Number: 1Y0-440
Passing Score: 800
Time Limit: 120
File Version: 5.0

# Exam Code: 1Y0-440

# Exam Name: Architecting a Citrix Networking Solution

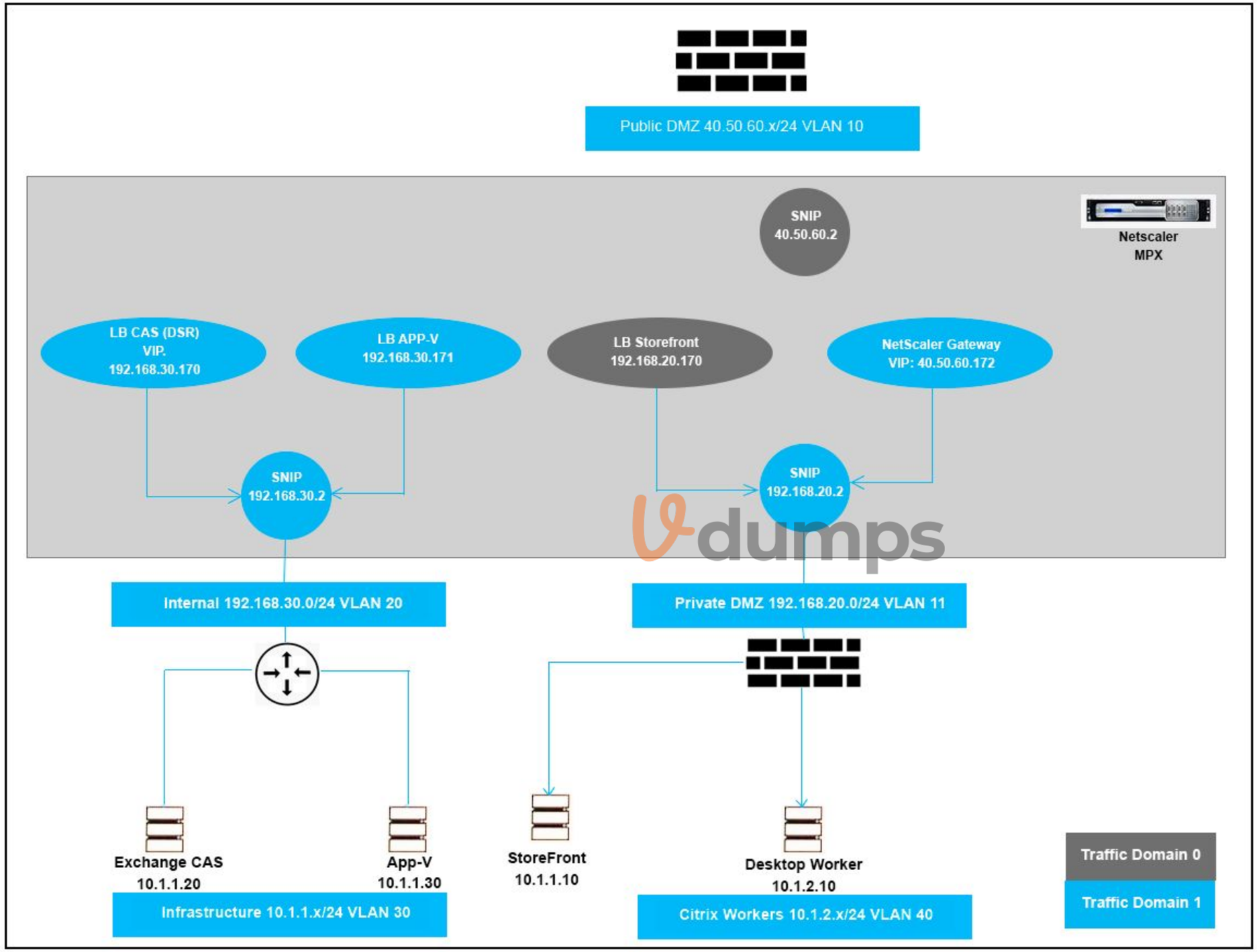
**Exam A**

**QUESTION 1**
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:
Two (2) pairs of NetScaler MPX appliances deployed in the DMZ and internal network.
High Availability will be accessible for each NetScaler MPX
The external NetScaler MPX appliance will be deployed in multi-arm mode.
The internal NetScaler MPX will be deployed in single-arm mode wherein it will be connected to Cisco ACI Fabric.
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**
**Section:**

**QUESTION 2**
Scenario: A Citrix Architect and a team of Workspacelab members met to discuss a NetScaler design project. They captured the following requirements from this design discussion:
A pair of NetScaler MPX appliances will be deployed in the DMZ network.
High Availability will be accessible in the NetScaler MPX in the DMZ Network.
Load balancing should be performed for the internal network services like Microsoft Exchange Client Access Services and Microsoft App-V.
The load balancing should be performed for StoreFront.
The NetScaler Gateway virtual server will be utilizing the StoreFront load-balancing virtual server.
The NetScaler Gateway virtual server and StoreFront.
The NetScaler Gateway virtual service and StoreFront and load-balancing services are publicly accessible.
The traffic for internal and external services must be isolated.
Click the Exhibit button to review the logical network diagram.




Which two design decisions are incorrect based on these requirements? (Choose two.)

A. LB StoreFront bound to traffic Domain 0
B. NetScaler Gateway VIP bound to Traffic Domain 1

C. LB APP-V bound to Traffic Domain 1
D. SNIP 192.168.20.2 bound to Traffic Domain 1

**Correct Answer: A, B**
**Section:**

**QUESTION 3**
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**
**Section:**

**QUESTION 4**
Scenario: A Citrix Architect needs to deploy SAML integration between NetScaler (Identity Provider) and ShareFile (Service Provider). The design requirements for SAML setup are as follows:
NetScaler must be deployed as the Identity Provider (IDP).
ShareFile server must be deployed as the SAML Service Provider (SP).
The users in domain workspacelab.com must be able to perform Single Sign-on to ShareFile after authenticating at the NetScaler.
The User ID must be UserPrincipalName.
The User ID and Password must be evaluated by NetScaler against the Active Directory servers SFO-ADS-001 and SFO-ADS-002.
After successful authentication, NetScaler creates a SAML Assertion and passes it back to ShareFile.
Single Sign-on must be performed.
SHA 1 algorithm must be utilized.
The verification environment details are as follows:
Domain Name: workspacelab.com
NetScaler AAA virtual server URL https://auth.workspacelab.com
ShareFile URL https://sharefile.workspacelab.com
Which SAML IDP action will meet the design requirements?

A. add authentication samIIdPProfile SAMI-IDP --samISPCertName Cert_1 --samIIdPCertName Cert_2 --assertionConsimerServiceURL ''https://auth.workspacelab.com/samIIssueName auth.workspacelab.com -signatureAlg RSA-SHA256-digestMethod SHA256-encryptAssertion ON -serviceProviderUD sharefile.workspacelad.com
B. add authentication samIIdPProfile SAMI-IDP --samISPCertName Cert_1 --samIIdPCertName Cert_2 --assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs'' --samIIssuerName sharefile.workspacelab.com --signatureAlg RSA-SHA256 --digestMethod SHA256 --serviceProviderID sharefile.workspacelab.com
C. add authentication samIIdPProfile SAMI-IDP --samISPCertName Cert_1 --samIIdPCertName Cert_2 --assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs'' --samIIssuerName auth.workspacelab.com --signatureAlg RSA-SHA1-digestMethod SHA1 --encryptAssertion ON --serviceProviderID sharefile.workspacelab.com
D. add authentication samIIdPProfile SAMI-IDP --samISPCertName Cert_1 --samIIdPCertName Cert_2 --assertionConsimerServiceURL https://sharefile.workspacelab.com/saml/acs'' --samIIssuerName sharefile.workspacelab.com --signatureAlg RSA-SHA1 --digestMethod SHA1 --encryptAssertion ON --serviceProviderID sharefile.workspacelab.com

**Correct Answer: C**
**Section:**

**QUESTION 5**
What can help a Citrix Architect prepare to discuss time scales and resource requirements?

A. Creating a high-level project plan.
B. Meeting with each member of the project team to assign tasks.
C. Designing the new environment.
D. Setting expectations with the project's key stakeholders.
E. Identifying challenges associated with the project.

**Correct Answer: A**
**Section:**

**QUESTION 6**
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.
A pair of NetScaler MPX appliances will be deployed in the DMZ network and another pair in the internal network.
High availability will be accessible between the pair of NetScaler MPX appliances in the DMZ network.
Multi-factor authentication must be configured for the NetScaler Gateway virtual server.
The NetScaler Gateway virtual server is integrated with the StoreFront server.
Load balancing must be deployed for users from the workspacelab.com domain.
The workspacelab users should be authenticated using Cert Policy and LDAP.
All the client certificates must be SHA 256-signed, 2048 bits, and have UserPrincipalName as the subject.
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**
**Section:**

**QUESTION 7**
Which markup language can a Citrix use along with NITRO API to create a StyleBook?

A. GML
B. XML
C. HTML
D. YAML

**Correct Answer: D**
**Section:**
**Explanation:**

**QUESTION 8**
Scenario: The Workspacelab team has configured their NetScaler Management and Analytics (NMAS) environment. A Citrix Architect needs to log on to the NMAS to check the settings.
Which two authentication methods are supported to meet this requirement? (Choose two.)

A. Certificate
B. RADIUS
C. TACACS
D. Director
E. SAML
F. AAA

**Correct Answer: B, C**
**Section:**

**QUESTION 9**
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: B, D**
**Section:**

**QUESTION 10**
Scenario: A Citrix Architect has implemented two high availability pairs of MPX 5500 and MPX 11500 devices respectively with 12.0.53.13 nc version. The NetScaler devices are set up to handle NetScaler Gateway, Load Balancing, Application Firewall, and Content Switching. The Workspacelab infrastructure is set up to be monitored with NMAS version 12.0.53.13 nc by the Workspacelab administrators. The Workspacelab team wants to implement one more pair of NetScaler MPX 7500 devices with version 12.0.53.13 nc.
The Citrix consulting team has assigned the task to implement these NetScaler devices in the infrastructure and set them up to be monitored and managed by NMAS.
The following are the requirements that were discussed during the project initiation call:
NMAS should be configured to get the infrastructure information under sections such as HDX Insight, WEB Insight, and Security Insight.
Configuration on the new MPX devices should be identical to MPX 11500 devices.
Configuration changes after the deployment and initial setup should be optimized using NMAS.
NMAS should be utilized to configure templates that can be utilized by the Workspacelab team in future deployment.
As per the requirement from the Workspacelab team, NMAS should be store the audited data for only 15 days.
Which process should the architect utilize to ensure that the deployment of MPX 11500 devices are optimized and that it is correct, before deploying the devices in production?

A. Under Stylebooks; Inbuilt and composite stylebook templates should be utilized prior to deployment.
B. Under Stylebooks; Public and composite stylebook templates should be utilized prior to deployment.
C. Under Configuration Management; Configuration Audit and Advice should be used prior to deployment.
D. Under Configuration jobs; Configuration Audit and Advice should be used prior to deployment.

**Correct Answer: C**
**Section:**

**QUESTION 11**
Scenario: A Citrix Architect needs to assess a NetScaler Gateway deployment that was recently completed by a customer and is currently in pre-production testing. The NetScaler Gateway needs to use ICA proxy to provide access to a XenApp and XenDesktop environment. During the assessment, the customer informs the architect that users are NOT able to launch published resources using the Gateway virtual server.
Click the Exhibit button to view the troubleshooting details collected by the customer.

| Issue Details |
| --- |
| • External users trying to launch a Shared Hosted Desktop via a NetScaler gateway connection receive an ICA file from StoreFront.<br>• However, they are unable to launch the Shared Hosted Desktop.<br>• The following ports are open on the firewall between the NetScaler gateway and the internal network where the Virtual Delivery Agent machines are located:<br>Bidirectional: TCP 80, TCP 443, TCP 2598, TCP 1494<br>• Users located on the internal network who connect directly to the StoreFront server are able to launch the Shared Hosted Desktop. |

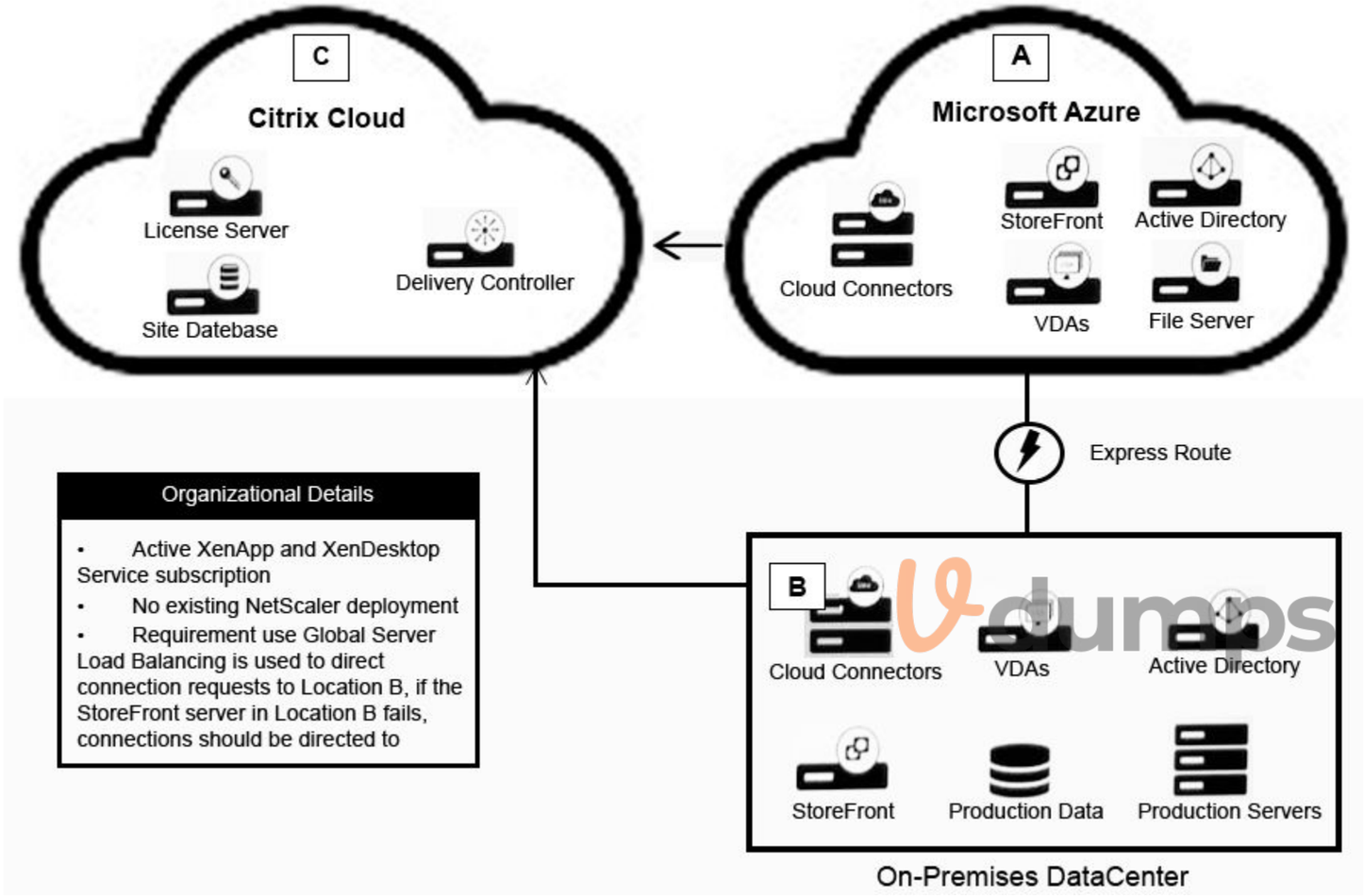
What is the cause of this issue?

