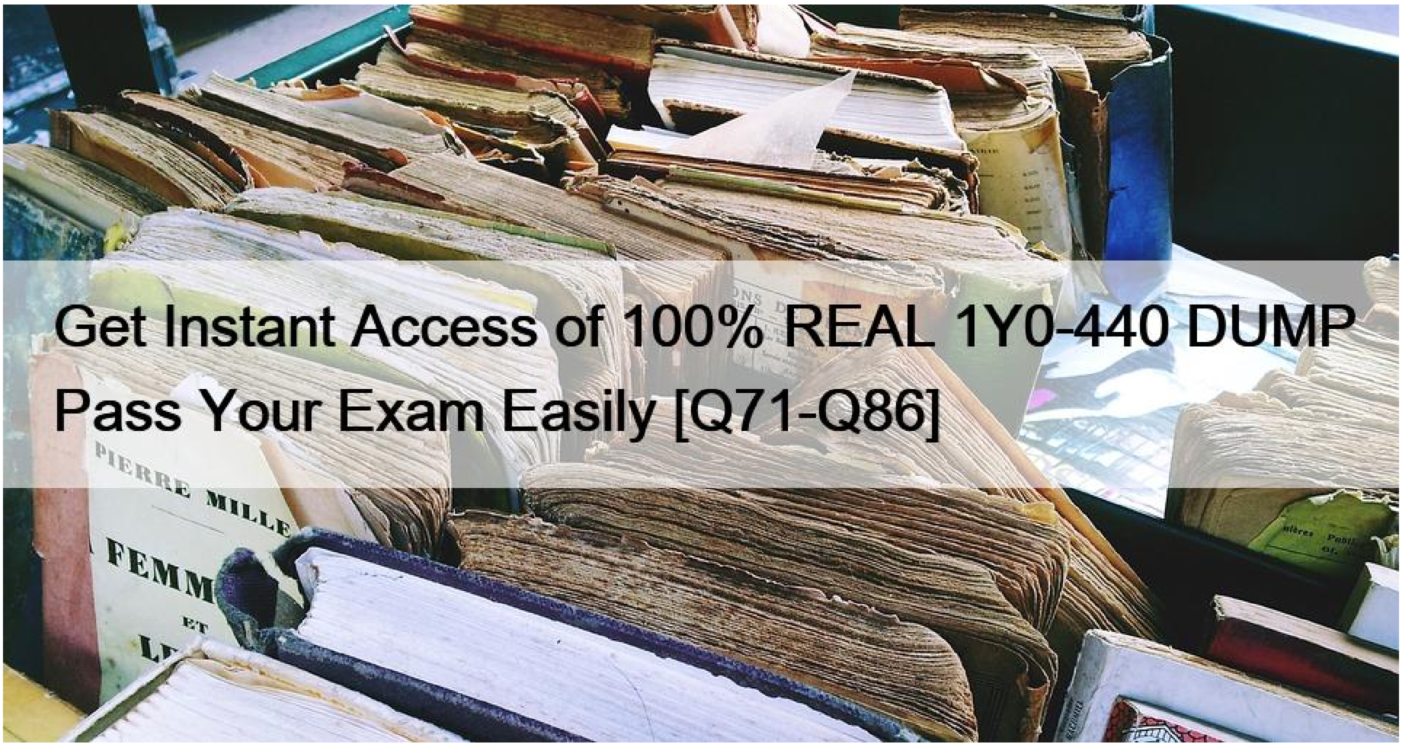
Get Instant Access of 100% REAL 1Y0-440 DUMP Pass Your Exam Easily [Q71-Q86



Get Instant Access of 100% REAL 1Y0-440 DUMP Pass Your Exam Easily
1Y0-440 Free Exam Questions with Quality Guaranteed

NO.71 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?

