PassQueen
a.k.a dumpsqueen.com

Architecting a Citrix Networking Solution

Citrix 1Y0-440

Version Demo

Total Demo Questions: 20

Total Premium Questions: 203

Buy Premium PDF

https://passqueen.com

support@passqueen.com

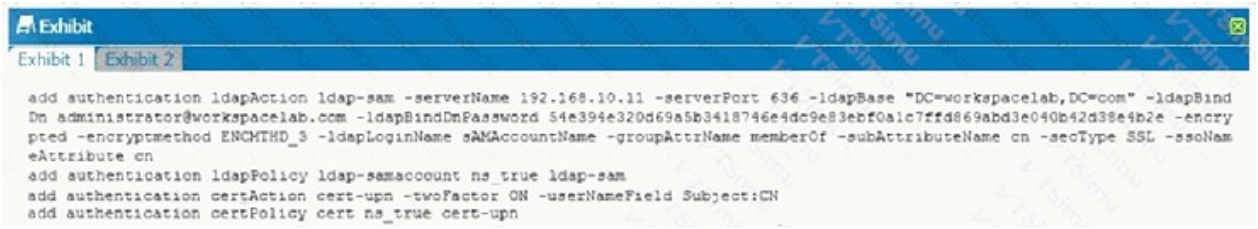
Topic Break Down

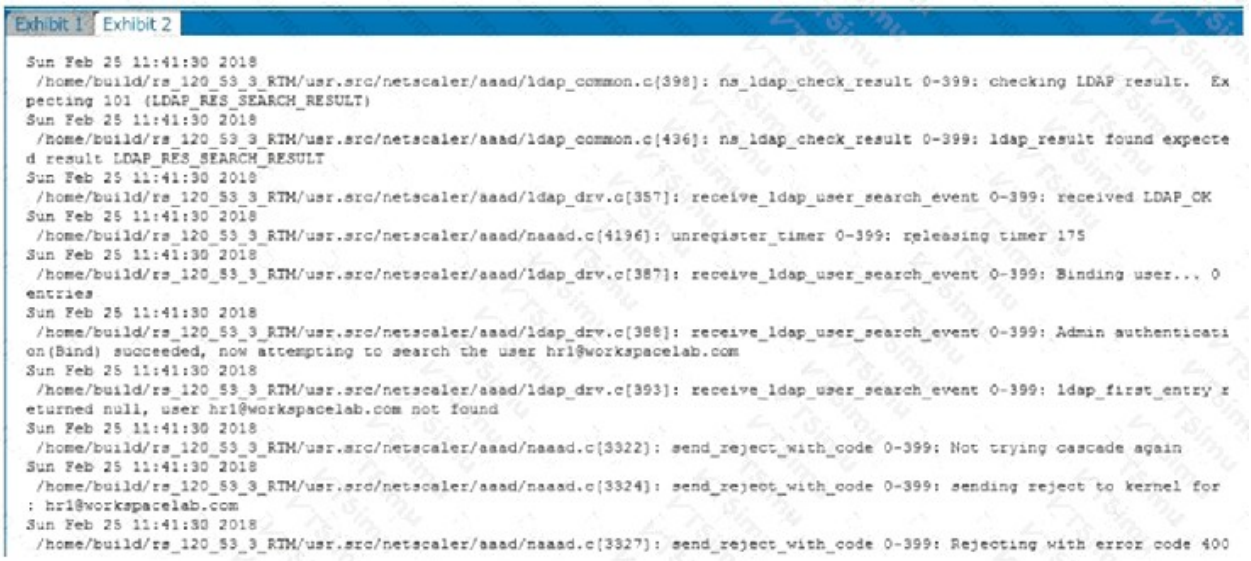
Topic	No. of Questions
Topic 1, Networking Methodology	2
Topic 2, Assessing the Environment	23
Topic 3, Designing the Citrix Networking Solution	63
Topic 4, Deploying the Citrix Networking Solution	6
Topic 5, Configuring the Citrix Networking Solution	81
Topic 6, Integrating Citrix Networking Solution	13
Topic 7, Supporting Citrix Networking Solution	15
Total	203

QUESTION NO: 1

Scenario: A Citrix Architect holds a design discussion with a team of Workspacelab members, and they capture the following requirements for the Citrix ADC design project:

Click the Exhibit button to review the output of aaad.debug and the configuration of the authentication policy.





What is causing this issue?

