1Y0-440 Dumps PDF New [2024 Ultimate Study Guide [Q89-Q111

1Y0-440 Dumps PDF New [2024] Ultimate Study Guide
1Y0-440 Exam Dumps PDF Updated Dump from ValidExam Guaranteed Success

Citrix 1Y0-440 certification exam is designed to validate the skills and knowledge required for a Citrix Networking Solution Architect. 1Y0-440 exam focuses on evaluating the ability to design and implement complex Citrix networking solutions that meet the requirements of businesses. It is ideal for individuals who want to demonstrate their expertise in designing Citrix networking solutions and want to advance their careers in this field.

QUESTION 89

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 customer s 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, TOP, and DNS based requests.

* needs to protect backend servers from overloading.

* needs to queue all the incoming requests 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 spammersThackers. 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 predetermined 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 implement to meet these requirements?
* Configure HTML SQL injection check on Application Firewall and enable Transform SQL special characters.
* Configure signatures manually and apply them to the Application Firewall profile.
* Configure HTML SQL Injection check on Application Firewall and enable Block SQLSplCharANDKeyword.
* Configure HTML cross-Site scripting and enable Check Request headers.

QUESTION 90

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.

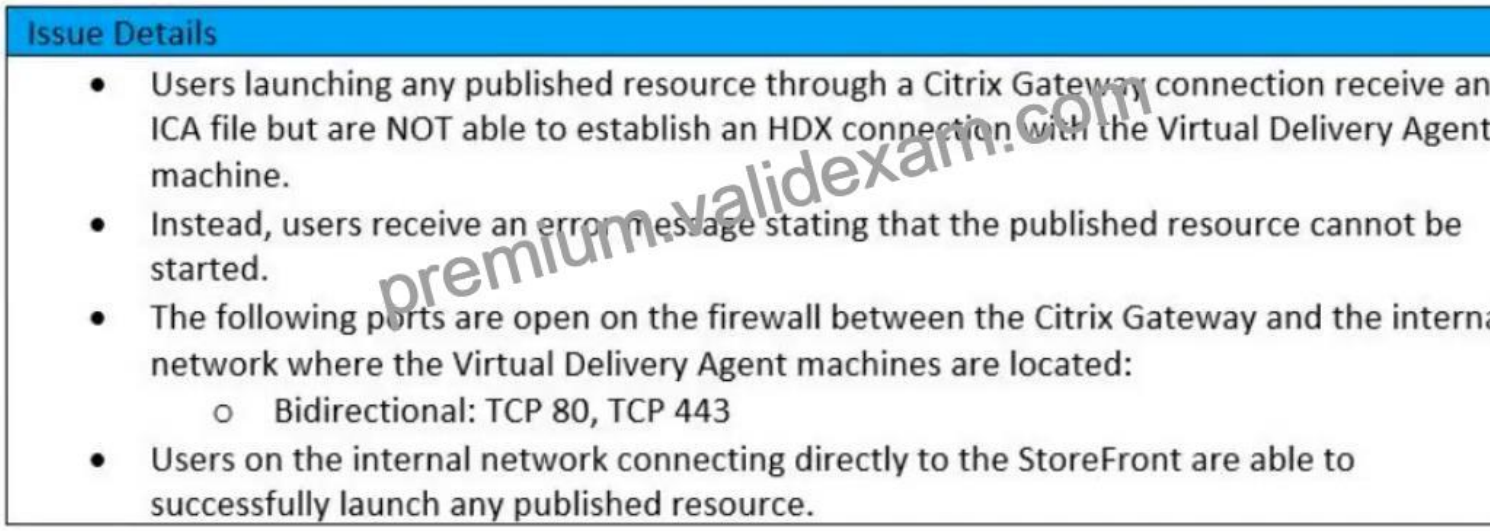
The users from the DMZ should NOT have access to servers in the internal zone Which deployment mode should the architect use to deploy the Citrix ADC pair in the DMZ?
* One-Arm Mode
* Two-Arm Mode
* Hybrid Mode
* Transparent Mode

QUESTION 91

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.



