1Y0-440.30q

Number: 1Y0-440
Passing Score: 800
Time Limit: 120 min

1Y0-440

Architecting a Citrix Networking Solution

Exam A

QUESTION 1
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: (none)
Explanation

Explanation/Reference:
QUESTION 2
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: (none)
Explanation

Explanation/Reference:
Reference: https://www.citrix.com/blogs/2012/03/30/desktop-transformation-high-level-project-plan/

QUESTION 3
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: (none)
Explanation

Explanation/Reference:

QUESTION 4
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: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.citrix.com/en-us/netscaler-mas/12/authentication-and-rbac/configuring.html

QUESTION 5
Scenario: A Citrix Architect has configured NetScaler Gateway integration with a XenApp environment to provide access to users from two domains: vendorlab.com and workslab.com. The Authentication method used is LDAP.

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

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

Correct Answer: BD
Section: (none)
Explanation

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

QUESTION 6
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: (none)
Explanation

Explanation/Reference:

QUESTION 7
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: (none)
Explanation

Explanation/Reference:

QUESTION 8

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 NetScaler 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: (none)
Explanation

Explanation/Reference:

QUESTION 9
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: BE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.citrix.com/en-us/citrix-adc/12-1/appexpert/appqoe.html https://docs.citrix.com/en-us/citrix-adc/12-1/appexpert/rate-limiting.html

QUESTION 10
A Citrix Architect needs to make sure that maximum concurrent AAA user sessions are limited to 4000 as a security restriction.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.carlstalhood.com/category/netscaler/netscaler-11-1/netscaler-gateway-11-1/

QUESTION 11
Which encoding type can a Citrix Architect use to encode the StyleBook content, when importing the StyleBook configuration under source attribute?

A. Hex
B. base64

C. URL
D. Unicode

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.citrix.com/en-us/netscaler-mas/12/stylebooks/how-to-use-api-to-create-configuration-from-stylebooks/import-custom-stylebooks.html

QUESTION 12
Scenario: A Citrix Architect needs to assess an existing on-premises NetScaler deployment which includes Advanced Endpoint Analysis scans. During a previous security audit, the team discovered that certain endpoint devices were able to perform unauthorized actions despite NOT meeting pre-established criteria.

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

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

Requirements

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

Configurations

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

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

A. Item 6
B. Item 7
C. Item 1
D. Item 3
E. Item 5
F. Item 2
G. Item 4

Correct Answer: F
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
_____ content type supports sending NITRO commands to NetScaler. (Choose the correct option to complete sentence.)

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
Scenario: A Citrix Architect has met with a team of Workspacelab members for a design discussion. They have captured the following requirements for NetScaler design project:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Which parameter must a Citrix Architect configure to ensure that HDX Proxy Connection terminates upon AAA Session TimeOut?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.citrix.com/content/dam/citrix/en_us/citrix-developer/documents/Netscaler/how-do-i-ica-session-timeout-with-aaa.pdf

QUESTION 16
Scenario: A Citrix Architect needs to design a new multi-datacenter NetScaler deployment. The customer wants NetScaler 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.

GSLB Requirements
• Users should be directed to the nearest available datacenter when they initiate a connection to a backend resource. • The nearest datacenter should be determined by the least Time to First Byte (TTFB) among all the available services, as evidenced by response code 200. • Services with fewer active connections should also be prioritized.

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. Static proximity
D. least connection
E. Least packets
F. Source IP hash

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.citrix.com/en-us/netscaler/12/global-server-load-balancing/methods/configuring-algorithm-based-methods.html

QUESTION 17
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 connect to internal resources, including intranet web pages, StoreFront, and the Microsoft Outlook Web App. • Users should be presented with two logon options: NetScaler Gateway Plugin and StoreFront. • Once connected, all outbound network traffic from the client device should pass through the NetScaler Gateway.