A. ldapLoginName is set as sAMAccountName

B. UserNamefield is set as subjecticn

C. Password used is incorrect

D. User does NOT exist in database

ANSWER: A

Explanation:

ldapLoginName is set as sAMAccountName is the cause of the LDAP failure. In a certificate-plus-LDAP authentication flow, Citrix ADC first derives a user identity from the client certificate and then passes that identity to the next LDAP authentication factor. The stated certificate requirement means that the identity supplied by the certificate is the user's User Principal Name, typically in a format such as `user@workspacelab.com`. The LDAP action must therefore search Active Directory using an attribute that contains that UPN, namely `userPrincipalName`.

When `ldapLoginName` is configured as `sAMAccountName`, Citrix ADC constructs the LDAP lookup using the UPN value against the sAMAccountName attribute. sAMAccountName ordinarily contains the legacy short logon name, such as `user`, rather than the UPN. As a result, the LDAP search cannot locate the matching directory object and authentication fails after certificate authentication. Configuring the LDAP action with `userPrincipalName` as the login attribute aligns the certificate-derived identity with the Active Directory lookup and supports the required single sign-on flow. Citrix documents certificate authentication and LDAP authentication configuration in its certificate authentication documentation and LDAP authentication documentation.

QUESTION NO: 2

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

A. Single Sign-on Domain

B. Request Profile

C. Name

D. Enable Persistent Cookie

E. Expression

ANSWER: B C E

Explanation:

Creating a Citrix ADC session policy requires a unique **Name**, a **Request Profile**, and an **Expression**. The Name identifies the policy object on the appliance and is the value used later when the policy is bound at the global, virtual-server, group, or user level. The Request Profile associates the session policy with the session-profile settings that should be applied when the policy evaluates successfully. Those profile settings can control the user's VPN/session behavior, such as clientless access, plug-in behavior, endpoint analysis, and other session parameters.

The Expression supplies the policy rule that determines which incoming requests or connection contexts match. Citrix ADC evaluates this expression to decide whether the linked Request Profile applies. Together, the policy name, matching expression, and associated profile define the complete policy relationship: an identifiable policy object, the criteria for invoking it, and the session configuration delivered on a match. Citrix documents session policies as rules that use an expression and invoke a session profile, and its command reference lists the policy name, rule, and profile association as the key session-policy configuration elements. See Citrix ADC session policies documentation and the Citrix ADC session policy command reference.

QUESTION NO: 3

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.

ANSWER: B

Explanation:

The SharePoint load-balancing VIP FQDN and the AAA VIP FQDN should be in the trusted site of the client browser. SharePoint document editing and uploading can involve both the browser and Microsoft Office or WebDAV-based client components. In this design, the browser authenticates through the Citrix ADC (formerly NetScaler) AAA virtual server and receives the persistent authentication cookie, while the non-browser component must also be able to participate in the authenticated SharePoint access flow. Adding both fully qualified domain names to the client browser's Trusted Sites zone establishes the required trust relationship for this integrated browser and rich-client behavior.

Both names are important because authentication is handled at the AAA virtual server, whereas access to SharePoint is made through the load-balancing virtual server. Trusting the complete set of URLs used in the transaction enables the persistent cookie to be used consistently when Office applications or other non-browser integrations access SharePoint

resources. Citrix documents this requirement specifically for SharePoint deployments using persistent cookies to support document operations. See Citrix Knowledge Center article CTX209054 and the Citrix ADC authentication documentation.

QUESTION NO: 4

Which three protections can a Citrix Architect configure by using the Citrix ADC Web Application Firewall feature? (Choose three.)

A. SQL injection protection

B. Cross-site scripting protection

C. Form field consistency protection

D. Full VPN tunneling for remote users

E. DNS delegation for GSLB domains

ANSWER: A B C

Explanation:

SQL injection protection is a Citrix ADC Web Application Firewall capability that detects and blocks malicious SQL patterns in application requests. **Cross-site scripting protection** helps protect applications against malicious script content that could be injected into web requests. **Form field consistency protection** validates submitted form data against the expected form structure and configured field rules.

Citrix ADC Web Application Firewall applies security checks to HTTP and HTTPS applications and can use signatures, learned profiles, and configured security checks to protect applications from common web attacks. The feature is distinct from remote-access and DNS functions, which are provided by other Citrix ADC capabilities. See the Citrix ADC Web Application Firewall documentation.