Which two reasons could cause this issue? (Choose two)
* The StoreFront URL configured in the Citrix Gateway session profile is NOT correct.
* The required ports have NOT been opened on the firewall between the Citrix Gateway and the Virtual Delivery Agent machines
* There are no backend Virtual Delivery Agent (VDA) machines available to host the selected published resource
* The Secure Ticket Authority (STA) servers have NOT been configured in the Citrix Gateway settings
* The two-factor authentication is NOT configured on the Citrix Gateway

QUESTION 92

A Citrix Architect can execute a configuration job using a DeployMasterConfiguration template on a NetScaler_____deployed_____. (Choose the correct option to complete sentence.)
* CPX; as part of a high availability pair
* CPX; as a stand alone device
* SDX; with less than 6 partitions and dedicated management interface
* MPX; as part of the cluster but Cluster IP is NOT configured
* SDX; with no partitions as a stand alone device

QUESTION 93

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.)
* Certificate
* RADIUS
* TACACS
* Director

* SAML
* AAA

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

QUESTION 94

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

* ICA connections
* Total Connected Users
* Active user session
* Maximum User session

QUESTION 95

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

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

* Item 6
* Item 7
* Item 1
* Item 3
* Item 5
* Item 2
* Item 4

QUESTION 96

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.
- By default, only connections coming from the internal network (192.168.10.0/24) should be permitted to access the web server.
- The Accountants group is authorized to access URLs with a ".zip" extension; all other users must NOT be authorized for this.
- 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?

* Item 1
* Item 3
* Item 4
* Item 5
* Item 2

Explanation/Reference:

QUESTION 97

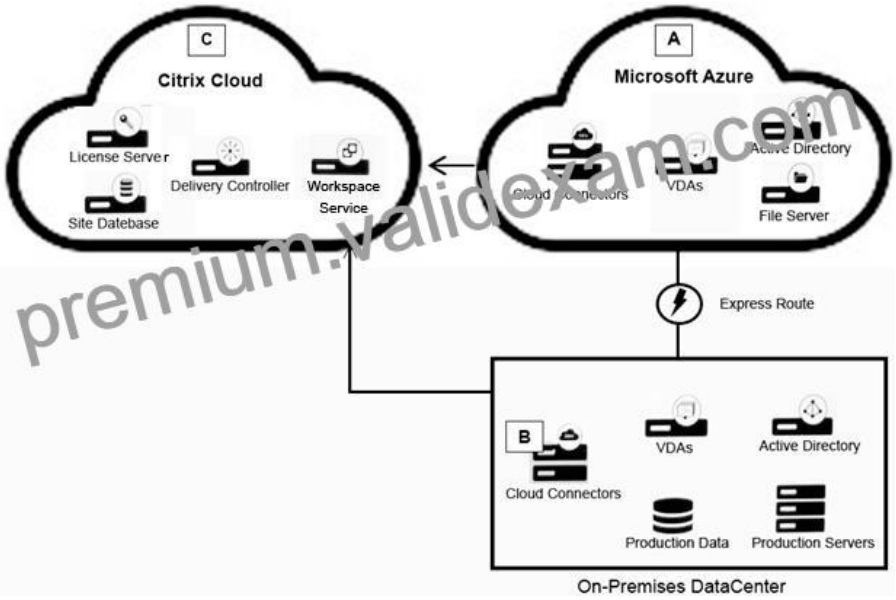
Scenario: A Citrix Architect needs to design a hybrid XenApp and XenApp and XenDesktop environment which will include Citrix Cloud as well as resource locations in on-premises datacenter and Microsoft Azure.

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.)

* Citrix Gateway as a Service, no Citrix products
* No Citrix products, Citrix ADC (BYO)
* Citrix Gateway as a Service, Citrix ADC (BYO)
* No Citrix products, Citrix ICA Proxy (cloud-licensed)
* Citrix Gateway as a Service, Citrix ICA Proxy (cloud-licensed)
* No Citrix products; Citrix Gateway appliance

QUESTION 98

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.

What should the architect do to meet these requirements?
* Delete the existing profile and create a new profile of type: XML Application (SOAP)
* Modify the existing profile to include sessionization
* Create a new basic profile and use pre-existing HTML settings.
* Modify existing profile settings, change HTML settings, and ensure to exclude uploaded files from security checks.

QUESTION 99

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?
* Two standalone Citrix ADC instances in the AWS marketplace, then deploy them as a cluster in the AWS management console
* 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
* Two standalone Citrix ADC instances in the AWS marketplace, then deploy them as an Active-Passive high availability pair in the AWS management console
* 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
* Two Single AMI Citrix CloudFormation templates in the AWS marketplace then configure a high availability pair

QUESTION 100

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?
* Net Profile
* Mac-based forwarding option enabled.
* Resilient deployment mode
* Backup route
Explanation

QUESTION 101

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?
* add cs policy Pol3 -rule “http.REQ.URL.containsC’WEB”)” -action Act3
* add cs policy Pol3 -rule “http.REQ.URLcontainsf’citrix”)” -action Act3
* set cs vserver Vserver -caseSensitive ON
* add cs policy Pol3 -rule “http.REQ.URLPATH_AND_QUERY.con

QUESTION 102

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.