Configurations

Name	Type	Setting	Configuration
Item 1	Network Configuration	Home Page	NOT configured
Item 2	Client Experience	URL for Web-based email	NOT configured
Item 3	Client Experience	Split Tunnel	OFF
Item 4	Client Experience	Client Choices	Enabled
Item 5	Published Applications	ICA Proxy	OFF

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

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 18
Scenario: A Citrix Architect needs to deploy a load balancing for an application server on the NetScaler. The authentication must be performed on the NetScaler. After the authentication, the Single Sign-on with the application servers must be performed using Kerberos impersonation.

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

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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which request can a Citrix Architect utilize to create a NITRO API command to add a NetScaler appliance with NSIP address 10.102.29.60 to the cluster?

```
HTTP Method POST
URL: http://<netscaler-ip-address>/nitro/v1/config/clustermode
Request Headers
Cookie: NITRO_AUTH_TOKEN=<tokenvalue>
Content-Type: application/json
Request Payload
{
   "clusternode":
   {
     "nodeid".1,
     "ipaddress"."10.102.29.60",
     "state"."ACTIVE",
     "backplane"."1/1/2"
   }
}
HTTP Method PUT
URL: http://<netscaler-ip-address>/nitro/v1/config/clustermode
Request Headers
Content-Type: text/yaml
Request Payload
{
   "clusternode":
   {
     "nodeid".1,
     "ipaddress"."10.102.29.60",
     "state"."ACTIVE",
     "backplane"."1/1/2"
   }
}
```

A.

B.

```
HTTP Method POST
URL: http://<netscaler-ip-address>/nitro/v1/config/clustermode
Request Headers
Content-Type: application/text
Request Payload
{
   "clusternode":
   {
     "nodeid".1,
     "ipaddress"."10.102.29.60",
     "state"."ACTIVE",
     "backplane"."1/1/2"
   }
}
```

```
HTTP Method PUT
URL: http://<netscaler-ip-address>/nitro/v1/config/clustermode
Request Headers
Cookie NITRO_AUTH_TOKEN=<tokenvalue>
Content-Type: application/json
Request Payload
{
   "clusternode":
   {
     "nodeid".1,
     "ipaddress"."10.102.29.60",
     "state"."ACTIVE",
     "backplane"."1/1/2"
   }
}
```

C.

D.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://developer-docs.citrix.com/projects/netscaler-nitro-api/en/12.0/usecases/

QUESTION 20
Scenario: A Citrix Architect needs to design a new NetScaler Gateway deployment to provide secure RDP access to backend Windows machines.

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

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

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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: (none)
Explanation