A. The required ports have NOT been opened on the firewall between the NetScaler gateway and the Virtual Delivery Agent (VDA) machines.
B. The StoreFront URL configured in the NetScaler gateway session profile is incorrect.
C. The Citrix License Server is NOT reachable.
D. The Secure Ticket Authority (STA) servers are load balanced on the NetScaler.

**Correct Answer: D**
**Section:**

**QUESTION 12**
Scenario: A Citrix Architect needs to design a hybrid XenApp and XenDesktop environment which will include Citrix Cloud as well as resource locations in an on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:

Active XenApp and XenDesktop Service subscription
No existing NetScaler deployment
Global Server Load Balancing is used to direct connection requests to Location B, if the StoreFront server in Location B fails, connections should be directed to Location A.
Click the Exhibit button to view the conceptual environment architecture.




The architect should use _____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. NetScaler ADC (BYO); NetScaler gateway appliance
B. NetScaler ADC (BYO); No NetScaler products
C. NetScaler ADC (BYO); NetScaler ADC (BYO)
D. NetScaler Gateway appliance; NetScaler Gateway appliance
E. NetScaler Gateway appliance; NetScaler ADC (BYO)

**Correct Answer: B**
**Section:**
**Explanation:**
-- NetScaler Gateway as a service doesnot perform loadbalancing, GSLB and two factor authentication. -- NetScaler ADC (BYO) is for full feature ADC. (Azure Support only BYO). -- NetScaler ICA Proxy doesnot perform loadbalancing, GSLB. Cloud Hosted NetScaler Gateway can only be deployed in ICA-Proxy mode to enable remote access to published resources.
Note the requirements: -- Multifactor authentication -- Loadbalancing in site B

**QUESTION 13**
Scenario: A Citrix Architect needs to assess an existing NetScaler Gateway deployment. During the assessment, the architect collected key requirements for VPN users, as well as the current session profile settings that are applied to those users.
Click the Exhibit button to view the information collected by the architect.

| Requirements |
|---|
| • Users should use the NetScaler Gateway plugin to authenticate and connect to internal resources, including intranet web pages and StoreFront.<br>• After authenticating users should be directed to the organization's intranet portal.<br>• Once connected, outbound traffic from the client device should only pass through the NetScaler Gateway if it is directed toward an intranet resource. |

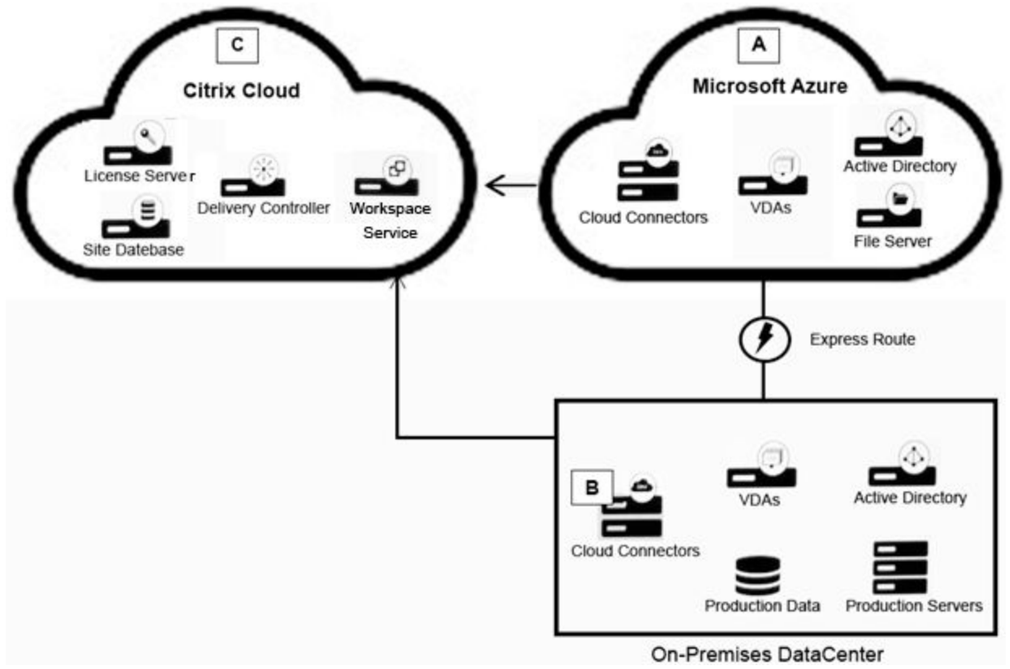
| Configurations | | | |
|---|---|---|---|
| **Name** | **Type** | **Setting** | **Configuration** |
| Item 1 | Network Configuration | Home Page | home.workspacelabs.net |
| Item 2 | Client Experience | Split Tunnel | ON |
| Item 3 | Client Experience | Clientless Access | ON |
| Item 4 | Client Experience | Client Choices | Not enabled |
| Item 5 | Published Applications | ICA Proxy | OFF |

Which configurations should the architect change to meet all the stated requirements?

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

**Correct Answer: B**
**Section:**

**QUESTION 14**
Scenario: A Citrix Architect needs to design a hybrid XenApp and XenApp and XenDesktop environment which will include Citrix Cloud as well as resource locations in on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:
Active XenApp and XenDesktop Service subscription
No existing NetScaler deployment
About 3,000 remote users are expected to regularly access the environment
Multi-factor authentication should be used for all external connections
Solution must provide load balancing for backend application servers
Load-balancing services must be in Location B
Click the Exhibit button to view the conceptual environment architecture.




The architect should use _____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. Citrix Gateway as a Service, no NetScaler products
B. No Citrix products, Citrix ADC (BYO)
C. Citrix Gateway as a Service, Citrix ADC (BYO)
D. No Citrix products, Citrix ICA Proxy (cloud-licensed)
E. Citrix Gateway as a Service, Citrix ICA Proxy (cloud-licensed)
F. No Citrix products; Citrix Gateway appliance

**Correct Answer: C**
**Section:**

**QUESTION 15**
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:
Minimize deployment costs where possible.
Provide dedicated bandwidth for each web application.
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**
**Section:**

**QUESTION 16**
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.
They captured the following requirements during the design discussion held for a Citrix ADC design project:
All three (3) Workspacelab sites (DC, NDR, and DR) will have similar NetScaler configurations and design.
Both external and internal NetScaler MPX appliances will have Global Server Load Balancing (GSLB) configured and deployed in Active/Passive mode.
GSLB should resolve both A and AAA DNS queries.
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.
When the external NetScaler replies to DNS traffic coming in through Cisco Firepower IPS, the replies should be sent back through the same path.
On the internal NetScaler, both the front-end VIP and backend SNIP will be part of the same subnet.
The external NetScaler will act as default gateway for the backend servers.
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 the design requirements above?

A. MAC-based Forwarding must be enabled on the External NetScaler Pair.
B. NSIP of the External NetScaler must be configured as the default gateway on the backend servers.
C. The Internal NetScaler must be deployed in Transparent mode.
D. The ADNS service must be configured with an IPv6 address.

**Correct Answer: C**
**Section:**

**QUESTION 17**
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 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 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 access to resources on the basis of priority.
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 desired 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 two security features should the architect configure to meet these requirements? (Choose two.)

A. Pattern sets
B. Rate limiting
C. HTTP DDOS
D. Data sets
E. APPQOE

**Correct Answer: B, E**
**Section:**

**QUESTION 18**
Scenario: The following NetScaler environment requirements were discussed during a design meeting between a Citrix Architect and the Workspacelab team:
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).
NetScaler should recognize Uniform Resource Identifier (URI) and close the session to NetScaler 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 method can the architect use to redirect the user accessing https://mail.citrix.com to 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**
**Section:**

**QUESTION 19**
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:
Two pairs of NetScaler MPX appliances will be deployed in the DMZ network and the internal network.
High availability will be accessible between the pair of NetScaler MPX appliances in the DMZ network.
Multi-factor authentication must be configured for the NetScaler Gateway virtual server.
The NetScaler Gateway virtual server is integrated with XenApp/XenDesktop environment.
Load balancing must be deployed for the users from the workspacelab.com and vendorlab.com domains.
The logon page must show the workspacelab logo.
Certificate verification must be performed to identify and extract the username.
The client certificate must have UserPrincipalName as a subject.
All the managed workstations for the workspace users must have a client identifications certificate installed on it.
The workspacelab users connecting from a managed workstation with a client certificate on it should be authenticated using LDAP.
The workspacelab users connecting from a workstation without a client certificate 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 NetScaler Gateway.
A domain drop down list must be provided if the user connects to the NetScaler Gateway virtual server externally.
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 assess 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: ???
      RHIstate: ???
      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**
**Section:**

**QUESTION 20**
A Citrix Architect needs to configure advanced features of NetScaler by using StyleBooks as a resource in the Heat service.
What is the correct sequence of tasks to be completed for configuring NetScaler using the Heat stack?

A. 1. Install NetScaler Bundle for OpenStack2. Deploy the Heat stack3. Register OpenStack with NMAS4. Add NetScaler instances (Optional)5. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource6. Create service packages (Add OpenStack tenants)
B. 1. Install NetScaler Bundle for OpenStack2. Register OpenStack with NMAS3. Add NetScaler instances (Optional)4. Create service packages (Add OpenStack tenants)5. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource6. Deploy the Heat stack
C. 1. Install NetScaler Bundle for OpenStack2. Add NetScaler instances (Optional)3. Create service packages (Add OpenStack tenants)4. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource5. Register OpenStack with NMAS6. Deploy the Heat stack
D. 1. Install NetScaler Bundle for OpenStack2. Prepare the HOT by using the NetScaler heat resources and NetScaler Network Resource3. Register OpenStack with NMAS4. Deploy the Heat stack5. Add NetScaler instances (Optional)6. Create service packages (Add OpenStack tenants)

**Correct Answer: D**
**Section:**

**QUESTION 21**
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: B**
**Section:**

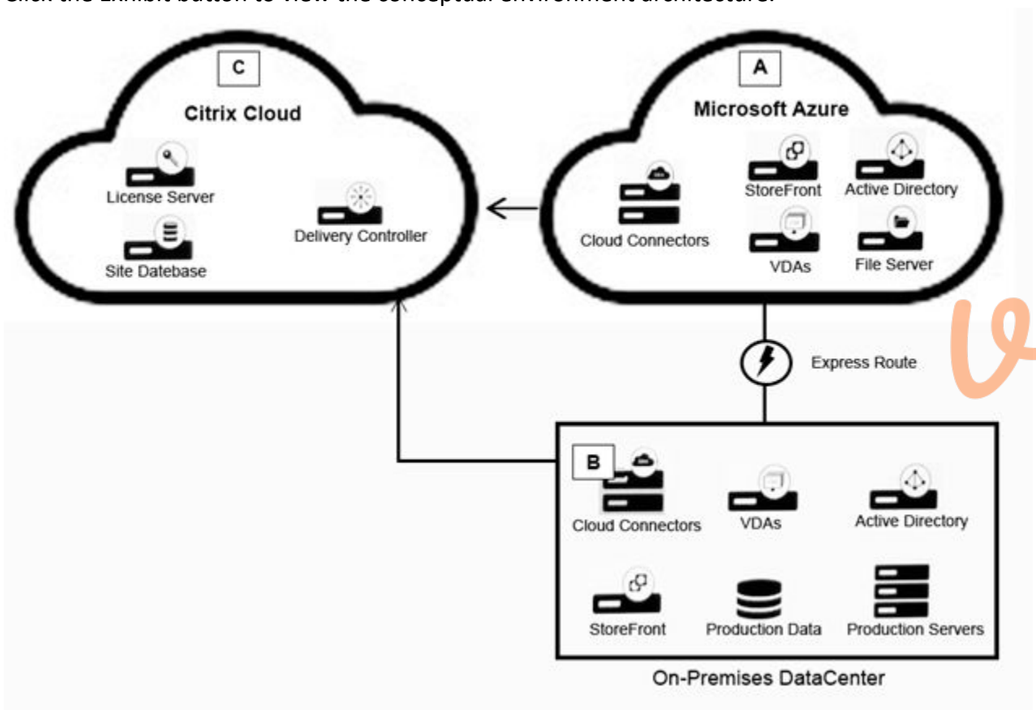
**QUESTION 22**
Scenario: More than 10,000 users will access a customer's environment. The current networking infrastructure is capable of supporting the entire workforce of users. However, the number of support staff is limited, and management needs to ensure that they are capable of supporting the 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

**Correct Answer: A**
**Section:**

**QUESTION 23**
Scenario: A Citrix Architect needs to design a hybrid XenApp and XenDesktop environment which will include as well as resource locations in an on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:
Active XenApp and XenDesktop Service subscription
No existing NetScaler deployment
Minimization of additional costs
All users should correct directly to the resource locations containing the servers which will host HDX sessions
Click the Exhibit button to view the conceptual environment architecture.