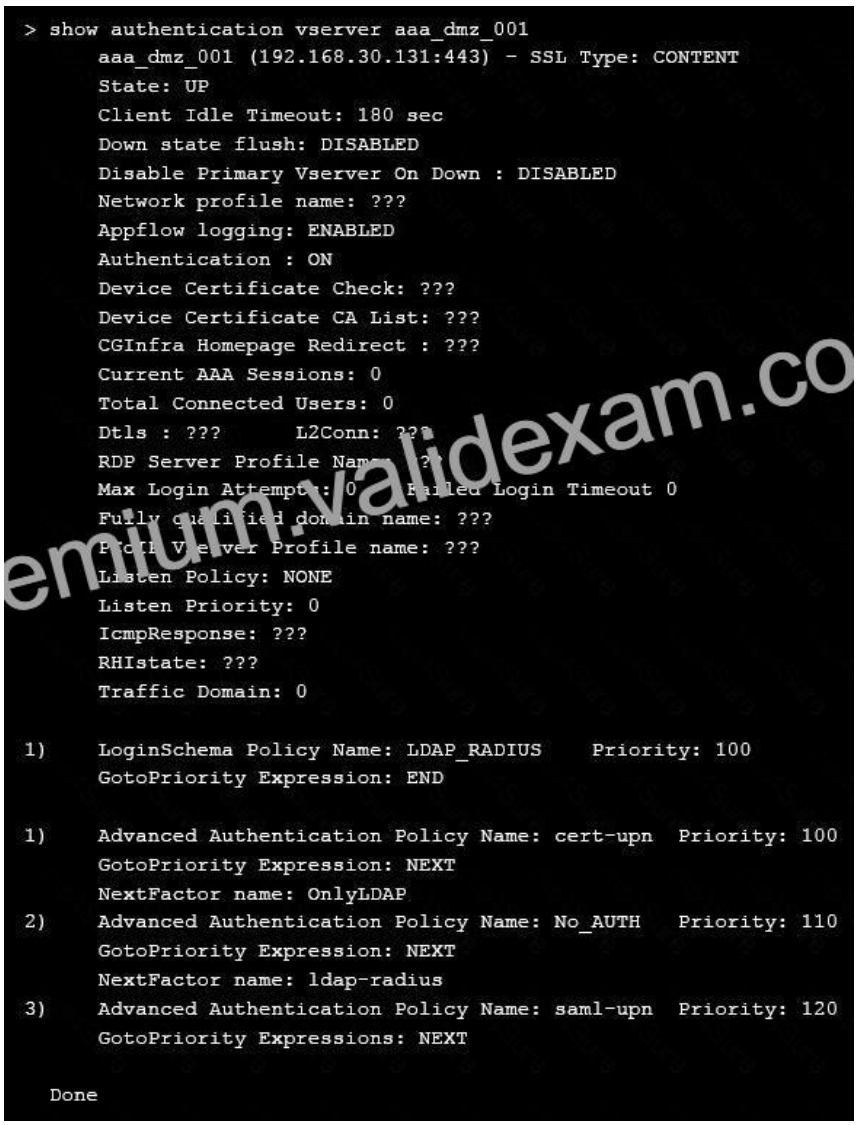
* Single Sign-on must be performed between StoreFront and NetScaler Gateway.

* 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.



What should the architect do to correct this configuration?

* Unbind LoginSchema Policy LDAP_RADIUS from the virtual server.
* Bind the Portal theme as Domaindropdown.
* Bind the LoginSchema Policy Domaindropdown to priority 90.
* Bind the Default LoginSchema Policy as Domaindropdown.

QUESTION 103

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. • After authenticating users should be directed to the organization's intranet portal. • Once connected, outbound traffic from the client device should only pass through the NetScaler Gateway if it is directed to a hosted 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?

* Item 4
* Item 3
* Item 5
* Item 2
* Item 1

QUESTION 104

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

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

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

Requirements

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

Configurations

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

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

* Item 3
* Item 4
* Item 2
* Item 6

QUESTION 105

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

* ICA connections
* Total Connected Users
* Active user session
* Maximum User session

QUESTION 106

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?
* Interface 0/1 must be used for DNS traffic.
* The SNIP of the external NetScaler must be configured as default gateway on the back-end servers.
* ADNS service must be used with IPv6 address.
* Policy-Based Route with next hop as CISCO IPS must be configured on the external NetScaler.