* add tm sessionAction prof -sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON

-ssoCredential PRIMARY -httpOnlyCookie NO

* add vpn sessionAction prof-sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON

-ssoCredential SECONDARY -httpOnlyCookie NO

* add vpn sessionAction prof -sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON

-ssoCredential PRIMARY -httpOnlyCookie NO

* add tm sessionAction prof -sessTimeout 30 -defaultAuthorizationAction ALLOW -SSO ON

-ssoCredential SECONDARY -httpOnlyCookie NO

NO.72 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?
* 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
* 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
* 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)
* 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

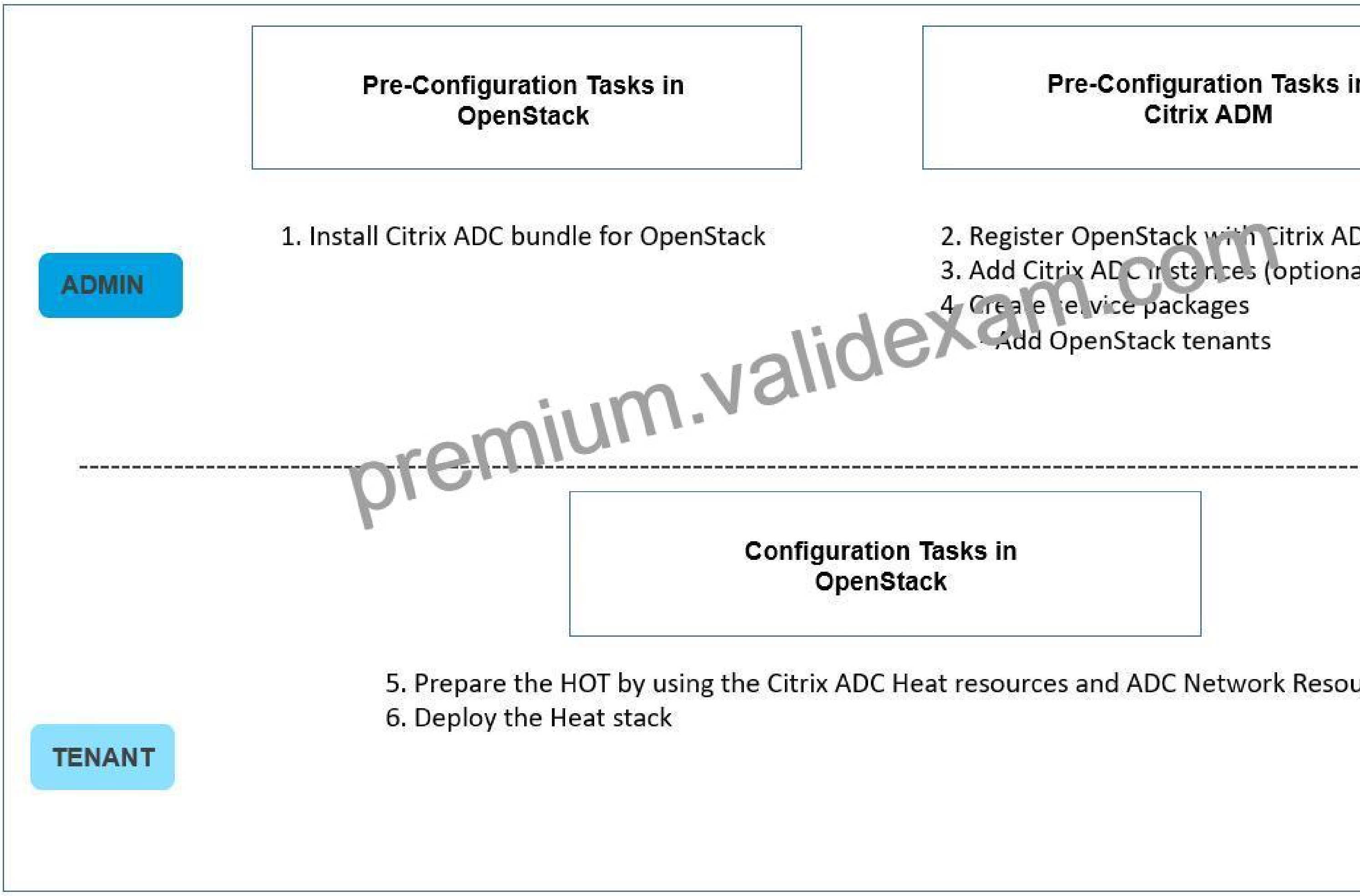
4. Deploy the Heat stack

5. Add NetScaler instances (Optional)

6. Create service packages (Add OpenStack tenants)
Explanation

&#8211;

