Free Questions for 1Y0-440 by vceexamstest

Shared by Sellers on 29-01-2024

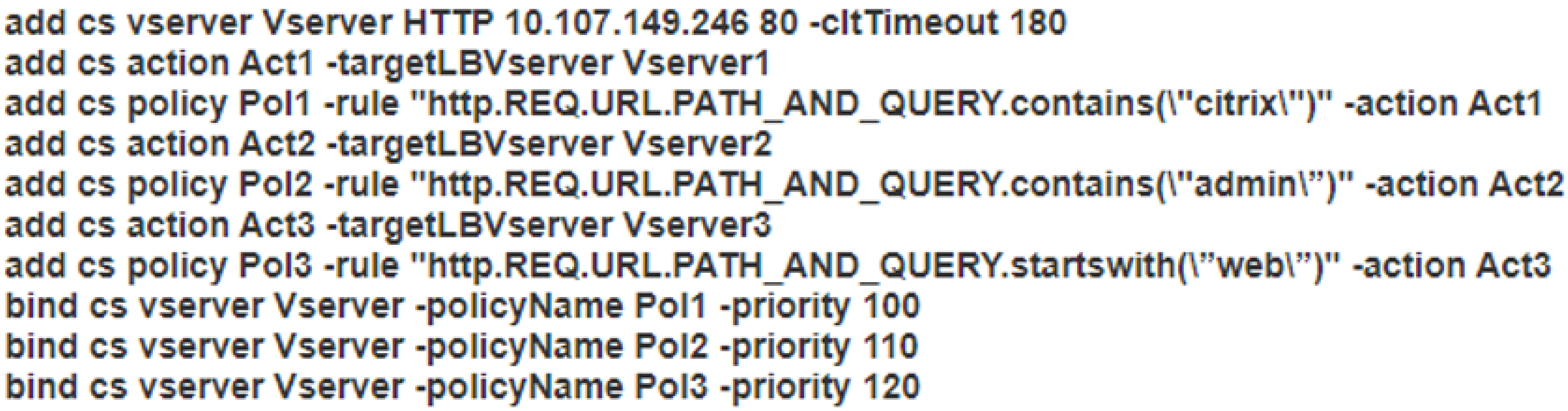
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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

Answer:

D

Question 2

Question Type: **MultipleChoice**

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

Options:

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

Answer:

B, D, E

Explanation:

Verified Answer: A, E, F

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 3

Question Type: **MultipleChoice**

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?

Options:

A- SAML

B- Cert

C- RADIUS

D- LDAP UPN

Answer:

C

Question 4

Question Type: **MultipleChoice**

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?

Options:

A- StyleBooks

B- Orchestration

C- Configuration

D- Jobs Analytics

Answer:

A

Question 5

Question Type: MultipleChoice

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?

Options:

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

Answer:

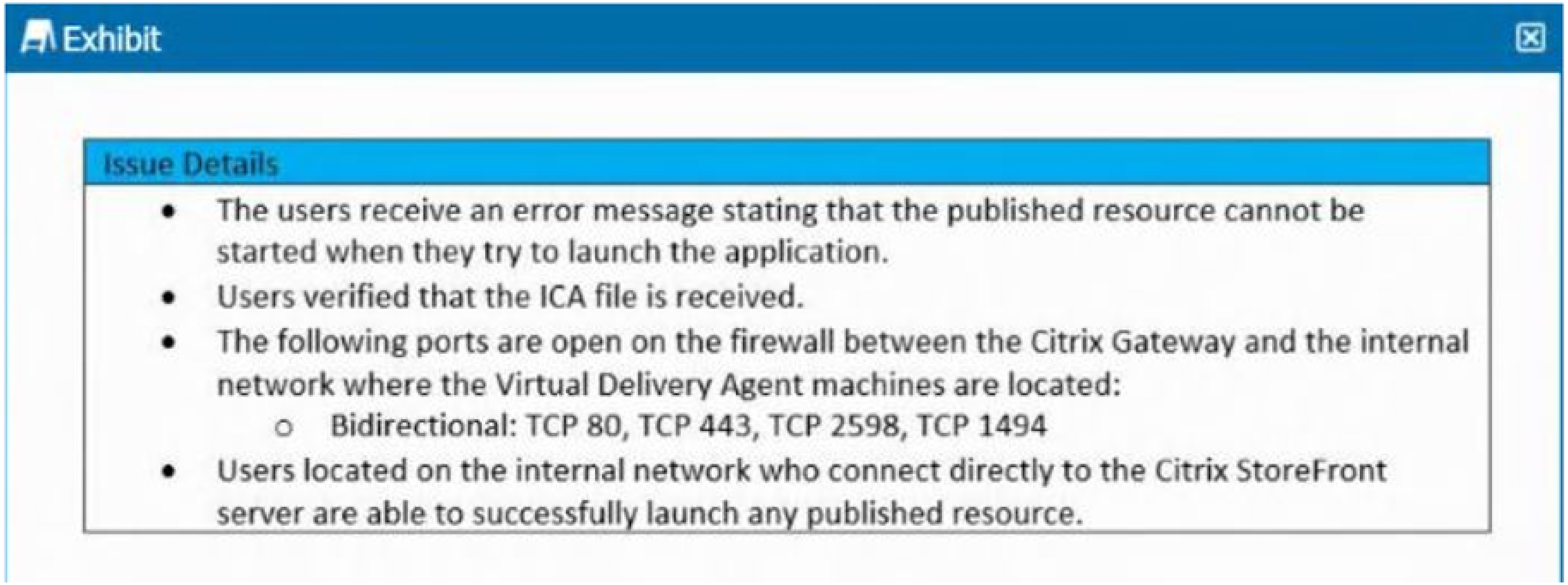
A

Question 6

Question Type: MultipleChoice

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

- The users receive an error message stating that the published resource cannot be started when they try to launch the application.
- Users verified that the ICA file is received.
- The following ports are open on the firewall between the Citrix Gateway and the internal network where the Virtual Delivery Agent machines are located:
    - Bidirectional: TCP 80, TCP 443, TCP 2598, TCP 1494
- Users located on the internal network who connect directly to the Citrix StoreFront server are able to successfully launch any published resource.

What is the cause of this issue?

Options:

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.

Answer:

B

Question 7

Question Type: MultipleChoice

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?

Options:

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

Answer:

A

Question 8

Question Type: MultipleChoice

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?

Options:

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.

Answer:

C

Question 9

Question Type: **MultipleChoice**

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.)

Options:

A- Design

B- Define

C- Manage

D- Deploy

E- Assess

Answer:

A, C

Question 10

Question Type: MultipleChoice

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

Options:

A- Credential Index

B- Default Authorization Action

C- ICA Proxy Migration

D- Session Timeout

E- Expression

F- Name

G- Enable Persistent Cookie

Answer:

A, B, D, G