QUESTION 107

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

QUESTION 108

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?
* add responder action act redirect “https://mail.citrix.com” -responseStatusCode 302 add responder policy pol HTTP.REQ.IS_VALID act
* add lb server test SSL 10.107.149.243.80 -persistenceType NONE -cltTimeout 180 -redirectFromPort 80 -httpsRedirectUrl https://mail.citrix.com
* add lb server test SSL 10.107.149.243.443 -persistenceType NONE -cltTimeout 180 -redirectFromPort 80 -httpsRedirectUrl https://mail.citrix.com
* add responder action act redirect “https:// + HTTP REQ.HOSTNAME. HTTP_URL_SAFE + HTTP.REQ.URL_PATH_AND_QUERY.HTTP_URL_SAFEnn” -responseStatusCode 302 add responder policy pol HTTP.REQ.IS_VALID act

QUESTION 109

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?

A

```
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"
   }
}
```

B

```
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"
   }
}
```

C

```
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"
   }
}
```

D

```
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
{
   "clustermode":
   {
     "nodeid".1,
     "ipaddress"."10.102.29.60",
     "state"."ACTIVE",
     "backplane"."1/1/2"
   }
}
```


* Option A
* Option B
* Option C
* Option D

QUESTION 110

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.

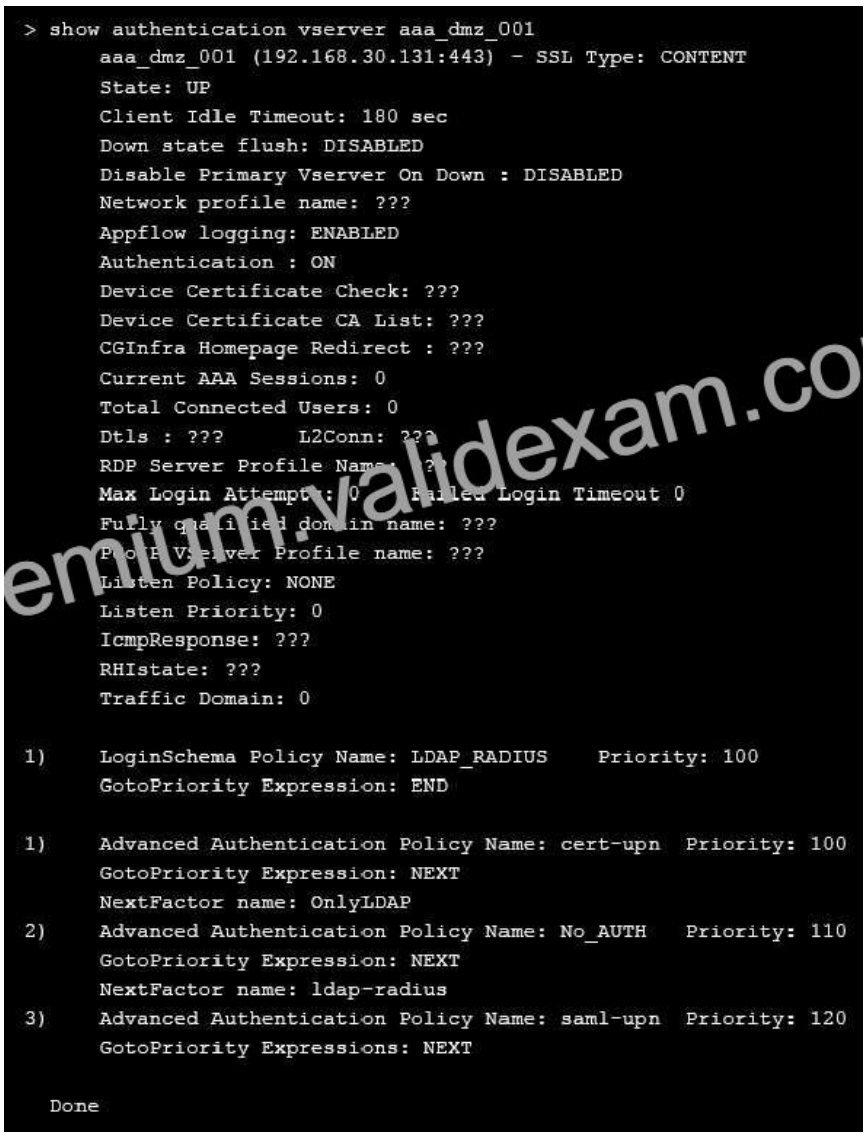
* Single Sign-on must be performed between StoreFront and NetScaler Gateway.

* 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.



What should the architect do to correct this configuration?

* Unbind LoginSchema Policy LDAP_RADIUS from the virtual server.
* Bind the Portal theme as Domaindropdown.
* Bind the LoginSchema Policy Domaindropdown to priority 90.
* Bind the Default LoginSchema Policy as Domaindropdown.

QUESTION 111

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?
* 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
* 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
* 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
* 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

Pass Your Citrix Exam with 1Y0-440 Exam Dumps: https://www.validexam.com/1Y0-440-latest-dumps.html]