Workflow to configure ADC instances using Heat


Pre-Configuration Tasks in OpenStack
Pre-Configuration Tasks in Citrix ADM
ADMIN
Configuration Tasks in OpenStack
TENANT

1. Install Citrix ADC bundle for OpenStack

2. Register OpenStack with Citrix AD
3. Add Citrix ADC instances (optiona
4. Create service packages
- Add OpenStack tenants

5. Prepare the HOT by using the Citrix ADC Heat resources and ADC Network Resou
6. Deploy the Heat stack

NO.73 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, NOR, and DR) will have similar Citrix ADC configurations and design.

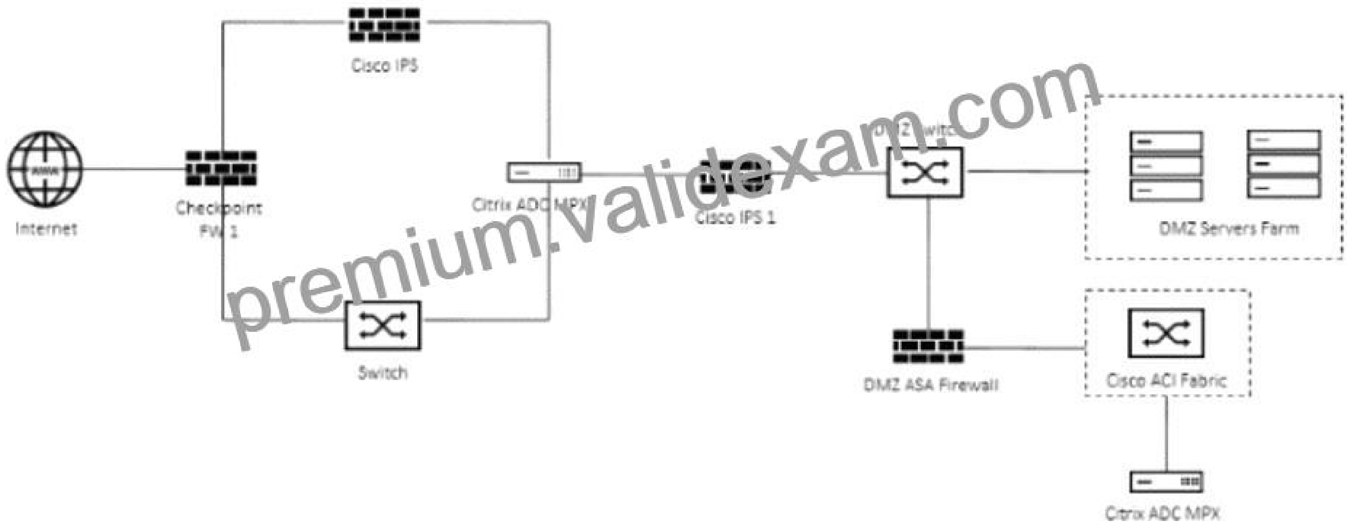
* The external Citrix ADC MPX1 appliances will have Global Server Load Balancing (GSLB) configured and deployed in Active/Active mode.

* 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.



On which firewall should the architect configure the access policy to permit the MEP communication between the sites?

- CISCO IPS 1 and Checkpoint FW1
- CISCO IPS and CISCO IPS1
- CISCO IPS and Checkpoint FW1
- Checkpoint FW1 and DMZ ASA Firewall

NO.74 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

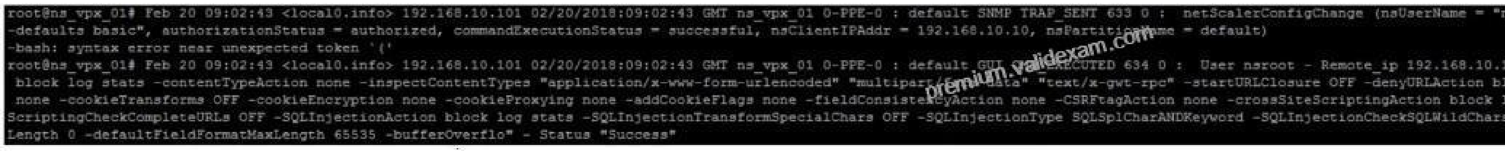
After deployment in pre-production, the team identifies the following additional security features and changes as further requirements:

* 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 = "n
-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 192.168.10.1
 block log stats -contentTypeAction none -inspectContentTypes "application/x-www-form-urlencoded" "multipart/form-data" "text/x-gwt-rpc" -startURLClosure OFF -denyURLAction bl
 none -cookieTransforms OFF -cookieEncryption none -cookieProxying none -addCookieFlags none -fieldConsistencyAction none -CSRFtagAction none -crossSiteScriptingAction block l
ScriptingCheckCompleteURLs OFF -SQLInjectionAction block log stats -SQLInjectionTransformSpecialChars OFF -SQLInjectionType SQLSplCharANDKeyword -SQLInjectionCheckSQLWildChars
Length 0 -defaultFieldFormatMaxLength 65535 -bufferOverflo" - Status "Success"
```

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.

NO.75 Which three tasks can a Citrix Architect select and schedule using the Citrix ADC maintenance tasks?

(Choose three.)
* Convert Citrix Web App Firewall Policy Instances.
* Upgrade Citrix ADC CPX Instances
* Upgrade Citrix ADC Instances.
* Convert a high availability pair of Instances to Cluster.
* Convert cluster instances to a high availability pair.
* Configure a high availability pair of Citrix ADC Instances.

NO.76 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?
* Global Session Settings
* AAA Parameters
* Active User Session
* AAA Virtual Server
Explanation/Reference: https://www.carlstalhood.com/category/netscaler/netscaler-11-1/netscaler-gateway-11-1/