QUESTION NO: 5

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

A. Event Manager

B. instance

C. File

D. Plug and Play

E. Action

ANSWER: B C

Explanation:

instance and **File** are the required settings when Citrix Application Delivery Management configures CPX from a pre-existing CPX device. The instance setting identifies the existing CPX instance that ADM will use as the source. This lets ADM obtain the relevant CPX context and configuration from a device that is already registered and manageable in the ADM inventory. The File setting identifies the configuration file to use for the CPX deployment or configuration operation. Together, these settings provide both the source CPX device and the configuration artifact needed to apply a consistent CPX configuration.

This approach supports repeatable deployment and configuration practices: an architect can use a known-working CPX instance as the basis for another CPX configuration while explicitly selecting the file that contains the desired NetScaler configuration. CPX is the containerized form factor of the Citrix ADC/NetScaler data plane, and ADM provides centralized

management and configuration workflows for such instances. Citrix documentation for CPX is available in the Citrix ADC CPX documentation, and ADM management concepts are documented in the Citrix Application Delivery Management documentation.

QUESTION NO: 6

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

Which configuration should the architect choose to accomplish this?

A. Two standalone Citrix ADC instances in the AWS marketplace, then deploy them as a cluster in the AWS management console

B. A Citrix ADC VPX high-availability pair using a Citrix CloudFormation template in the AWS Marketplace, then deploy it to create an active-passive high-availability pair

C. Two standalone Citrix ADC instances in the AWS marketplace, then deploy them as an Active-Passive high availability pair in the AWS management console

D. Two standalone Citrix ADC instances in the AWS marketplace, deploy them in the AWS management console, then use an AWS Elastic Load Balancing load balancer to distribute client traffic across both instances

E. Two Single AMI Citrix CloudFormation templates in the AWS marketplace then configure a high availability pair

ANSWER: B

Explanation:

A Citrix ADC VPX high-availability pair deployed with the Citrix CloudFormation template is the appropriate design for this requirement. Citrix provides AWS CloudFormation templates specifically to automate deployment of Citrix ADC high-availability configurations. The template creates the required AWS resources and Citrix ADC instances, applies the networking configuration needed for an internet-facing deployment, and establishes an active-passive HA relationship between the appliances. For a single Availability Zone design, both appliances can be placed in that zone while retaining the availability benefits of independent instances and Citrix ADC HA state synchronization. The active appliance processes the application load-balancing traffic; if it becomes unavailable, the secondary appliance can assume the active role. CloudFormation is particularly suitable because it makes the deployment repeatable and ensures that AWS-side configuration—such as interfaces, security groups, routing-related settings, and address association required by the template—is consistently created alongside the ADC pair. Citrix documents deploying an HA pair on AWS through its CloudFormation-based workflow, including the topology choices for one or more Availability Zones. See NetScaler documentation for deploying a Citrix ADC HA pair on AWS and the maintained NetScaler ADC CloudFormation templates repository.

QUESTION NO: 7

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

ANSWER: A

Explanation:

Item 5 is the configuration that must be changed because the assessment exhibit identifies it as the session-profile setting whose current value does not satisfy the stated VPN-user requirements. A Citrix Gateway session profile defines the settings delivered to users after authentication, including the VPN client experience and access behavior. The effective settings must align with the organization's required user access model, rather than merely reflecting a default or inherited configuration. Updating Item 5 brings the applied session-profile configuration into compliance with the requirements while preserving the remaining settings that already meet the documented design criteria.

Citrix recommends configuring user experience and access behavior through Citrix Gateway session profiles and policies, then binding the appropriate policy so that the required profile is applied to the intended users. This permits administrators to make targeted changes without unnecessarily altering unrelated gateway settings or affecting users governed by different policies. Citrix Gateway session-profile and policy configuration is documented at Citrix Gateway session profiles and policies. Additional guidance on configuring the VPN client experience is available in the Citrix Gateway client experience documentation.

QUESTION NO: 8

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 two 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

ANSWER: A D

Explanation:

Simplify Management is prioritized because the existing network can already accommodate the anticipated user population, while the constrained support team must still operate and maintain the environment effectively. A Citrix networking design should therefore emphasize centralized administration, policy consistency, monitoring, automation, and repeatable configuration processes. These capabilities allow a small operations team to manage a large deployment without requiring a proportional increase in administrative effort.

Reduce Costs is also prioritized because limited support staffing is an operational-cost constraint. Reducing manual administrative activities, accelerating troubleshooting, and using centralized management lowers the ongoing cost of supporting the environment. The requirement is not merely to make the platform technically functional for more users; it is to do so within available support resources and without expanding the operational burden. Citrix Application Delivery Management provides centralized management, orchestration, analytics, and automation capabilities intended to improve operational efficiency across Citrix ADC instances. See the Citrix Application Delivery Management documentation and the Citrix ADC product overview.