The architect should use_____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. No NetScaler products; NetScaler ICA Proxy (cloud-licensed)
B. NetScaler Gateway as a Service; NetScaler ICA Proxy (cloud-licensed)
C. NetScaler Gateway as a Service; no NetScaler products
D. No NetScaler products; NetScaler Gateway appliance
E. NetScaler gateway as a Service; NetScaler ADC (BYO)

**Correct Answer: C**
**Section:**

**QUESTION 24**
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: B, D**
**Section:**

**QUESTION 25**
Which session parameter does the default authorization setting control when authentication, authorization, and auditing profiles are configured?

A. Determines the default logging level
B. Determines whether the NetScaler appliance will allow or deny access to content for which there is no specific authorization policy
C. Determines the default period after which the user is automatically disconnected and must authenticate again to access the intranet
D. Determines whether the NetScaler appliance will log users onto all web applications automatically after they authenticate or will pass users to the web application logon page to authenticate for each application.
E. Controls are amount of time the users can be idle before they are automatically disconnected.

**Correct Answer: B**
**Section:**

**QUESTION 26**
Scenario: A Citrix Architect has deployed two MPX devices, 12.0.53.13 nc and MPX 11500 models, in 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 enabled the following features on the NetScaler devices. Content Switching, SSL Offloading, Load Balancing, NetScaler Gateway, Application Firewall in hybrid security and Appflow. All are enabled to send monitoring information to NMAS 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).
NetScaler should recognize Uniform Resource Identifier (URl) and close the session to NetScaler when users hit the Logoff button in Microsoft Outlook web access.
Users should be able to authenticate using either user principal name (UPN) or sAMAccountName.
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 monitor will meet these requirements?

A. add lb monitor mon_rpc HTTP-ECV --send ''GET /rpc/healthcheck.htm'' recv 200 -LRTM DISABLED
B. add lb monitor mon_rpc HTTP-ECV --send ''GET /rpc/healthcheck.htm'' recv 200 -LRTM ENABLED
C. add lb monitor mon_rpc HTTP --send ''GET /rpc/healthcheck.htm'' recv 200 -LRTM DISABLED --secure YES
D. add lb monitor mon_rpc HTTP-ECV --send ''GET/rpc/healthcheck.htm'' recv 200 -LRTM DISABLED --secure YES

**Correct Answer: D**
**Section:**

**QUESTION 27**
Which NetScaler Management and Analytics System (NMAS) utility can a Citrix Architect utilize to verify the configuration template created by the NMAS StyleBook, before actually executing it on the NetScaler?

A. Dry Run

B. configpack
C. NITRO API
D. configcheck

**Correct Answer: A**
**Section:**

**QUESTION 28**
Scenario: A Citrix Architect needs to design a new NetScaler Gateway deployment for a customer. During the design discussions, the architect learns that the customer would like to allow external RDP connections to internal Windows machines but does NOT want client drive redirection enabled on these connections.
Where should the architect enable the options to allow the customer to complete their requirement?

A. NetScaler Gateway global settings
B. RDP bookmark
C. Session policy
D. RDP server profile
E. Session profile
F. RDP client profile

**Correct Answer: F**
**Section:**

**QUESTION 29**
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

**Correct Answer: B, D**
**Section:**

**QUESTION 30**
Scenario: A Citrix Architect needs to design a new Citrix ADC 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 |
|---|---|
| Connections that should receive full VPN access | • User should be a member of the "Executives" group.<br>• Connections should be using the NetScaler Gateway Plugin.<br>• Connections can come from any IP address source. |

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. ICAProxy, stateless gateway

B. CVPN; single gateway
C. CVPN; stateless gateway
D. ICAProxy; single gateway

**Correct Answer: B**
**Section:**

**QUESTION 31**
Scenario: A Citrix Architect is asked by management at the Workslab organization to review their existing configuration and make the necessary upgrades. The architect recommends small changes to the pre-existing NetScaler configuration. Currently, the NetScaler MPX devices are configured in a high availability pair, and the outbound traffic is load-balanced between two Internet service providers 9ISPs). However, the failover is NOT happening correctly.
The following requirements were discussed during the design requirements phase:
The return traffic for a specific flow should be routed through the same path while using Link Load Balancing.
The link should fail over if the ISP router is up and intermediary devices to an ISP router are down.
Traffic going through one ISP router should fail over to the secondary ISP, and the traffic should NOT flow through both routers simultaneously.
What should the architect configure with Link Load balancing (LLB) to meet this requirement?

A. Net Profile
B. Mac-based forwarding option enabled.
C. Resilient deployment mode
D. Backup route

**Correct Answer: D**
**Section:**

**QUESTION 32**
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:
A pair of NetScaler MPX appliances will be deployed in the DMZ network.
High availability will be accessible on the NetScaler MPX in the DMZ Network.
Load balancing should be performed for the mail servers for Partnerlab and Vendorlab.
The traffic for both of the organizations must be isolated.
Separate Management accounts must be available for each client.
The load-balancing IP addresses must be identical.
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**
**Section:**

**QUESTION 33**
Which four load-balancing methods support Citrix ADC Virtual Server-Level Slow Start? (Choose four.)

A. URLHash
B. Least response time
C. Least Packets
D. Least Connection
E. LRTM
F. Least bandwidth
G. SRCIPSRCPORTHash

**Correct Answer: B, D, E, F**
**Section:**

**QUESTION 34**
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.<br>• The "Level2Support" group should have read-only access, except for enable/disable servers/services.<br>• The "NetScalerArchitect" user, which is part of the "NetScalerAdmins" group, should have full access.<br>• 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**
**Section:**

**QUESTION 35**
A Citrix Architect needs to define the architect and operational processes required to implement and maintain the production environment.
In which phase of the Citrix Methodology will the architect define this?

A. Define
B. Deploy
C. Assess
D. Review
E. Manage
F. Design

**Correct Answer: F**
**Section:**

**QUESTION 36**
Scenario: A Citrix Architect needs to configure a full VPN session profile to meet the following requirements:
Users should be able to send the traffic only for the allowed networks through the VPN tunnel.
Only the DNS requests ending with the configured DNS suffix workspacelab.com must be sent to NetScaler Gateway.
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: D**
**Section:**
**Explanation:**
https://support.citrix.com/article/CTX207149

**QUESTION 37**
Under which two circumstances will a service be taken out of the slow start phase with automated slow start? (Choose two.)

A. The service does NOT receive traffic for three successive increment intervals.
B. The server request rate parameters are set above 25 requests per second.
C. The actual request rate is slower than the new service request rate.
D. The percentage of traffic that the new service must receive is greater or equal to 50.

E. The request rate has been incremented 100 times.

**Correct Answer: A, C**
**Section:**

**QUESTION 38**
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

**Correct Answer: C**
**Section:**

**QUESTION 39**
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.
"SAML Assertion verification failed; Please contact your administrator."
The events in the /var/log/ns.log at the time of this issue are as follows:
Feb 23 20:35:21 <local0.err> 10.148.138.5 23/02/2018:20:35:21 GMT vorsbl 0-PPE-0 : default AAATM Message 3225369 0 "SAML: ParseAssertion: parsed attribute NameID, value is nameid"
Feb 23 20:35:21 <local0.err> 10.148.138.5 23/02/2018:20:35:21 GMT vorsbl 0-PPE-0 : default AAATM Message 3225370 0 "SAML verify digest: algorithms differ, expected SHA1 found SHA256"
Feb 23 20:35:44 <local0.err> 10.148.138.5 23/02/2018:20:35:44 GMT vorsbl 0-PPE-0 : default AAATM Message 3225373 0 "SAML: ParseAssertion: parsed attribute NameID, value is nameid"
Feb 23 20:35:44 <local0.err> 10.148.138.5 23/02/2018:20:35:44 GMT vorsbl 0-PPE-0 : default AAATM Message 3225374 0 "SAML verify digest: algorithms differ, expected SHA1 found SHA256"
Feb 23 20:37:55 <local0.err> 10.148.138.5 23/02/2018:20:37:55 GMT vorsbl 0-PPE-0 : default AAATM Message 3225378 0 "SAML: ParseAssertion: parsed attribute NameID, value is nameid"
Feb 23 20:37:55 <local0.err> 10.148.138.5 23/02/2018:20:37:55 GMT vorsbl 0-PPE-0 : default AAATM Message 3225379 0 "SAML verify digest: algorithms differ, expected SHA1 found SHA256"
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

**Correct Answer: C**
**Section:**

**QUESTION 40**
Scenario: A Citrix Architect has deployed Authentication for the SharePoint server through NetScaler. In order to ensure that users are able to edit or upload documents, the architect has configured persistent cookies on the NetScaler profile.
Which action should the architect take to ensure that cookies are shared between the browser and non-browser applications?

A. The time zone should be the same on the NetScaler, client, and SharePoint server.
B. The SharePoint load-balancing VIP FQDN and the AAA VIP FQDN should be in the trusted site of the client browser.
C. The Secure flag must be enabled on the cookie.
D. The cookie type should be HttpOnly.

**Correct Answer: B**
**Section:**

**QUESTION 41**
Scenario: A Citrix Architect needs to assess an existing NetScaler gateway deployment. During the assessment, the architect collects key requirements for different user groups, as well as the current session profile settings that are applied to those users.
Click the Exhibit button to view the information collected by the architect.

| Requirements |
| --- |
| • All users will access the environment using Citrix Receiver for Web.<br>• The Accountants group should ONLY have access to assigned desktops and applications in StoreFront.<br>• The Managers group should have access to assigned desktops and applications in StoreFront as well as internal web applications and file servers. |

**Configurations**

| Location | Type | Setting | Configuration |
| --- | --- | --- | --- |
| NetScaler gateway session policy (Gateway-Policy) | N/A | Policy expression | ns_true |
| NetScaler gateway session policy (Gateway-Policy) | N/A | Session profile | Gateway-Profile |
| NetScaler gateway session policy (Gateway-Profile) | Client Experience | Clientless Access | ON |
| NetScaler gateway session policy (Gateway-Profile) | Published Applications | ICA Proxy | ON |
| NetScaler gateway session policy (Gateway-Profile) | Published Applications | Web Interface Address | http://sf-vip.workspacelabs.net/Citrix/StoreWeb |
| StoreFront (Store) | Store Settings | Remote Access | No VPN tunnel |

Which configuration should the architect make to meet these requirements?

A. Change the Clientless Access settings in an existing session profile.
B. Change the remote Access settings in StoreFront.

C. Change ICA proxy settings in an existing session profile.
D. Change the policy expression in an existing session policy.
E. Create a new session profile and policy.

**Correct Answer: A**
**Section:**

**QUESTION 42**
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 |
| --- |
| • By default, no connection should have access to network resources unless authorized based on the other requirements.<br>• By default, only connections coming from the internal network (192.168.10.0/24) should be permitted to access the web server.<br>• The Accountants group is authorized to access URLs with a ".zip" extension; all other users must NOT be authorized for this.<br>• The Executives group is authorized to access the web server from inside OR outside the internal network. |

**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: D**
**Section:**

**QUESTION 43**
For which three reasons should a Citrix Architect perform a capabilities assessment when designing and deploying a new NetScaler in an existing environment? (Choose three.)

A. Understand the skill set of the company.
B. Assess and identify potential risks for the design and build phase.
C. Establish and prioritize the key drivers behind a project.
D. Determine operating systems and application usage.
E. Identify other planned projects and initiatives that must be integrated with the design and build phase.

**Correct Answer: A, B, E**
**Section:**

**QUESTION 44**
Which step does a Citrix Architect need to ensure during the Define phase when following the Citrix Methodology?

A. Testing steps were integrated.
B. The project manager agrees with road map timelines.
C. A phased roll out was completed.
D. Existing networking infrastructure is ready.
E. The redundancy deployment decision was made.

**Correct Answer: B**
**Section:**

**QUESTION 45**
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:
All three (3) Workspacelab sites (DC, NDR, and DR) will have similar NetScaler configuration and design.
Both external and internal NetScaler MPX appliances will have Global Server Load balancing (GSLB) configured and deployed in Active/Passive mode.
GSLB should resolve both A and AAA DNS queries.
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.
When the external NetScaler replies to DNS traffic coming in through Cisco Firepower IPS, the replies should be sent back through the same path.
On the internal NetScaler, both front-end VIP and back-end SNIP will be part of the same subnet.
USIP is configured on the DMZ NetScaler appliances.
The external NetScaler will act default gateway for back-end servers.
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: B**

**Section:**
**Explanation:**
https://support.citrix.com/article/CTX117346

**QUESTION 46**
Scenario: A Citrix Architect has sent the following request to the NetScaler:

```
HTTP Method
POST
URL
http://<netscaler-ip-address>/nitro/v1/config?clusterinstance
Requests Headers
Cookie:NITRO_AUTH_TOKEN=<tokenvalue>
Content-Type:application
Request Payload
{
  "clusterinstance":
  {
    "clid":1,
    "preemption":"ENABLED"
  }
}
```

Which response would indicate the successful execution of the NITRO command?

A. 302
B. 201
C. 202
D. 200

**Correct Answer: B**
**Section:**
**Explanation:**
https://developer-docs.citrix.com/projects/netscaler-nitro-api/en/12.0/usecases/

**QUESTION 47**
Scenario: A Citrix Architect has configured a load balancing virtual server for RADIUS authentication. The architect observes that, when the radius authentication action has the virtual server IP address, the authentication falls. However, when any of the individual server IP addresses are used, the authentication works fine.
How should the architect troubleshoot this issue?