NO.77 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.

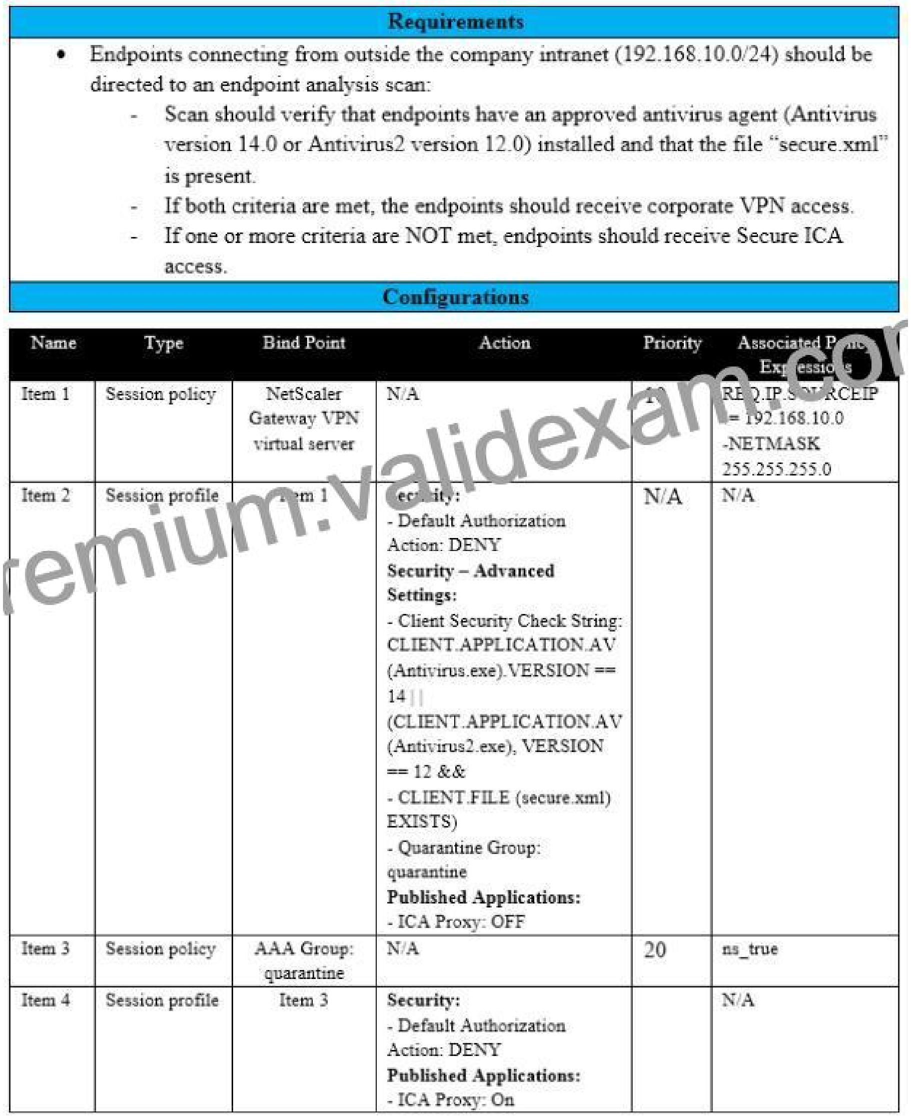
* Once the transfer is successful, auto-delete the configuration file from the NMAS.

Which SNMP trap will trigger the configuration file backup?
* netScalerConfigSave
* sysTotSaveConfigs
* netScalerConfigChange
* sysconfigSave

NO.78 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:
  - Scan should verify that endpoints have an approved antivirus agent (Antivirus version 14.0 or Antivirus2 version 12.0) installed and that 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	Associated Policy Expressions
Item 1	Session policy	NetScaler Gateway VPN virtual server	N/A	10	REQ.IP.SOURCEIP != 192.168.10.0 -NETMASK 255.255.255.0
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

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

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

NO.79 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.

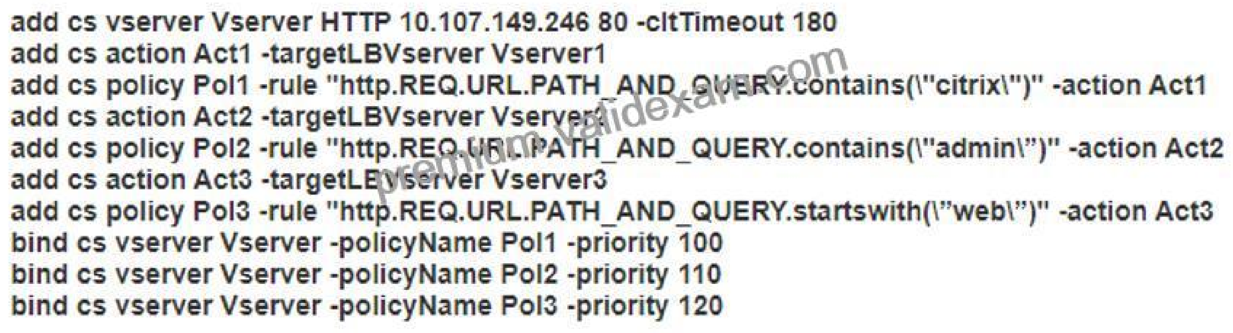
Which action should the architect take to ensure that cookies are shared between the browser and non- browser applications?
* The time zone should be the same on the NetScaler, client, and SharePoint server.
* The SharePoint load-balancing VIP FQDN and the AAA VIP FQDN should be in the trusted site of the client browser.
* The Secure flag must be enabled on the cookie.