QUESTION NO: 9

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

A. Determine operating system and application usage.

B. Identify other planned projects and initiatives that must be integrated with the design and build phase.

C. Determine the new environment networking requirements.

D. Establish and prioritize the key drivers behind a project.

E. Assess and identify potential risks for the design and build phase.

ANSWER: B E

Explanation:

A capabilities assessment is used to understand the organizational and technical conditions that can affect successful delivery of the Citrix ADC solution, particularly where the appliance must coexist with established services, teams, processes, and change schedules. **Identify other planned projects and initiatives that must be integrated with the design and build phase.** is correct because dependencies such as data-center moves, network refreshes, security-program changes, application releases, or identity-service changes can affect sequencing, ownership, testing, and implementation windows. Capturing these initiatives early lets the architect align the ADC design and rollout plan with the wider environment rather than treating the deployment as an isolated activity.

Assess and identify potential risks for the design and build phase. is also correct because an assessment should expose risks that require mitigation before implementation, including routing or firewall dependencies, availability constraints, operational support readiness, change-control restrictions, and migration impacts. Citrix ADC deployment planning requires consideration of the existing network topology and integration points, while Citrix's architecture guidance emphasizes documenting assumptions, dependencies, and risks as part of a sound design process. The assessment findings provide inputs for implementation planning, validation criteria, rollback preparation, and stakeholder decisions. See the Citrix ADC deployment documentation and the Citrix Tech Zone reference architectures.

QUESTION NO: 10

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

A. Single Sign-on Domain

B. Credential Index

C. KCD Profile

D. Default Authentication Group

E. Single Sign-on to Web Applications

F. Session Idle Time

ANSWER: A E F

Explanation:

Single Sign-on Domain, **Single Sign-on to Web Applications**, and **Session Idle Time** are valid Citrix Gateway session-profile settings used to tailor the user session. Single Sign-on Domain identifies the domain used when Gateway performs single sign-on for published resources, allowing the session configuration to provide the appropriate domain context for authentication. Single Sign-on to Web Applications enables Gateway single sign-on behavior for web applications accessed through the Gateway portal, supporting a smoother user experience by passing authenticated credentials where the configured application and authentication method support it.

Session Idle Time is a session-management control that defines how long an inactive Gateway session may remain open before the appliance terminates or disconnects it according to the configured policy. This is an important architectural setting because it balances user convenience with security requirements for unattended sessions. These settings are configured through Citrix Gateway session profiles and can be applied selectively through session policies, enabling different user groups, access methods, or resource scenarios to receive appropriate session behavior. Citrix documents session policies and profiles as the mechanism for controlling Gateway user-session parameters, including single sign-on and timeout-related behavior. See Citrix Gateway session policies and profiles documentation and Citrix Gateway single sign-on documentation.

QUESTION NO: 11

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

Click the Exhibit button to view the troubleshooting details collected by the customer.

Issue Details
• External users trying to launch a Shared Hosted Desktop via a NetScaler gateway connection receive an ICA file from StoreFront. • However, they are unable to launch the Shared Hosted Desktop. • The following ports are open on the firewall between the NetScaler 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 StoreFront server are able to launch the Shared Hosted Desktop.

What is the cause of this issue?

A. The required ports have NOT been opened on the firewall between the NetScaler gateway and the Virtual Delivery Agent (VDA) machines.

B. The StoreFront URL configured in the NetScaler gateway session profile is incorrect.

C. The Citrix License Server is NOT reachable.

D. The Secure Ticket Authority (STA) servers are load balanced on the NetScaler.

ANSWER: D

Explanation:

The Secure Ticket Authority (STA) servers are load balanced on the NetScaler. For ICA proxy resource launches, StoreFront requests an STA ticket from a specific Delivery Controller STA service. Citrix Gateway must then validate that ticket with the same STA that issued it. An STA ticket is not a shared, cluster-wide token that another Delivery Controller can validate merely because it is part of the same load-balancing group. When the Gateway is configured with a load-balanced virtual server as the STA endpoint, ticket validation can be sent to a different backend Delivery Controller than the one that issued the ticket. The result is an invalid-ticket condition and the published application or desktop fails to launch, even though users can authenticate and enumerate resources successfully. Configure the individual Delivery Controller STA URLs directly on Citrix Gateway and ensure that the same STA list, in the same order, is configured in StoreFront. This preserves the required ticket-issuance and validation behavior while providing STA redundancy. Citrix documents STA configuration requirements for Gateway ICA proxy deployments in CTX101810: Configuring Secure Ticket Authority on Citrix Gateway and in the Citrix Gateway documentation.