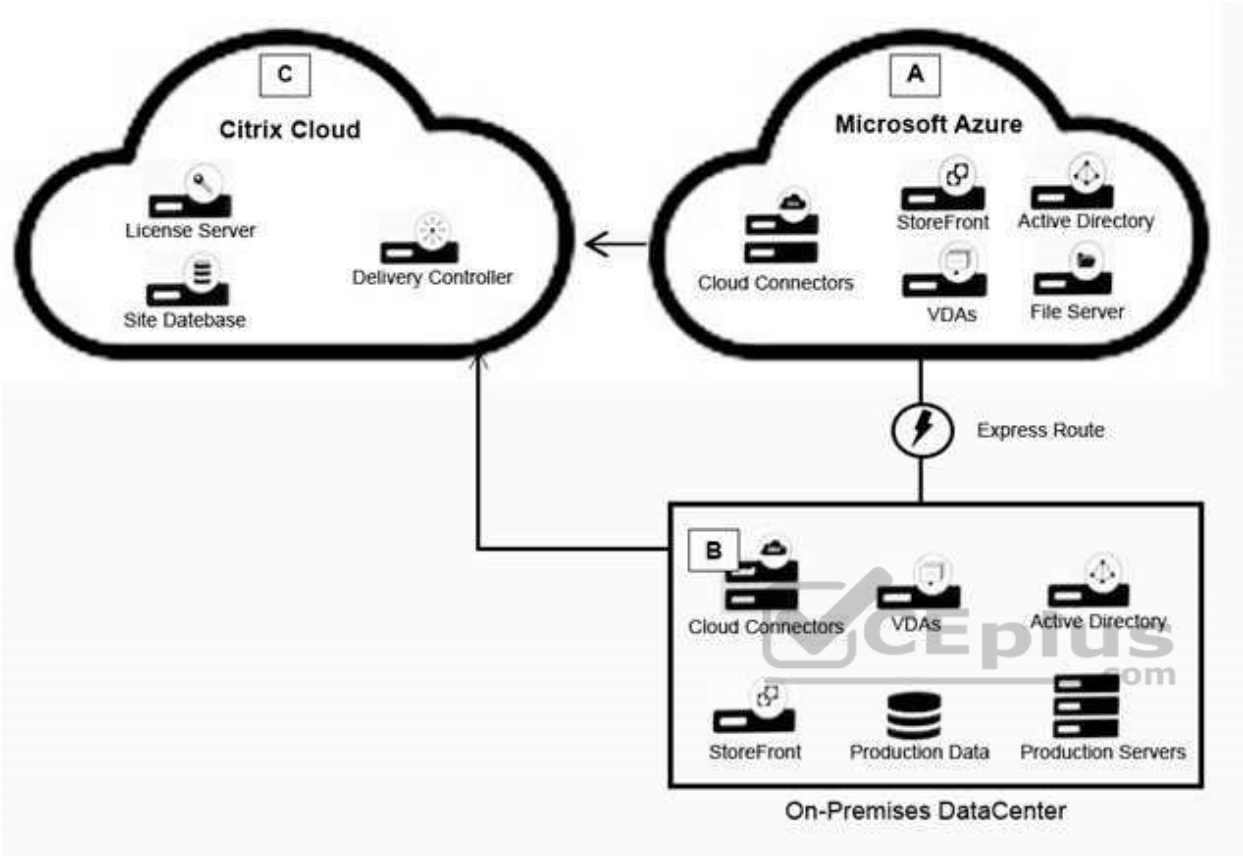
Explanation/Reference:

QUESTION 22
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: (none)
Explanation
Explanation/Reference:

QUESTION 23
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: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 (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 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: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Which four load-balancing methods support NetScaler Virtual Server-Level Slow Start? (Choose four.)

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

Correct Answer: BCDF
Section: (none)
Explanation

Explanation/Reference:
Reference: https://support.citrix.com/article/CTX108886

QUESTION 26
Scenario: A Citrix Architect needs to assess an existing NetScaler configuration. The customer recently found that members of certain administrator groups were receiving permissions on the production NetScaler appliances that do NOT align with the designed security requirements.

Click the Exhibit button to view the configured command policies for the production NetScaler deployment.

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

Configurations

Name	Type	Bind Point	Action	Commands Spec	Priority
Item 1	Command Policy	"NetScaler Admins" group	ALLOW	^(?!shell)(?!sftp)(?!scp) (?!batch) (?!source) (?!.*superuser) (?!.*nsroot) (?!show\s+system\s+(user | cmdPolicy))(?!(set | add | rm | create | export | kill) \s+system) (?!unbind | bind)\s+system\s+(user | group)) (?!diff\s+ns\s+ns\s+config) (?!\S+\s+ns\s+partition).*	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	"NetScalerArchitect"	ALLOW	.*	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: (none)
Explanation

Explanation/Reference:

QUESTION 27
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: (none)
Explanation

Explanation/Reference:
Reference: https://www.slideshare.net/davidmcg/designing-your-xenapp-75-environment

QUESTION 28
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: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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 vorsb1 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 vorsb1 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 vorsb1 0-PPE-0 : default AAATM Message 3225373 0 : “SAML : ParseAssertion: parsed attribute NameID, value is named
Feb 23 20:35:44 <local0.err> 10.148.138.5 23/02/2018:20:35:44 GMT vorsb1 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 vorsb1 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 vorsb1 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: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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: (none)
Explanation

Explanation/Reference:
Reference: https://support.citrix.com/article/CTX209054