A. Change the Logon name attribute in Radius Action
B. Ensure that TCP port 1821 is open from NSIP to backend Radius servers
C. Verify the shared secret on Citrix ADC
D. Change the Radius client from NSIP to SNIP on the Radius server

**Correct Answer: D**
**Section:**

**QUESTION 48**

Which three parameters must a Citrix Architect designate when creating a new session policy? (Choose three.)

A. Single Sign-on Domain
B. Request Profile
C. Name
D. Enable Persistent Cookie
E. Expression

**Correct Answer: B, C, E**
**Section:**

**QUESTION 49**
For which two reasons should a Citrix Architect perform a capabilities assessment when designing and deploying a new Citrix ADC in an existing environment? (Choose two.)

A. Determine operating system and application usage.
B. Identify other planned projects and initiatives that must be integrated with the design and build phase.
C. Determine the new environment networking requirements.
D. Establish and prioritize the key drivers behind a project.
E. Assess and identify potential risks for the design and build phase.

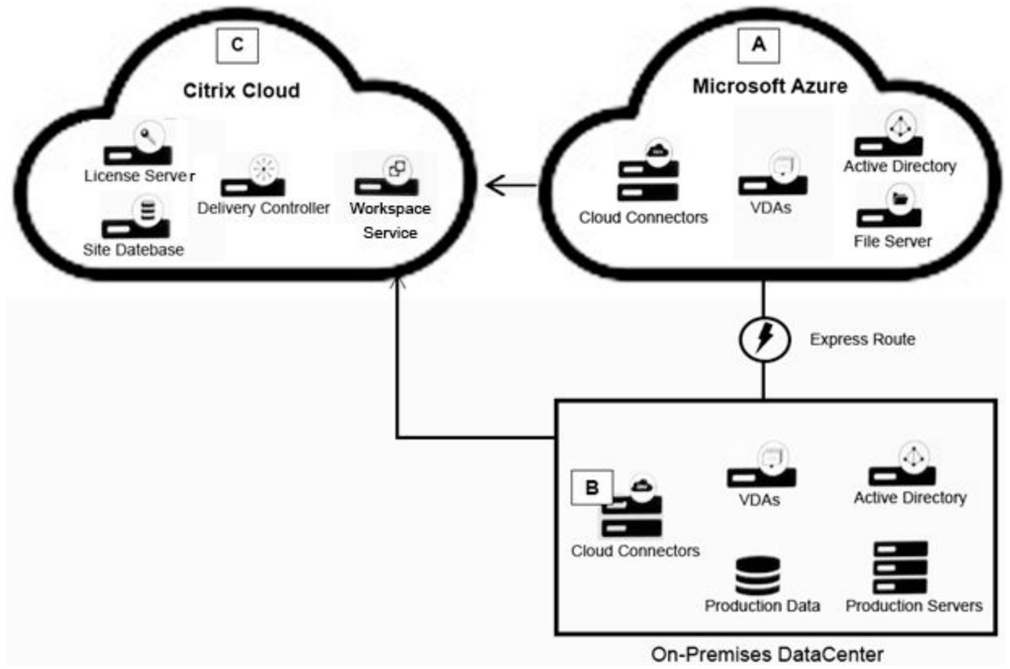
**Correct Answer: B, E**
**Section:**

**QUESTION 50**
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

**Correct Answer: B, C, F, G**
**Section:**

**QUESTION 51**
Scenario: A Citrix Architect needs to design a hybrid XenApp and XenApp and XenDesktop environment which will include Citrix Cloud as well as resource locations in on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:
Active XenApp and XenDesktop Service subscription
No existing Citrix deployment
About 3,000 remote users are expected to regularly access the environment
Multi-factor authentication should be used for all external connections
Solution must provide load balancing for backend application servers
Load-balancing services must be in Location B
Click the Exhibit button to view the conceptual environment architecture.




The architect should use _____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. Citrix Gateway as a Service, no Citrix products
B. No Citrix products, Citrix ADC (BYO)
C. Citrix Gateway as a Service, Citrix ADC (BYO)
D. No Citrix products, Citrix ICA Proxy (cloud-licensed)
E. Citrix Gateway as a Service, Citrix ICA Proxy (cloud-licensed)
F. No Citrix products; Citrix Gateway appliance

**Correct Answer: C**
**Section:**

**QUESTION 52**
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.
<a target='_blank' href='http://mail.citrix.com/'>Which Responder policy can be utilized to redirect the users from http://mail.citrix.com to https://mail.citrix.com/owa?</a>

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

**Correct Answer: A**
**Section:**

**QUESTION 53**
Which two options should a Citrix Architect evaluate during a capabilities assessment? (Choose two.)

A. Users and applications
B. Disaster recovery requirements
C. Network infrastructure
D. Conformance to the ISO model

**Correct Answer: A, C**
**Section:**

**QUESTION 54**
Which two types of database deployments are supported in Citrix Application Delivery Management? (Choose two.)

A. High Availability
B. Multiple Server
C. Single Server
D. Cluster instance
E. Cloud Services

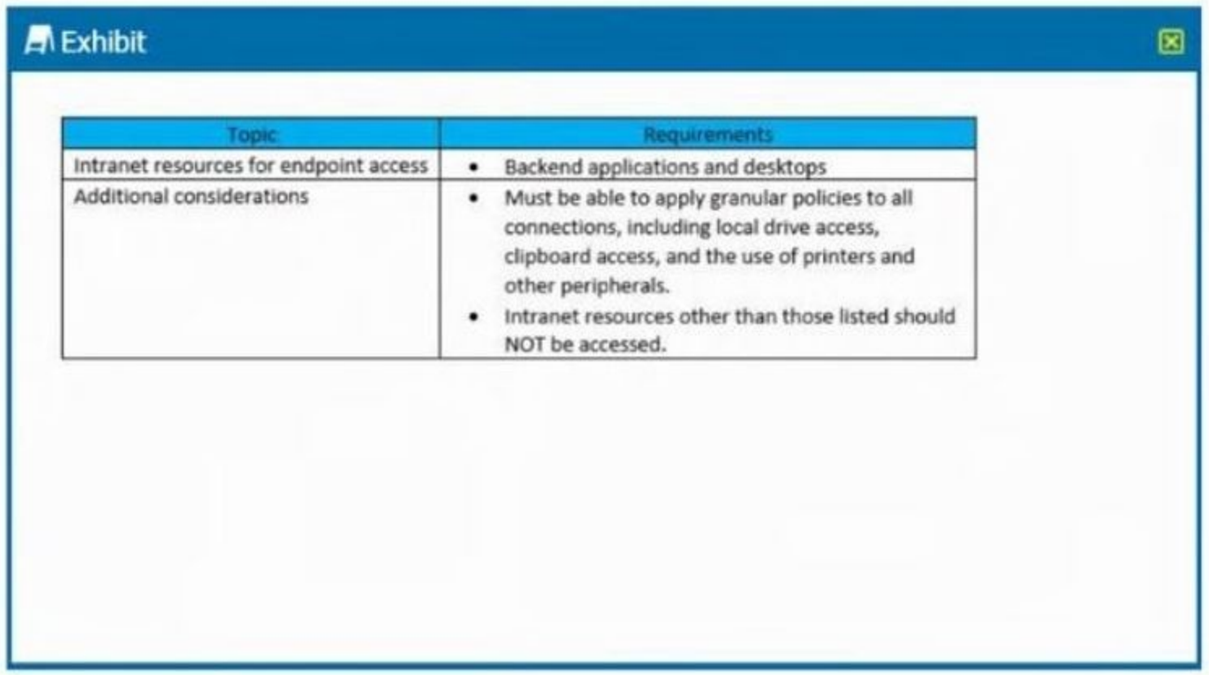
**Correct Answer: A, C**
**Section:**

**QUESTION 55**
Scenario: The Workspacelab team has configured their Citrix ADC Management and Analytics (Citrix Application Delivery Management) environment. A Citrix Architect needs to log on to the Citrix Application Delivery Management to check the settings.
Which two authentication methods are supported to meet this requirement? (Choose two.)

A. Certificate
B. RADIUS
C. TACACS
D. Director
E. SAML
F. AAA

**Correct Answer: B, C**
**Section:**

**QUESTION 56**
Scenario: A Citrix Architect needs to design a new Citrix Gateway deployment for a customer. During the design discussions, the architect documents the key requirements for the Citrix Gateway.




Click the Exhibit button to view the key requirements.
The architect should configure Citrix Gateway for _____in order to meet the stated requirements. (Choose the correct option to complete the sentence.)

A. ICA proxy
B. Client access
C. VPN access
D. ROP proxy

**Correct Answer: A**
**Section:**

**QUESTION 57**
Scenario: A Citrix Architect needs to deploy a Citrix ADC appliance for Workspacelab, which will provide application load balancing services to Partnerlab and Vendorlab.
The setup requirements are as follows:
A pair of Citrix ADC MPX appliances will be deployed in the DMZ network.
High availability will be accessible on the Citrix ADC MPX in the DMZ Network.
Load balancing should be performed for the mail servers for Partnerlab and Vendorlab.
The traffic for both of the organizations must be isolated.
Separate Management accounts must be available for each client.
The load-balancing IP addresses must be identical.
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: B**
**Section:**

**QUESTION 58**
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.
They captured the following requirements during the design discussion held for a Citrix ADC design project:
All three (3) Workspacelab sites (DC, NDR, and DR) will have similar Citrix ADC configurations and design.
Both external and internal Citrix ADC MPX appliances will have Global Server Load Balancing (GSLB) configured and deployed in Active/Passive mode.
GSLB should resolve both A and AAA DNS queries.
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.
When the external Citrix ADC replies to DNS traffic coming in through Cisco Firepower IPS, the replies should be sent back through the same path.
On the internal Citrix ADC, both the front-end VIP and backend SNIP will be part of the same subnet.
The external Citrix ADC will act as default gateway for the backend servers.
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 the design requirements above?

A. MAC-based Forwarding must be enabled on the External Citrix ADC Pair.
B. NSIP of the External Citrix ADC must be configured as the default gateway on the backend servers.
C. The Internal Citrix ADC must be deployed in Transparent mode.
D. The ADNS service must be configured with an IPv6 address.

**Correct Answer: A**
**Section:**

**QUESTION 59**
Scenario: A Citrix Architect observes the following configurations while performing an assessment of a Citrix ADC deployment:
Citrix Gateway virtual server nsg-dmz-001 is configured in ICA Proxy mode.
The authentication method used is Plaintext LDAP.
The session policies bound are configured to integrate with StoreFront in ICA proxy mode to perform Single Sign-on.
The connection to LDAP server is performed using SNIP by Citrix ADC.
To meet the new design requirement the architect needs to change the SNIP used for communication with LDAP servers.
Which AAA parameter must the architect verify to update the source IP address for the communication from Citrix ADC to the LDAP server?

A. AAA Session IP
B. NetProfile
C. aaadnatip
D. MappedIPAddress

**Correct Answer: C**
**Section:**

**QUESTION 60**
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

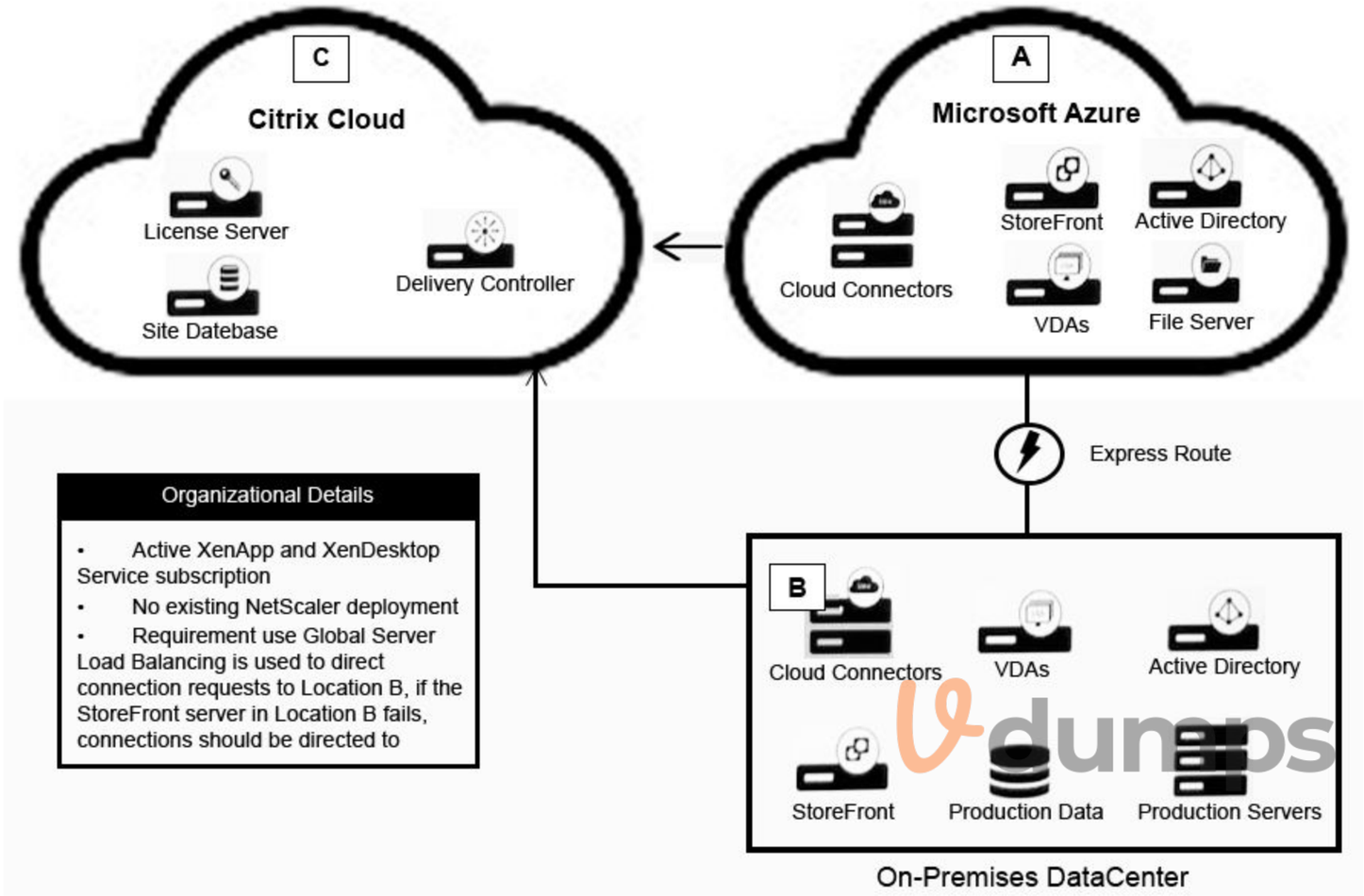
**Correct Answer: C, D**
**Section:**

**QUESTION 61**
Which three tasks can a Citrix Architect select and schedule using the Citrix ADC maintenance tasks? (Choose three.)