* The cookie type should be HttpOnly.
Explanation/Reference: https://support.citrix.com/article/CTX209054

NO.80 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?
* 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)
* 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
* 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
* 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)

NO.81 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 &#8220;503 &#8211; Service Unavailable&#8221; 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 &#8220;http.REQ.URL.containsC&#8217;WEB&#8221;)&#8221; -action Act3
* add cs policy Pol3 -rule &#8220;http.REQ.URLcontainsf&#8217;citrix&#8221;)&#8221; -action Act3
* set cs vserver Vserver -caseSensitive ON
* add cs policy Pol3 -rule &#8220;http.REQ.URLPATH_AND_QUERY.con

NO.82 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.)
* Running Configuration
* Target Instance
* Saved Configuration
* Source Instance
* Configuration Source

NO.83 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.
Explanation

https://support.citrix.com/article/CTX117346

NO.84 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.

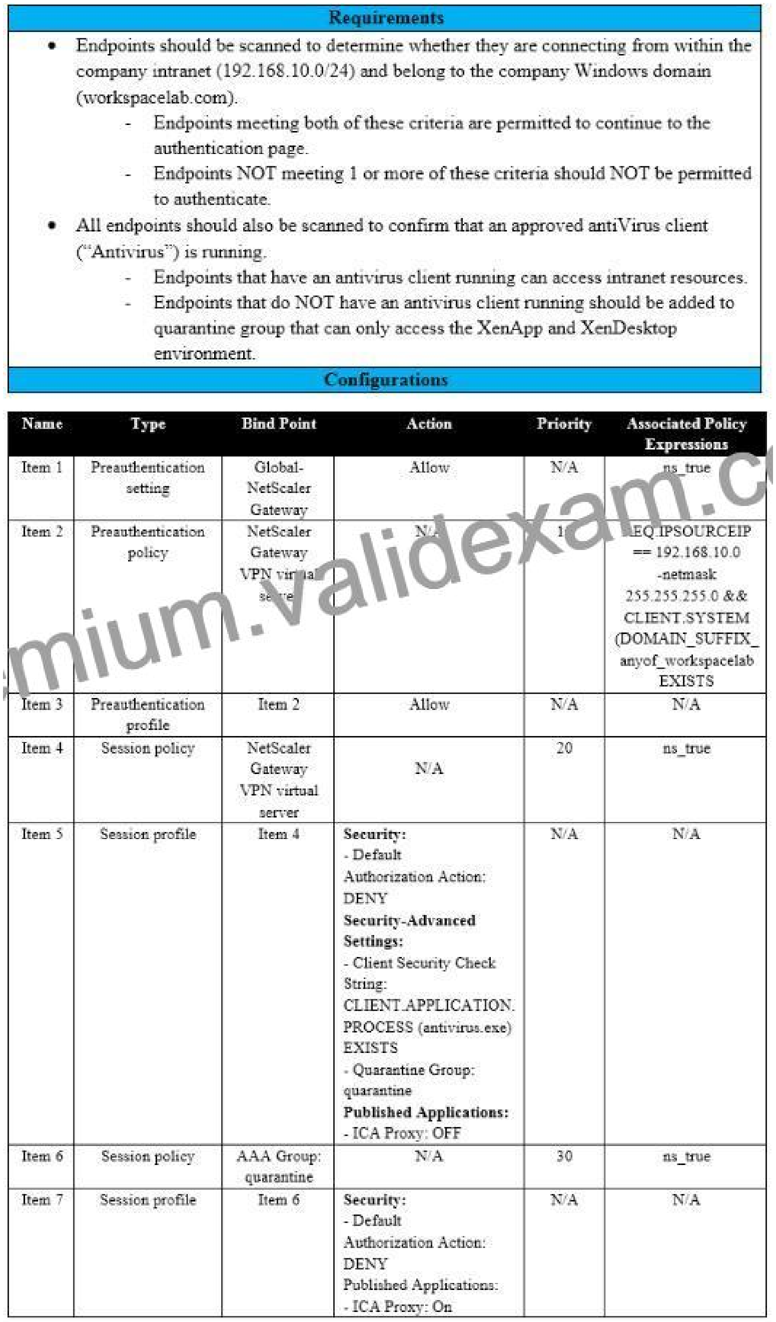
For this deployment, the architect should configure each NetScaler VPX machine to have ______ network interface(s) and configure IP address by using ________. (Choose the correct option to complete the sentence).

