLOW  | 1        | Client.IP.SRC.NE (192.168.10.0/24)        |

Which item should the architect change or remove to align the authorization configuration with the security requirements of the organization?

- A. Item 1
- B. Item 3
- C. Item 4
- D. Item 5
- E. Item 2

Correct Answer: E

## QUESTION 12

Which two features are supported on LbaaSV1? (Choose two.)

- A. Cookie Insertion
- B. Layer 7 Load Balancing
- C. Certificate Bundle
- D. Layer 4 Load balancing
- E. Server name Indicator

Correct Answer: DE

### QUESTION 13

Scenario: Based on a discussion between a Citrix Architect and a team of Workspacelab members, the MPX Logical layout for Workspacelab has been created across three (3) sites.

The requirements captured during the design discussion held for a NetScaler design project are as follows:

1.

Two (2) pairs of NetScaler MPX appliances deployed in the DMZ and internal network.

2.

High Availability will be accessible for each NetScaler MPX

3.

The external NetScaler MPX appliance will be deployed in multi-arm mode.

4.

The internal NetScaler MPX will be deployed in single-arm mode wherein it will be connected to Cisco ACI Fabric.

5.

All three (3) Workspacelab sites: Dc, NDR and DR, will have similar NetScaler configurations and design.

How many NetScaler MPX appliances should the architect deploy at each site to meet the design requirements above?

- A. 4
- B. 12
- C. 6
- D. 2

Correct Answer: C

**QUESTION 14**

Scenario: A Citrix Architect and a team of Workspacelab members have met for a design discussion about the NetScaler Design Project. They captured the following requirements:

1.  
Two pairs of NetScaler MPX appliances will be deployed in the DMZ network and 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 XenApp/XenDesktop environment.
5.  
Load balancing must be deployed for the users from the workspacelab.com and vendorlab.com domains.
6.  
The logon page must show the workspacelab logo.
7.  
Certificate verification must be performed to identify and extract the username.
8.  
The client certificate must have UserPrincipalName as a subject.
9.  
All the managed workstations for the workspace users must have a client identifications certificate installed on it.
- 10.The workspacelab users connecting from a managed workstation with a client certificate on it should be authenticated using LDAP. 11.The workspacelab users connecting from a workstation without a client certificate should be authenticated using LDAP and RADIUS.
- 12.The vendorlab users should be authenticated using Active Directory Federation Service.
- 13.The user credentials must NOT be shared between workspacelab and vendorlab.
- 14.Single Sign-on must be performed between StoreFront and NetScaler Gateway.

15. A domain drop down list must be provided if the user connects to the NetScaler Gateway virtual server externally.

16. The domain of the user connecting externally must be identified using the domain selected from the domain drop down list.

On performing the deployment, the architect observes that users are always prompted with two-factor authentication when trying to access externally from an unmanaged workstation.

Click the exhibit button to view the configuration.

```
> show authentication vserver aaa_dmz_001
aaa_dmz_001 (192.168.30.131:443) - SSL Type: CONTENT
State: UP
Client Idle Timeout: 180 sec
Down state flush: DISABLED
Disable Primary Vserver On Down : DISABLED
Network profile name: ???
Appflow logging: ENABLED
Authentication : ON
Device Certificate Check: ???
Device Certificate CA List: ???
CGInfra Homepage Redirect : ???
Current AAA Sessions: 0
Total Connected Users: 0
Dtls : ???      L2Conn: ???
RDP Server Profile Name: ???
Max Login Attempts: 0      Failed Login Timeout 0
Fully qualified domain name: ???
PCoIP VServer Profile name: ???
Listen Policy: NONE
Listen Priority: 0
IcmpResponse: ???
RHlstate: ???
Traffic Domain: 0

1)  LoginSchema Policy Name: LDAP_RADIUS      Priority: 100
    GotoPriority Expression: END

1)  Advanced Authentication Policy Name: cert-upn  Priority: 100
    GotoPriority Expression: NEXT
    NextFactor name: OnlyLDAP
2)  Advanced Authentication Policy Name: No_AUTH  Priority: 110
    GotoPriority Expression: NEXT
    NextFactor name: ldap-radius
3)  Advanced Authentication Policy Name: saml-upn  Priority: 120
    GotoPriority Expressions: NEXT

Done
```

What should the architect do to correct this configuration?

A. Unbind LoginSchema Policy LDAP\_RADIUS from the virtual server.

- B. Bind the Portal theme as Domaindropdown.
- C. Bind the LoginSchema Policy Domaindropdown to priority 90.
- D. Bind the Default LoginSchema Policy as Domaindropdown.

Correct Answer: D

---

#### QUESTION 15

Scenario: A Citrix Architect needs to deploy a load balancing for an application server on the NetScaler. The authentication must be performed on the NetScaler. After the authentication, the Single Sign-on with the application servers must be performed using Kerberos impersonation.

Which three authentication methods can the Architect utilize to gather the credentials from the user in this scenario? (Choose three.)

- A. SAML
- B. OTP
- C. TACACS
- D. WEBAUTH
- E. LDAP

Correct Answer: ADE

[1Y0-440 VCE Dumps](#)

[1Y0-440 Practice Test](#)

[1Y0-440 Braindumps](#)