A. Convert Citrix Web App Firewall Policy Instances.
B. Upgrade Citrix ADC CPX Instances
C. Upgrade Citrix ADC Instances.
D. Convert a high availability pair of Instances to Cluster.
E. Convert cluster instances to a high availability pair.
F. Configure a high availability pair of Citrix ADC Instances.

**Correct Answer: B, D, F**
**Section:**

**QUESTION 62**
Scenario: A Citrix Architect needs to design a hybrid Citrix Virtual App and Citrix Virtual Desktop environment which will include Citrix Cloud as well as resource locations in an on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:
Active Citrix Virtual App and Citrix Virtual Desktops Service subscription
No existing NetScaler deployment
Global Server Load Balancing is used to direct connection requests to Location B, if the StoreFront server in Location B fails, connections should be directed to Location A.
Click the Exhibit button to view the conceptual environment architecture.




The architect should use _____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. Citrix ADC (BYO); Citrix gateway appliance
B. Citrix ADC (BYO); No Citrix products
C. Citrix ADC (BYO); Citrix ADC (BYO)
D. Citrix Gateway appliance; Citrix Gateway appliance
E. Citrix Gateway appliance; Citrix ADC (BYO)

**Correct Answer: E**
**Section:**

**QUESTION 63**
Scenario: A Citrix Architect needs to design a new Citrix ADC 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.

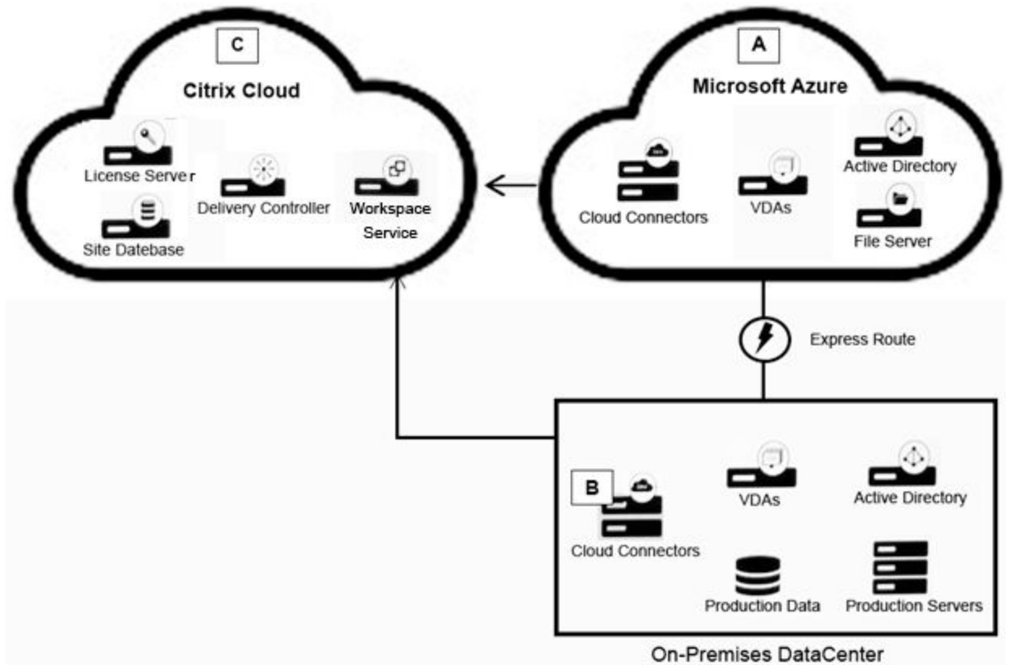
| Topic | Requirements |
|---|---|
| User experience | Once the user authenticates, they should be able to access bookmarks to authorized machines on the Gateway portal. When a bookmark is clicked, an RDP connection to the backend machine will be established. |
| Additional considerations | • A Secure Ticket Authority (STA) server should not be required for the deployment.<br>• Minimize the amount of configuration and maintenance required for the solution. |

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. ICAProxy, stateless gateway
B. CVPN; single gateway
C. CVPN; stateless gateway
D. ICAProxy; single gateway

**Correct Answer: B**
**Section:**

**QUESTION 64**
Scenario: A Citrix Architect needs to design a hybrid Citrix Virtual App and Citrix Virtual Desktop environment which will include Citrix Cloud as well as resource locations in on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:
Active Citrix Virtual App and Citrix Virtual Desktop Service subscription
No existing NetScaler deployment
About 3,000 remote users are expected to regularly access the environment
Multi-factor authentication should be used for all external connections
Solution must provide load balancing for backend application servers
Load-balancing services must be in Location B
Click the Exhibit button to view the conceptual environment architecture.

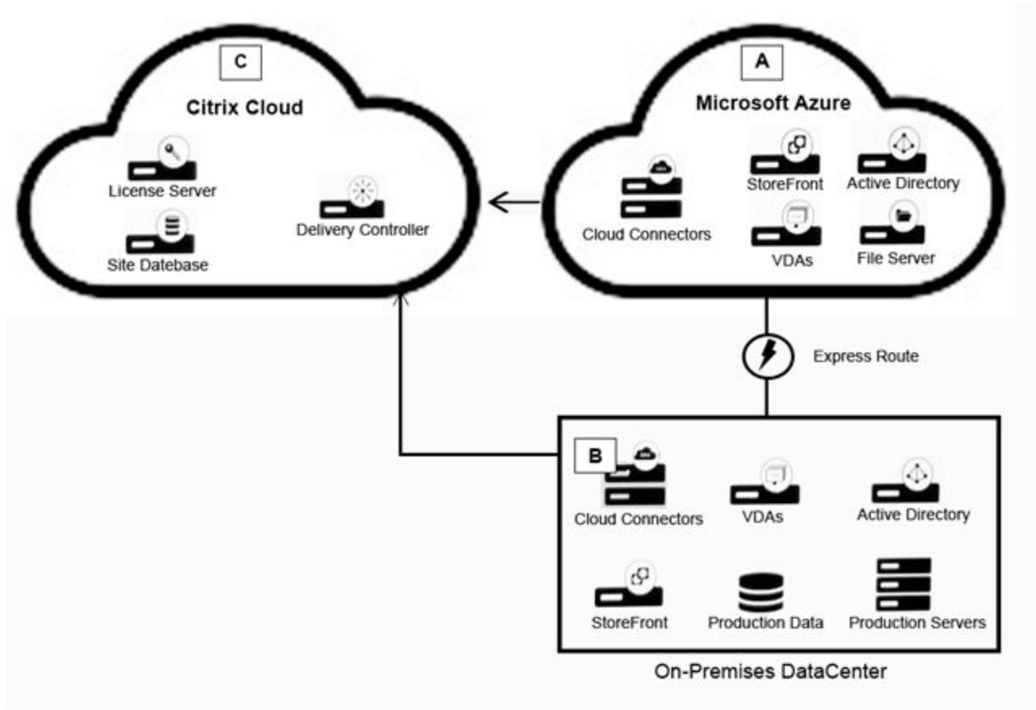



The architect should use _____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. Citrix Gateway as a Service, no Ctrix products
B. No Citrix products, Citrix ADC (BYO)
C. Citrix Gateway as a Service, Citrix ADC (BYO)
D. No Citrix products, Citrix ICA Proxy (cloud-licensed)
E. Citrix Gateway as a Service, Citrix ICA Proxy (cloud-licensed)
F. No Citrix products; Citrix Gateway appliance

**Correct Answer: C**
**Section:**

**QUESTION 65**
Scenario: A Citrix Architect needs to design a hybrid Citrix Virtual App and Citrix Virtual Desktop environment which will include as well as resource locations in an on-premises datacenter and Microsoft Azure.
Organizational details and requirements are as follows:
Active Citrix Virtual App and Citrix Virtual Desktop Service subscription
No existing Citrix deployment
Minimization of additional costs
All users should correct directly to the resource locations containing the servers which will host HDX sessions
Click the Exhibit button to view the conceptual environment architecture.




The architect should use_____ in Location A, and should use _____ in Location B. (Choose the correct option to complete the sentence.)

A. No Citrix products; Citrix ICA Proxy (cloud-licensed)
B. Citrix Gateway as a Service; Citrix ICA Proxy (cloud-licensed)
C. Citrix Gateway as a Service; no Citrix ADC products
D. No Citrix products; Citrix Gateway appliance
E. Citrix gateway as a Service; Citrix ADC (BYO)

**Correct Answer: C**
**Section:**

**QUESTION 66**
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

**Correct Answer: E**
**Section:**

**QUESTION 67**
Scenario: A Citrix Architect needs to conduct a capabilities assessment for an organization that wants to create a new Citrix ADC deployment. One of the organization's core business drivers is to ensure that key applications are always available to users.
Which capabilities must the architect verify to assess if the requirement is feasible with the current infrastructure?

A. Undocumented environment
B. issues image management processes
C. Disaster recovery and implementation
D. Training and certification of support staff and end users
E. Current Active Directory and DNS environment

**Correct Answer: C**
**Section:**

**QUESTION 68**
A Citrix Architect has deployed Citrix Application Delivery Management to monitor a high availability pair of Citrix ADC VPX devices.
The architect needs to deploy automated configuration backup to meet the following requirements:
The configuration backup file must be protected using a password.
The configuration backup must be performed each day at 8:00 AM GMT.
The configuration backup must also be performed if any changes are made in the ns.conf file.
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**
**Section:**

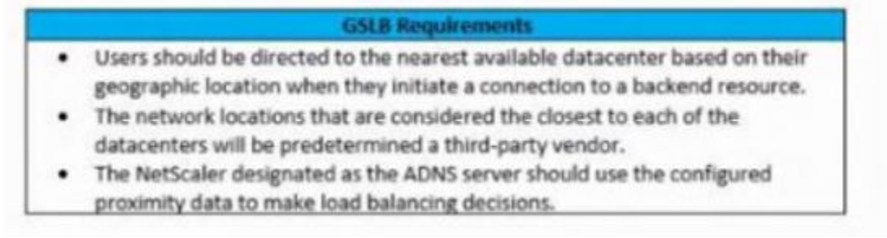
**QUESTION 69**
Scenario: The Workspacelab team has implemented a Citrix ADC high availability pair and Citrix ADC Management and Analytics (Citrix Application Delivery Management). The Citrix Application Delivery Management was configured by a Citrix Architect to monitor and manage these devices. The Workspacelab team wants to load balance their Microsoft SharePoint servers on the Citrix ADC and needs the process to be streamlined and administered using Citrix Application Delivery Management. The following requirements were discussed during the meeting.
* The Microsoft SharePoint server should be optimized. Load balanced, and secured in the network and should be deployed using Citrix Application Delivery Management.
* All the configurations should be verified before getting pushed to the Citrix Application Delivery Management.
What is a prerequisite for installing Microsoft SharePoint using Citrix Application Delivery Management?

A. Citrix ADC needs to have a platinum license Installed on it
B. Citrix Application Delivery Management should have a version higher than 12.0.53.13 nc
C. Citrix ADC MPX should be of 11500 series
D. Microsoft SharePoint version should be 2016

**Correct Answer: D**
**Section:**

**QUESTION 70**

Scenario: A Citrix Architect needs to design a new multi-datacenter Citrix ADC deployment. The customer wants Citrix ADC to provide access to various backend resources by using Global Server Load Balancing (GSLB) in an Active-Active deployment. Click the Exhibit button to view additional requirements identified by the architect.




Which GSLB algorithm or method should the architect use for the deployment based on the stated requirements?

A. Dynamic round trip time (RTT)
B. Least response time
C. Least packets
D. Source IP hash
E. Static proximity
F. Least connections

**Correct Answer: E**
**Section:**

**QUESTION 71**
Which session parameter does the default authorization setting control when authentication, authorization, and auditing profiles are configured?

A. Determines the default logging level
B. Determines whether the Citrix ADC appliance will allow or deny access to content for which there is no specific authorization policy
C. Determines the default period after which the user is automatically disconnected and must authenticate again to access the intranet
D. Determines whether the Citrix ADC appliance will log users onto all web applications automatically after they authenticate or will pass users to the web application logon page to authenticate for each application.
E. Controls are amount of time the users can be idle before they are automatically disconnected.
F. Determines whether the Citrix ADC appliance will use primary or the secondary authentication for SSO

**Correct Answer: B**
**Section:**

**QUESTION 72**
Scenario: A Citrix Architect needs to design a new Citrix Gateway deployment. During the design discussions, the architect documents the key requirements about when to provide VPN access for incoming connections to the Citrix Gateway virtual server. Click the Exhibit button to view the requirements.

Exhibit

| Topic | Requirements |
| --- | --- |
| Connections that should receive full VPN access | • User should be a member of the "Executives" group.<br>• Connections should be using the Citrix Gateway Plugin.<br>• Connections can come from any IP address source. |

Which policy expression will meet these requirements?

A. HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReciever"&&HTTP.REQ.USER.IS_MEMBER_OF("Executives")

B. CLIENT.IP.SRC.IN_SUBNET(192.168.1.0/24).NOT&&HTTP.REQ.HEADER("User-Agent".CONTAINS("CitrixReciever")&&HTTP.REQ.USER.IS_MEMBER_OF("Executives")

C. CLIENT.IP.SRC.IN_SUBNET(192.168.1.0/24).NOT&&HTTP.REQ.HEADER("User-Agent".CONTAINS("CitrixReciever").NOT&&HTTP.REQ.USER.IS_MEMBER_OF("Executives")

D. HTTP.REQ.USER.IS_MEMBER_OF("Executives")

E. !CLIENT.IP>SRC.IN_SUBNET(192.168.1.0/24)&&HTTP.REQ.USER.IS_MEMBER_OF("Executives")

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

**Correct Answer: A**
**Section:**

**QUESTION 73**
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. CPX; in high availability
B. SDX; in a highly availability pair

C. SDX; with less than 6 partitions
D. MPX; as back up cluster node

**Correct Answer: C**
**Section:**

**QUESTION 74**
Which two methods can a Citrix Architect use to create a Heat Orchestration template? (Choose two)

A. Direct Input
B. Configuration jobs
C. Citrix Web App Firewall Policies
D. File
E. Gateway Policies

**Correct Answer: A, D**
**Section:**

**QUESTION 75**
Which two parameters must a Citrix Architect specify in the configuration job to replicate a specific configuration snippet from one Crtnx ADC instance to multiple instances? (Choose two.)

A. Running Configuration
B. Target Instance
C. Saved Configuration
D. Source Instance
E. Configuration Source

**Correct Answer: A, E**
**Section:**

**QUESTION 76**
Scenario: A Citrix Architect holds a design discussion with a team of Workspacelab members, and they capture the following requirements for the Citrix ADC design project:
A pair of Citrlx ADC MPX appliances will be deployed in the DMZ network and another pair in the internal network.
High availability will be accessible between the pair of Citrix ADC MPX appliances in the DMZ network.
Multi-factor authentication must be configured for the Citrix Gateway virtual server.
The Citrix Gateway virtual server is integrated with the StoreFront server.
Load balancing must be configured for the StoreFront server. *Authentication must be deployed for users from the workspacelab.com domain.
The Workspacelab users should be authenticated using Cert Policy and LDAP.
All the client certificates must be SHA 256-signed, 2048 bits, and have UserPrincipalName as the subject.
Single Sign-on must be performed between StoreFront and Citrix 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

Exhibit 1 | Exhibit 2

```
add authentication ldapAction ldap-sam -serverName 192.168.10.11 -serverPort 636 -ldapBase "DC=workspacelab,DC=com" -ldapBind
Dn administrator@workspacelab.com -ldapBindDnPassword 54e394e320d69a5b3418746e4dc9e83ebf0a1c7ffd869abd3e040b42d38e4b2e -encry
pted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName memberOf -subAttributeName cn -secType SSL -ssoNam
eAttribute 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
```

Exhibit 1 | Exhibit 2

```
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.  Ex
pecting 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 expecte
d 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 authenticati
on(Bind) succeeded, now attempting to search the user hr1@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 r
eturned null, user hr1@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
: hr1@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 400
```

What is causing this issue?

A. IdapLoginName is set as sAMAccountName
B. UserNamefield is set as subjecticn
C. Password used is incorrect
D. User does NOT exist in database

**Correct Answer: B**
**Section:**

**QUESTION 77**

Scenario: A Citrix Architect needs to design a new solution within Microsoft Azure. The architect would like to create a highly available Citrix ADC VPX pair to provide load balancing for applications hosted in the Azure deployment which will receive traffic arriving from the Internet. In order to maximize its investment, the organization would like both Citrix ADC VPX instances to actively load-balance connection requests. Which two approaches are possible solutions for the architect to use to design the solution? (Choose two.)

A. Purchase two standalone Citrix ADC instances in the Microsoft Azure marketplace, then deploy them as a cluster.
B. Purchase two standalone Citrix ADC instances in the Microsoft Azure marketplace, deploy them, then use an external Azure load balancer to distribute client traffic across both instances.
C. Purchase a Citrix ADC HA Pair in the Microsoft Azure marketplace, then deploy them as an Active-Active GSLB configuration.
D. Purchase two standalone Citrix ADC instances in the Microsoft Azure marketplace, then deploy them as an Active-Passive high availability pair.
E. Purchase a Citrix ADC HA Pair in the Microsoft Azure marketplace, then deploy them as an Active-Passive high availability pair.

**Correct Answer: B, C**
**Section:**

**QUESTION 78**
Scenario: A Citrix Architect has configured two MPX devices in high availability mode with version 12.0.53.13 nc. After a discussion with the security team, the architect enabled the Application Firewall feature for additional protection.
In the initial deployment phase, the following security features were enabled:
IP address reputation
HTML SQL injection check
Start URL
HTML Cross-site scripting
Form-field consistency
After deployment in pre-production, the team identifies the following additional security features and changes as further requirements:
Application Firewall should retain the response of form field in its memory. When a client submits the form in the request, Application Firewall should check for inconsistencies in the request before sending it to the web server.
All the requests dropped by Application Firewall should get a pre-configured HTML error page with appropriate information.
The Application Firewall profile should be able to handle the data from the RSS feed and an ATOM-based site. Click the Exhibit button to view an excerpt of the existing configuration.


What should the architect do to meet these requirements?

A. Configure a new profile with web 2.0 and use the previously used Application Firewall security checks.
B. Configure a new HTML profile and use previously used Application Firewall security checks.
C. Configure a new profile with XML and use previously used Application Firewall security checks.
D. Modify an existing HTML profile and disable 'Drop invalid security check'

**Correct Answer: A**
**Section:**

**QUESTION 79**
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

**Correct Answer: A**
**Section:**

**QUESTION 80**

Which statement is applicable to Citrix Gateway split tunneling?

A. If you set split tunneling to reverse, the Citrix ADC Gateway plug-in sends only traffic destined for networks protected by Citrix ADC Gateway through the VPN tunnel. The Citrix ADC Gateway plug-in does NOT send network traffic destined for unprotected networks to Citrix ADC Gateway.
B. If you set split tunneling to reverse, the intranet applications define the network traffic that Citrix ADC Gateway does NOT intercept.
C. If you enable split tunneling, the intranet applications define the network traffic that Citrix ADC Gateway does NOT intercept.
D. If you enable split tunneling, the Citrix ADC Gateway plug-in captures all network traffic originating from a user device and sends the traffic through the VPN tunnel to Citrix ADC Gateway.
E. If you set split tunneling to reverse, the Citrix ADC Gateway plug-in captures all network traffic originating from a user device and sends the traffic through the VPN tunnel to Citrix ADC Gateway.

**Correct Answer: B**
**Section:**

**QUESTION 81**
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

**Correct Answer: E**
**Section:**

**QUESTION 82**
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: A, E**
**Section:**

**QUESTION 83**
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.<br>• The "Level2Support" group should have read-only access, except for enable/disable servers/services.<br>• The "NetScalerArchitect" user, which is part of the "NetScalerAdmins" group, should have full access.<br>• 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).* | 2 |
| Item 2 | Command Policy | "NetScaler Admins" group | DENY | .* | 1 |
| 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 | ^(?!clear ns config.*)(?!scp.*)(?!set ssl fips)(?!reset ssl fips)(?!diff ns config)(?!shell)(?!reboot)(?!batch)(?!s+\s+(?!system)(?!configstatus)(?!ns ns\.conf)(?!ns savedconfig)(?!ns runningConfig)(?!gslb runningConfig)(?!techsupport).* | 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

**Correct Answer: A**
**Section:**

**QUESTION 84**
Which four parameters can a Citrix Architect change after the initial creation of a session profile? (Choose four.)

A. Credential Index
B. Default Authorization Action
C. ICA Proxy Migration
D. Session Timeout
E. Expression
F. Name

G. Enable Persistent Cookie

**Correct Answer: A, B, D, G**
**Section:**

**QUESTION 85**
A Citrix Architect needs to evaluate and define the architecture and operational processes required to implement and maintain the production environment. In which two phases of the Citrix Methodology will the architect define this? (Choose two.)

A. Design
B. Define
C. Manage
D. Deploy
E. Assess

**Correct Answer: A, C**
**Section:**

**QUESTION 86**
Scenario: A Citrix Architect has implemented two high availability pairs of MPX 5500 and MPX 11500 devices respectively with 12.0.53.13 nc version. The Citrix ADC devices are set up to handle Citrix Gateway. Load Balancing. Application Firewall, and Content Switching. The Workspacelab infrastructure is set up to be monitored with Citrix Application Delivery Management version 12.0.53.13 nc by the Workspacelab administrators. The Workspacelab team wants to implement one more pair(s) of Citrix ADC MPX 7500 devices with version 12.0.53.13 nc.
The Citrix consulting team has assigned the task to implement these Citrix ADC devices in the infrastructure and set them up to be monitored and managed by Citrix ADC Management and Analytics {Citrix Application Delivery Management).
The following are the requirements that were discussed during the project initiation call:
Citrix Application Delivery Management should be configured to get the infrastructure information under sections such as HDX Insight, WEB Insight, and Security Insight.
Configuration on the new MPX devices should be identical to that of MPX 11500 devices.
Configuration changes after the deployment and initial setup should be optimized using Citrix Application Delivery Management.
Citrix Application Delivery Management should be utilized to configure templates that can be utilized by the Workspacelab team in future deployments.
As per the requirement from the Workspacelab team, Citrix Application Delivery Management should store the audited data for only 15 days.
However, the architect is NOT able to view any Information under Analytics. What should the architect do to fix this issue?

A. Use nsconfig from MPX 11500 devices and copy the same config to MPX 7500 devices.
B. Use Public Stylebooks and templates to configure the new MPX 11500 devices.
C. Use configuration jobs to replicate the entire configuration from MPX 11500 Instance to MPX 7500 devices.
D. Use Inbuilt Stylebooks and templates to configure the new MPX 11500 devices.

**Correct Answer: C**
**Section:**

**QUESTION 87**
Which three parameters must a Citrix Architect designate when creating a new session policy? (Choose three.)

A. Single Sign-on Domain
B. Request Profile
C. Name
D. Enable Persistent Cookie

E. Expression

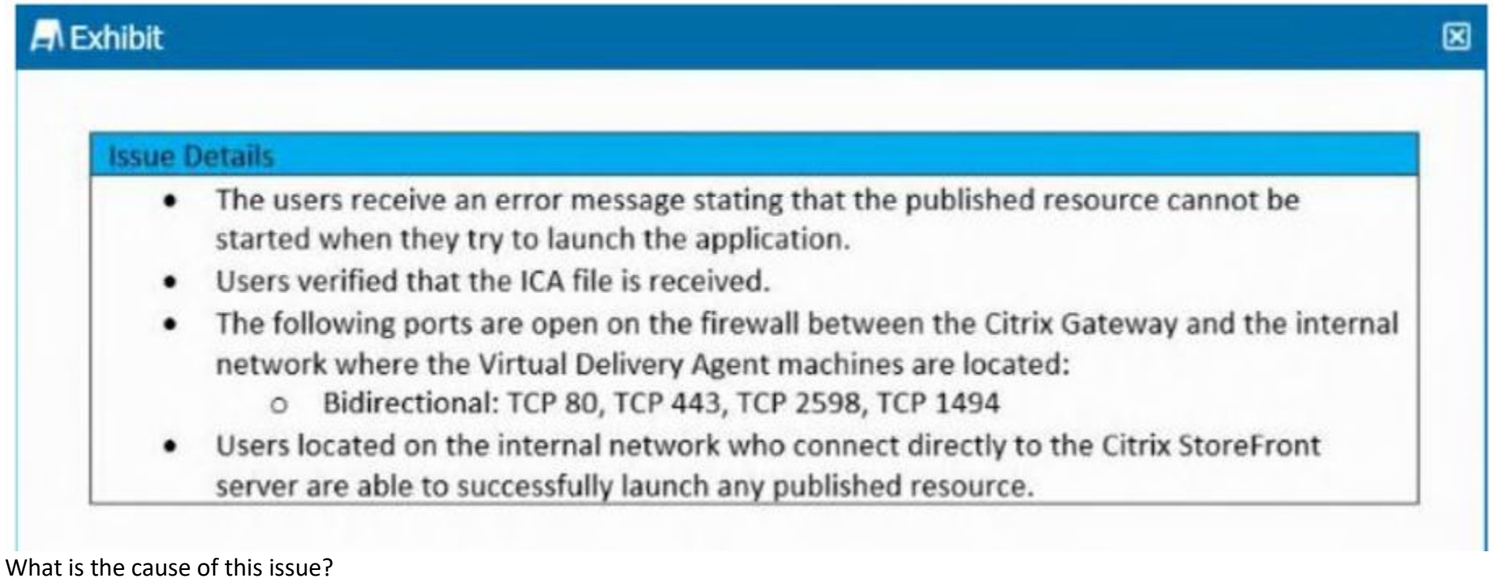
**Correct Answer: B, C, E**
**Section:**

**QUESTION 88**
Scenario: A junior Citrix Architect would like to use nFactor to perform authentication based on the domain. The junior architect has reached out to a supervisor for assistance and has been provided with the following step-by-step configuration guide:
Create Authentication policy for LDAP. RADIUS.
Create logon schema for Domain drop down. LDAP. LDAP+RADIUS, and noschema.
Create Authentication policy label for OnlyLDAR LDAP+RADIUS, and RADIUS.
Bind DOMAIN drop down as default logon schema policy
Create Authentication profile to bind the AAA virtual server.
Bind Authentication profile to Traffic management virtual server or Citrix Gateway virtual server.
What must the junior architect bind In order for the authentication to work correctly?

A. The authentication policy label to Citrix ADC AAA virtual server
B. The authentication policy label to the Citrix Gateway virtual server
C. The logon schema to the AAA virtual server
D. The logon schema to the Citrix ADC AAA virtual server
E. The authentication policy label to the Traffic management virtual server

**Correct Answer: A**
**Section:**

**QUESTION 89**
Scenario: A Citrix Architect needs to assess a Citrix Gateway deployment that was recently completed by a customer and is currently in pre-production testing. The Citrix Gateway needs to use ICA proxy to provide access to a Citrix Virtual Apps and Citrix Virtual Desktops environment. During the assessment, the customer informs the architect that users are NOT able to launch published resources using the Gateway virtual server.
Click the Exhibit button to view the troubleshooting details collected by the customer.




What is the cause of this issue?