* 4; Port Address Translation
* 1; Network Address Translation
* 1; Port Address Translation
* 2; Network Address Translation
* 4; Network Address Translation
* 2; Port Address Translation

NO.85 Scenario: A Citrix Architect needs to assess an existing on-premises NetScaler deployment which includes Advanced Endpoint Analysis scans. During a previous security audit, the team discovered that certain endpoint devices were able to perform unauthorized actions despite NOT meeting pre-established criteria.

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

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



Requirements

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

Configurations

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

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

* Item 6

* Item 7

* Item 1

* Item 3

* Item 5

* Item 2

* Item 4

NO.86 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.

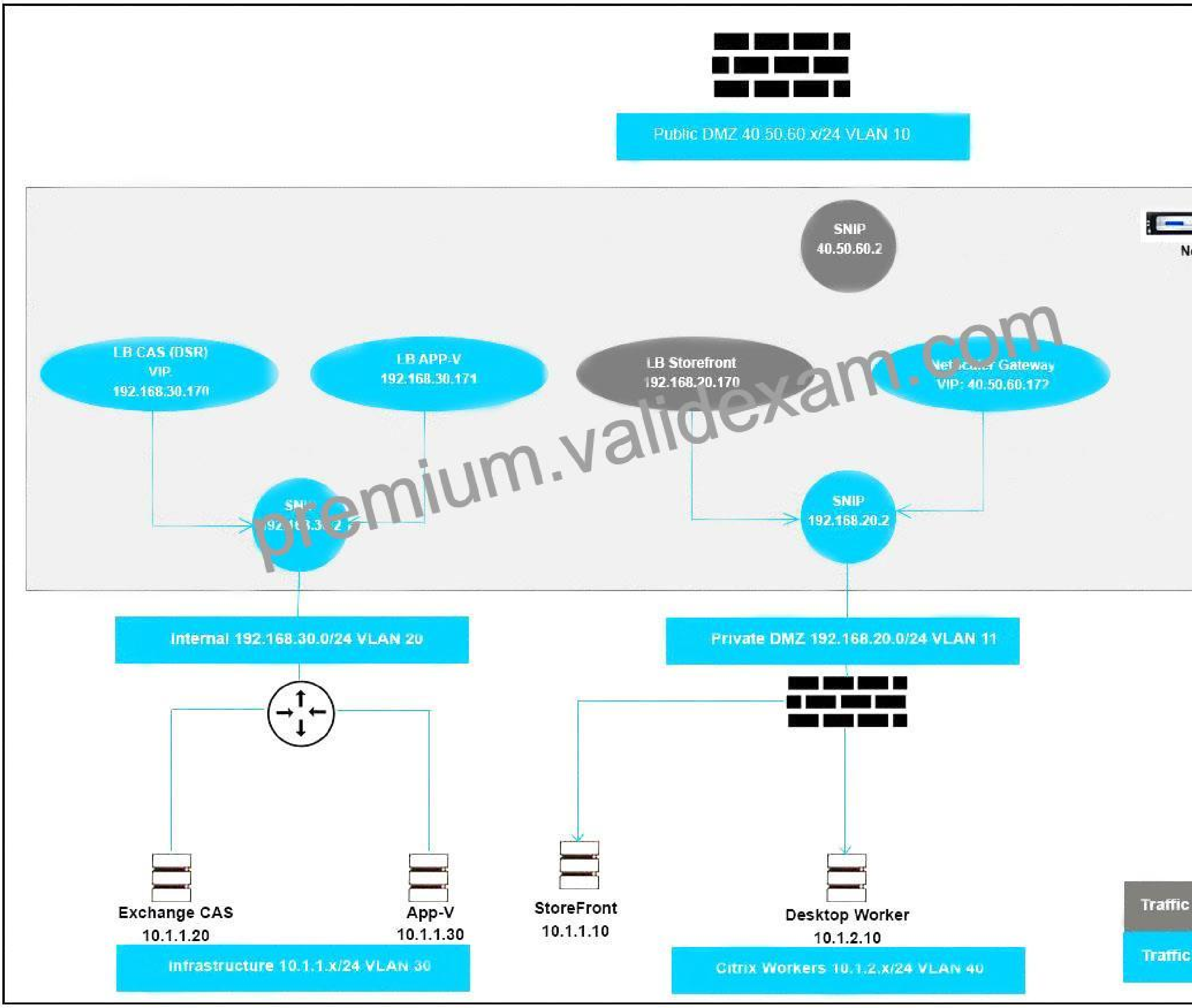
* The NetScaler Gateway virtual server will be utilizing the StoreFront load-balancing virtual server.

* 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.)

- LB StoreFront bound to traffic Domain 0
- Citrix Gateway VIP bound to Traffic Domain 1
- LB APP-V bound to Traffic Domain 1
- SNIP 192.168.20.2 bound to Traffic Domain 1

1Y0-440 Free Exam Files Downloaded Instantly: https://www.validexam.com/1Y0-440-latest-dumps.html]