A. There are NO backend Virtual Delivery Agent machines available to host the selected published resource.
B. The Secure Ticket Authority servers have NOT been configured in the Citrix Gateway settings.
C. The required ports have NOT been opened on the external firewall.
D. The StoreFront URL configured In the Citrix Gateway session profile is NOT correct.

**Correct Answer: B**
**Section:**

**QUESTION 90**
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 enabled 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 FITTP 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 either user principal name (UPN) or sAMAccountName.
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 monitor will meet these requirements?

A. add lb monitor mon.rpc HTTP-ECV -send 'GET /rpc/healthcheck.htm' recv 200 -LRTM DISABLED -secure YES
B. add lb monitor mon.rpc HTTP -send 'GET /rpc/healthcheck.htm' recv 200 -LRTM DISABLED -secure YES
C. add lb monitor mon.rpc HTTP-ECV -send 'GET /owa/healthcheck.htm' recv 200 -LRTM DISABLED
D. add lb monitor mon.rpc HTTP-ECV -send 'GET /owa/healthcheck.htm' recv 200 -LRTM ENABLED
E. add lb monitor mon.rpc HTTP-ECV -send 'GET /rpc/healthcheck.htm' recv 200 -LRTM ENABLED

**Correct Answer: A**
**Section:**

**QUESTION 91**
Scenario: The Workspacelab team has implemented Citrix ADC high availability pair and Citrix ADC Management and Analytics System (Citrix Application Delivery Management). The Citrix Application Delivery Management was configured by a Citrix Architect to monitor and manage these devices. The Workspacelab team wants to load balance their Microsoft SharePoint servers on the Citrix ADC and needs the process to be streamlined and administered using Citrix Application Delivery Management.
The following requirements were discussed during the meeting:
The Microsoft SharePoint server should be optimized, load balanced, and secured in the network and should be deployed using Citrix Application Delivery Management.
All the configurations should be yenned before getting pushed to the Citrix Application Delivery Management.
Which feature should the architect use to configure the Microsoft SharePoint server using Citrix Application Delivery Management?

A. StyleBooks
B. Orchestration
C. Configuration
D. Jobs Analytics

**Correct Answer: A**
**Section:**

**QUESTION 92**

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:
Multi-factor authentication must be configured for the Citrix Gateway virtual server.
The Citrix Gateway virtual server is integrated with the Citrix Virtual Apps and Desktops environment.
Load balancing must be configured for the StoreFront server.
Authentication must be deployed for the users from the workspacelab.com and vendorlab.com domains.
The logon page must have the workspacelab logo on it.
Certificate verification must be performed to identify and extract the username.
The client certificate must have UserPrincipalName as a subject.
All the managed workstations for the workspacelab users must have the client identification certificate installed on them.
The workspacelab users connecting from the internal 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.
The domain of the user connecting externally must be identified using the domain selected from the domain drop down list.
Which authentication policy must the architect execute first to meet the design requirements?

A. SAML
B. Cert
C. RADIUS
D. LDAP UPN

**Correct Answer: C**
**Section:**

**QUESTION 93**
Which three session settings are valid once a Citrix Architect has configured session settings to customize user sessions? (Choose three.)

A. Single Sign-on Domain
B. Credential Index
C. KCD Profile
D. Default Authentication Group
E. Single Sign-on to Web Applications
F. Session Idle Time

**Correct Answer: A, E, F**
**Section:**
**Explanation:**
Short But Comprehensive Explanation: The three session settings that are valid once a Citrix Architect has configured session settings to customize user sessions are:
Single Sign-on Domain: This setting specifies the domain name that is used for single sign-on authentication. This setting is required if the user account is in a different domain than the server running the published application1.
Single Sign-on to Web Applications: This setting enables or disables single sign-on to web applications that use basic, digest, or NTLM authentication. This setting requires the Citrix Secure Access client to be installed on the user device2.
Session Idle Time: This setting specifies the maximum time in minutes that a user session can remain idle before NetScaler Gateway disconnects the session. This setting helps to conserve server resources and prevent unauthorized access to inactive sessions3.
The other session settings are not valid for customizing user sessions. They are:
Credential Index: This setting specifies the index of the authentication server that is used to obtain the user credentials for single sign-on. This setting is not applicable for session policies, but only for authentication policies4.

KCD Profile: This setting specifies the name of the Kerberos constrained delegation profile that is used to delegate user credentials to back-end servers. This setting is not applicable for session policies, but only for traffic policies5.
Default Authentication Group: This setting specifies the name of the default group that is used to authorize users who do not belong to any group on the authentication server. This setting is not applicable for session policies, but only for authorization policies6.
Configure NetScaler Gateway session policies for StoreFront
Configuring Single Sign-on to Web Applications
Manage user sessions
[Configuring Credential Index]
[Configuring Kerberos Constrained Delegation]
[Configuring Default Authorization Groups]

**QUESTION 94**
Scenario: A Citrix Architect needs to configure a Content Switching virtual server to provide access to www.workspacelab.com. However, the architect observes that whenever the user tries to access www.worksapcelab.com/CITRIX/WEB, the user receives a '503 - Service Unavailable' response. The configuration snippet is as follows:

```
add cs vserver Vserver HTTP 10.107.149.246 80 -cltTimeout 180
add cs action Act1 -targetLBVserver Vserver1
add cs policy Pol1 -rule "http.REQ.URL.PATH_AND_QUERY.contains(\"citrix\")" -action Act1
add cs action Act2 -targetLBVserver Vserver2
add cs policy Pol2 -rule "http.REQ.URL.PATH_AND_QUERY.contains(\"admin\")" -action Act2
add cs action Act3 -targetLBVserver Vserver3
add cs policy Pol3 -rule "http.REQ.URL.PATH_AND_QUERY.startswith(\"web\")" -action Act3
bind cs vserver Vserver -policyName Pol1 -priority 100
bind cs vserver Vserver -policyName Pol2 -priority 110
bind cs vserver Vserver -policyName Pol3 -priority 120
```

What should the architect modify to resolve this issue?

A. add cs policy Pol3 -rule 'http.REQ.URL.containsC'WEB')' -action Act3
B. add cs policy Pol3 -rule 'http.REQ.URLcontainsf'citrix')' -action Act3
C. set cs vserver Vserver -caseSensitive ON
D. add cs policy Pol3 -rule 'http.REQ.URLPATH_AND_QUERY.con

**Correct Answer: D**
**Section:**

**QUESTION 95**
Which two settings should a Citrix Architect use on Citrix Application Delivery Management for configuring CPX using a pre-existing CPX device? (Choose two.)

A. Event Manager
B. instance
C. File
D. Plug and Play
E. Action

**Correct Answer: B, C**
**Section:**

**QUESTION 96**
Under which two circumstances will a service be taken out of the slow start phase with automated slow start? (Choose Two)

A. The Service is receiving more than 480 requests per second
B. The new service request rate is slower than the actual request rate
C. The Service does not receive traffic for four successive increment intervals
D. The request rate has been incremented 200 times
E. The percentage of traffic that the new service must receive is greater than or equal to 100.

**Correct Answer: D, E**
**Section:**

**QUESTION 97**
Scenario: A Citrix Architect has deployed an authentication setup for the load balancing virtual server for the SAP application. The authentication is being performed using RADIUS and LDAP. RADIUS is the first factor, and LDAP is the second factor in the authentication. The Single Sign-on with SAP application should be performed using LDAP credentials. Which session profile should be used to perform the Single Sign-on?

A. add tm sessionAction prof -sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON -ssoCredential PRIMARY -httpOnlyCookie NO
B. add vpn sessionAction prof-sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON -ssoCredential SECONDARY -httpOnlyCookie NO
C. add vpn sessionAction prof -sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON -ssoCredential PRIMARY -httpOnlyCookie NO
D. add tm sessionAction prof -sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON -ssoCredential SECONDARY -httpOnlyCookie NO

**Correct Answer: D**
**Section:**

**QUESTION 98**
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.

**Correct Answer: B, C, E**
**Section:**

**QUESTION 99**
Scenario: A Citrix Architect needs to deploy Single Sign-on form-based authentication through Citrix ADC for Outlook Web Access (OWA) 2013 for the users of the domain workspacelab com The Single Sign-on (SSO) must be performed based on sAMAccountName.
Which SSO action can the architect use to meet this requirement?

A. add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL '/owa' -userField username -passwdField password -ssoSuccessRule 'http RES SET_COOKIE COOKIE(V,cadata\M).VALUE(\Mcadata\').LENGTH.GT(70)M -responsesize 15000000 -submrtMethod POST
B. add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL '/owa/auth.owa' -userField user -passwdField password -ssoSuccessRule 'http RES SET_COOKIE COOKIEC'cadataV) VALUE(\'cadata\').LENGTH.GT(70)' -responsesize 15000000 -submrtMethod GET
C. add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL '/owa/owa.aspx' -userField usemame -passwdField password -ssoSuccessRule 'http RES SET_COOKIE COOKIE(\'cadata\') VALUE(\ncadata\') LENGTH.GT(70)' -responsesize 150 -submrtMethod POST

D. add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL '/owa/auth owa' -userField usemame -passwdField password -ssoSuccessRule 'http RES SET_COOKIE COOKIE(V'cadataV,)VALUE(V,cadata\') LENGTH GT(70)M -responsesize 15000000 -submrtMethod POST

**Correct Answer: D**
**Section:**
**Explanation:**
add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL '/owa/auth.owa' -userField username -passwdField password -ssoSuccessRule 'http.RES.SET_COOKIE.COOKIE(\'cadata\').VALUE(\'cadata\').LENGTH.GT(70' -responsesize 15000 -submitMethod POST

**QUESTION 100**
Scenario: A Citrix Architect captured the following requirements during a design discussion held for a Citrix ADC design project.
There will be a pair of Citrix ADC MPX appliances deployed in the DMZ and another pair deployed in the internal network
High availability will be accessible for each Citrix ADC MPX appliance in both the DMZ (external) and LAN (internal) networks
DMZ Citrix ADC MPX appliances will have GSLB configured and deployed in Active/Passive mode
Load balancing for the internal Microsoft Exchange servers will be configured on the internal Citrix ADC appliances
Load balancing for SAP application servers in the DMZ will be configured on the DMZ Citrix ADC appliances
For the DMZ Citrix ADC MPX pair, the data and management traffic will be sent over the same interface.
The DMZ Citrix ADC MPX pair will have three interfaces available.
The users from the DMZ should NOT have access to servers in the internal zone
Which deployment mode should the architect use to deploy the Citrix ADC pair in the DMZ?

A. One-Arm Mode
B. Two-Arm Mode
C. Hybrid Mode
D. Transparent Mode

**Correct Answer: A**
**Section:**

**QUESTION 101**
Scenario: A Citrix Architect has executed the following commands on the Citrix ADC:
In which scenario will the timeout work as configured?

A. If a session is non-idle, then the client browser will send an HTTP Response in which the URL will contain UA!=
B. If a session is non-idle, then the client browser will send an HTTP Request in which the URL will contain UA=0'
C. If a session is idle, then the client browser will keep on sending HTTP Requests in which URL will contain UA=0
D. If a session is idle, then the client browser will keep on sending HTTP Responses in which URL will contain UA!=

**Correct Answer: B**
**Section:**

**QUESTION 102**
What are three potential risks when examining the disaster recovery plan and implementation for a company? (Choose three)

A. Supporting infrastructure for proposed environment is NOT included in disaster recovery implementation
B. A disaster recovery plan exists but has never been tested
C. A disaster recovery location does NOT exist.
D. Users require mobile devices with continuous access

E. Optimal Gateway Routing decisions are NOT understood

**Correct Answer: A, B, C**
**Section:**

**QUESTION 103**
Scenario: A Citrix Architect has set up Citrix ADC 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 Citrix ADC security implementation project with the customers security team:
The Citrix ADC 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 Citrix ADC 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 access to resources on the basis of priority
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 desired 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. Configure Application Firewall with HTML cross-site scripting to block unwanted traffic
B. Configure pattern sets using regular expressions to block attacks
C. Configure Signatures manually and apply them to the Application Firewall profile
D. Configure signatures to auto-update and apply them to the Application Firewall profile
E. Configure IP address reputation and use IPREP and webroot to block the traffic

**Correct Answer: A**
**Section:**

**QUESTION 104**
Scenario: A Citrix Architect needs to assess a Citrix Gateway deployment that was recently completed by a customer and is currently in pre-production testing The Citrix Gateway needs to use ICA proxy to provide access to a Citrix Virtual Apps and Citrix Virtual Desktops environment. During the assessment, the customer informs the architect that users are NOT able to launch published resources using the Gateway virtual server.
Click the Exhibit button to view the troubleshooting details collected by the customer.

| Issue Details |
| --- |
| • Users launching any published resource through a Citrix Gateway connection receive an ICA file but are NOT able to establish an HDX connection with the Virtual Delivery Agent machine.<br>• Instead, users receive an error message stating that the published resource cannot be started.<br>• The following ports are open on the firewall between the Citrix Gateway and the internal network where the Virtual Delivery Agent machines are located:<br>  ○ Bidirectional: TCP 80, TCP 443<br>• Users on the internal network connecting directly to the StoreFront are able to successfully launch any published resource. |

Which two reasons could cause this issue? (Choose two)

A. The StoreFront URL configured in the Citrix Gateway session profile is NOT correct.
B. The required ports have NOT been opened on the firewall between the Citrix Gateway and the Virtual Delivery Agent machines
C. There are no backend Virtual Delivery Agent (VDA) machines available to host the selected published resource
D. The Secure Ticket Authority (STA) servers have NOT been configured in the Citrix Gateway settings
E. The two-factor authentication is NOT configured on the Citrix Gateway

**Correct Answer: B, D**
**Section:**

**QUESTION 105**
Scenario: A Citrix Architect needs to design a new solution within Amazon Web Services (AWS) The architect would like to create a high availability Citrix ADC VPX pair to provide load balancing for applications hosted in the AWS deployment within a single availability zone which will receive traffic arriving from the Internet.
Which configuration should the architect choose to accomplish this?

A. Two standalone Citrix ADC instances in the AWS marketplace, then deploy them as a cluster in the AWS management console
B. A Citrix ADC AWS-VPX Cluster using a Citrix CloudFormation template in the AWS marketplace, then deploy it to create an Active-Passive high availability pair
C. Two standalone Citrix ADC instances in the AWS marketplace, then deploy them as an Active-Passive high availability pair in the AWS management console
D. Two standalone Citrix ADC instances in the AWS marketplace, deploy them in the AWS management console, then use an AWS Elastic Load Balancing load balancer to distribute client traffic across both instances
E. Two Single AMI Citrix CloudFormation templates in the AWS marketplace then configure a high availability pair

**Correct Answer: C**
**Section:**

**QUESTION 106**
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.
They captured the following requirements during the design discussion held for a Citrix ADC design project:
All three (3) Workspacelab sites (DC NDR and DR) will have similar Citrix ADC configurations and design

Both external and internal Citrix ADC MPX appliances will have Global Server Load Balancing (GSLB) configured and deployed in Active/Passive mode
GSLB should resolve both A and AAA DNS queries.
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
When the external Citrix ADC replies to DNS traffic coming in through Cisco Firepower IPS the replies should be sent back through the same path
On the internal Citrix ADC. both front-end VIP and back-end SNIP will be part of the same subnet
USIP is configured on the DMZ Citrix ADC appliances
The external Citrix ADC will act as default gateway for back-end servers.
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. Mac Based Routing must be configured on the External Citrix ADC
B. Interface 0/1 must be used for DNS traffic
C. The SNIP of the external Citrix ADC must be configured as default gateway on the back-end servers
D. ADNS service must be used with IPv6 address
E. The SNIP of the internal Citrix ADC must be configured as the default gateway on the back-end servers.

**Correct Answer: E**
**Section:**

**QUESTION 107**
Scenario: A Citrix Architect needs to assess a Citrix Gateway deployment that was recently completed by a customer and is currently in pre-production testing. The Citrix Gateway needs to use ICA proxy to provide access to a Citrix Virtual Apps and Citrix Virtual Desktops environment. During the assessment, the customer informs the architect that users are NOT able to launch published resources using the Gateway virtual server.
Click the Exhibit button to view the troubleshooting details collected by the customer.

| Issue Details |
| --- |
| • External users trying to launch a Shared Hosted Desktop via a NetScaler gateway connection receive an ICA file from StoreFront.<br>• However, they are unable to launch the Shared Hosted Desktop.<br>• The following ports are open on the firewall between the NetScaler gateway and the internal network where the Virtual Delivery Agent machines are located:<br>Bidirectional: TCP 80, TCP 443, TCP 2598, TCP 1494<br>• Users located on the internal network who connect directly to the StoreFront server are able to launch the Shared Hosted Desktop. |

What is the cause of this issue?

A. The Secure Ticket Authority (STA) servers are load balanced on the Citrix ADC.
B. The required ports have NOT been opened on the firewall between the Citrix Gateway and the Virtual Delivery Agent (VDA) machines
C. The StoreFront URL configured in the Citrix Gateway session profile is incorrect
D. The Citrix License Server is NOT reachable

**Correct Answer: A**
**Section:**

**QUESTION 108**
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?

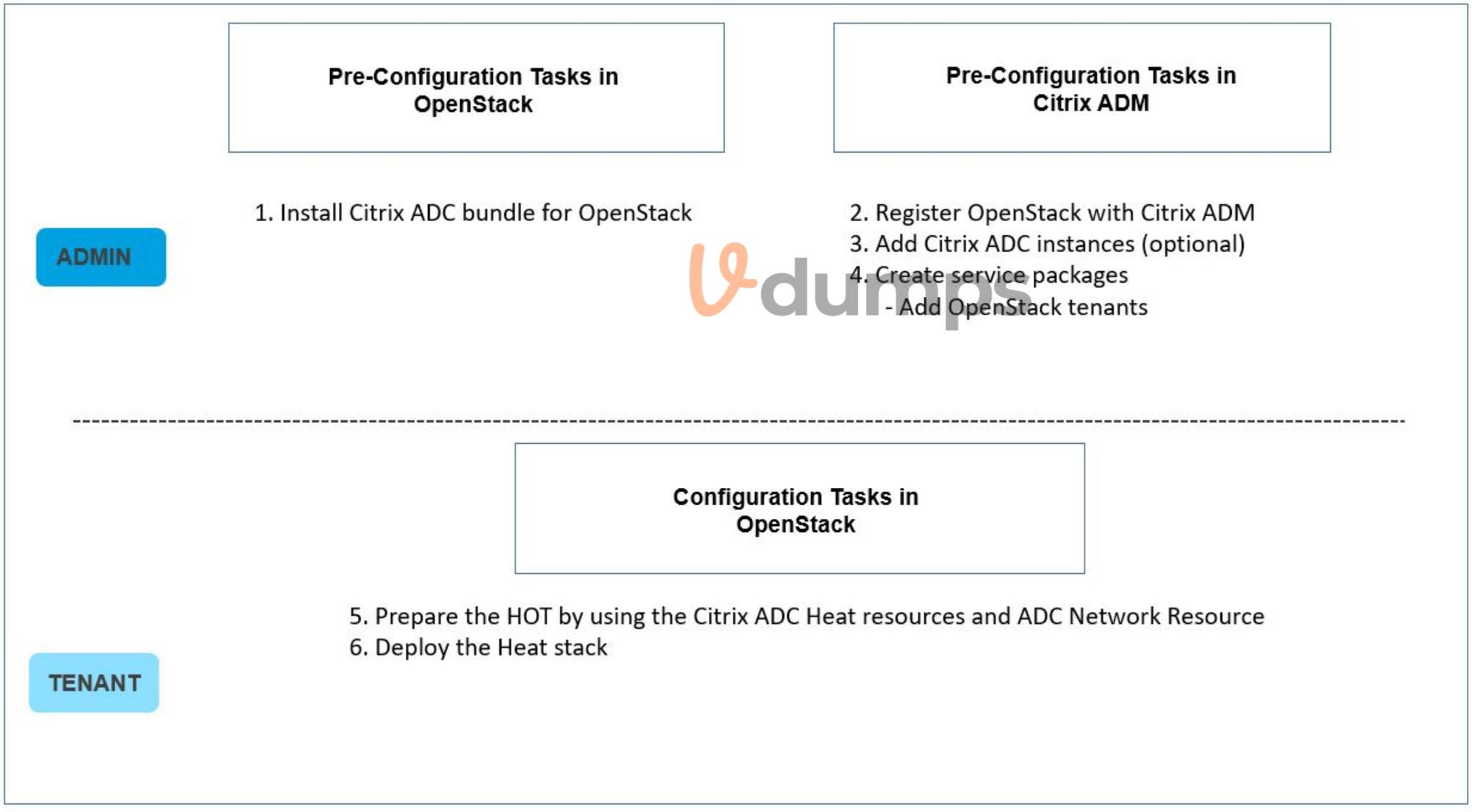
A. 1. Install Citrix ADC Bundle for OpenStack 2 Register OpenStack with Citrix Application Delivery Management 3. Add Citrix ADC instances (Optional) 4. Create service packages (Add OpenStack tenants) 5. Prepare the HOT by using the Citrix ADC Heat resources and Citrix ADC Network Resource 6. Deploy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

**Correct Answer: A**
**Section:**
**Explanation:**




**QUESTION 109**

Scenario: A Citrix Architect has configured two MPX devices in high availability mode with version 12.0.53.13 nc. After a discussion with the security team, the architect enabled the Application Firewall feature for additional protection.
In the initial deployment phase, the following security features were enabled:
IP address reputation
HTML SQL injection check
Start URL
HTML Cross-site scripting
Form-field consistency
After deployment in pre-production, the team identifies the following additional security features and changes as further requirements:
Application Firewall should retain the response of form field in its memory When a client submits the form in the next request. Application Firewall should check for inconsistency in the request before sending it to the web server
All the requests dropped by Application Firewall should receive a pre-configured HTML error page with appropriate information.
The Application Firewall profile should be able to handle the data from the RSS feed and an ATOM-based site.
Click the Exhibit button to view an excerpt of the existing configuration.

```
root@ns_vpx_01# Feb 20 09:02:43 <local0.info> 192.168.10.101 02/20/2018:09:02:43 GMT ns_vpx_01 0-PPE-0 : default SNMP TRAP_SENT 633 0 :  netScalerConfigChange (nsUserName = "nsroot", configurationCmd = "add appfw profile Appfirewall_340
-defaults basic", authorizationStatus = authorized, commandExecutionStatus = successful, nsClientIPAddr = 192.168.10.10, nsPartitionName = default)
-bash: syntax error near unexpected token `('
root@ns_vpx_01# Feb 20 09:02:43 <local0.info> 192.168.10.101 02/20/2018:09:02:43 GMT ns_vpx_01 0-PPE-0 : default GUI CMD_EXECUTED 634 0 :  User nsroot - Remote_ip 192.168.10.10 - Command "set appfw profile Appfirewall-340 -startURLAction
 block log stats -contentTypeAction none -inspectContentTypes "application/x-www-form-urlencoded" "multipart/form-data" "text/x-gwt-rpc" -startURLClosure OFF -denyURLAction block log stats -RefererHeaderCheck OFF -cookieConsistencyAction
 none -cookieTransforms OFF -cookieEncryption none -cookieProxying none -addCookieFlags none -fieldConsistencyAction none -CSRFtagAction none -crossSiteScriptingAction block log stats -crossSiteScriptingTransformUnsafeHTML OFF -crossSite
ScriptingCheckCompleteURLs OFF -SQLInjectionAction block log stats -SQLInjectionTransformSpecialChars OFF -SQLInjectionType SQLSplCharANDKeyword -SQLInjectionCheckSQLWildChars OFF -fieldFormatAction block log stats -defaultFieldFormatMin
Length 0 -defaultFieldFormatMaxLength 65535 -bufferOverflo" - Status "Success"
```

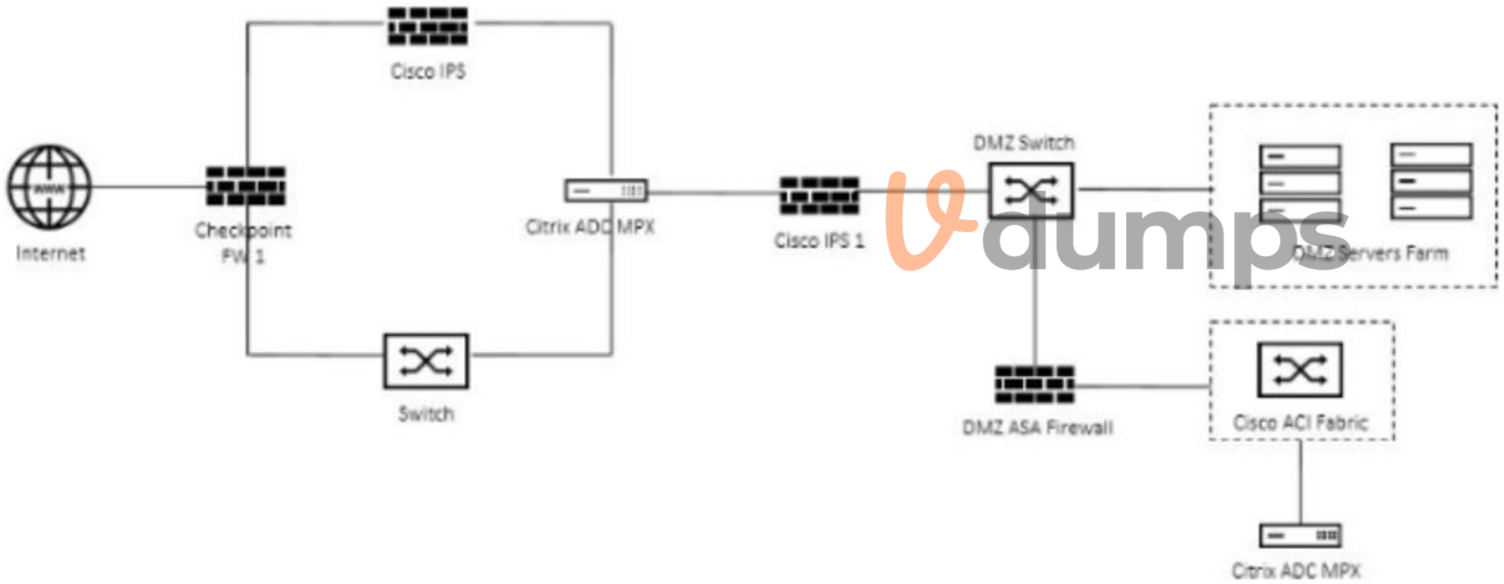
What should the architect do to meet these requirements?

A. Delete the existing profile and create a new profile of type: XML Application (SOAP)
B. Modify the existing profile to include sessionization
C. Create a new basic profile and use pre-existing HTML settings.
D. Modify existing profile settings, change HTML settings, and ensure to exclude uploaded files from security checks.

**Correct Answer: B**
**Section:**

**QUESTION 110**
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. NDR. and DR) will have similar Citrix ADC configurations and design.
The external Citrix ADC MPX 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 and the firewall policy prerequisites provided by the architect. On which two firewalls should the architect configure the policies? (Choose two.)

| Sr# | Port | Source | Destination | Notes |
|---|---|---|---|---|
| 1. | TCP 443 | NetScaler SNIP | SF1_IP<br>SF2_IP<br>SF3_IP | StoreFront |
| 2. | TCP 443 | NetScaler SNIP | XDC1_IP<br>XDC2_IP<br>XDC3_IP | STA<br>(Delivery Controller) |
| 3. | TCP 1494<br>TCP 2598 | NetScaler SNIP | VDA and Controllers subnets | ICA traffic |
| 4. | TCP 443<br>TCP 80 | Internet | NetScaler Gateway VIP | External access -<br>Port 80 will redirect the user to 443 |




A. CISCO IPS
B. CISCO IPS 1
C. DMZ ASA Firewall
D. Checkpoint FW1

**Correct Answer: C, D**
**Section:**

**QUESTION 111**
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
D. Create shadow accounts for the users of the Workspacelab domain in the Vendorlab domain

**Correct Answer: B**
**Section:**