QUESTION NO: 12

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 f the architect enabled the Appli cation 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

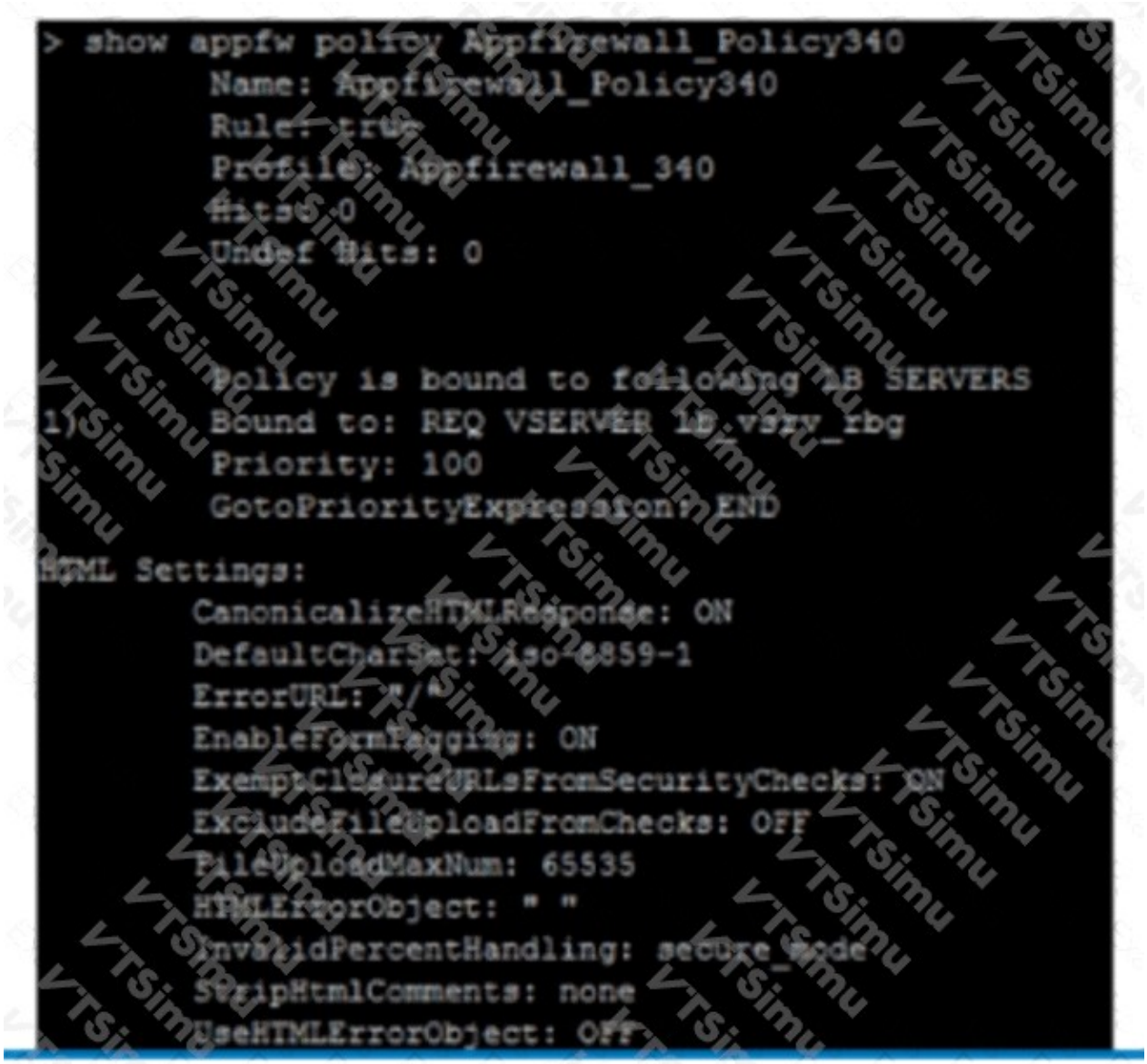
• Form-Field consistency

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 get a pre-configured HTML error page with appropriate information.

• The Application Firewall profile should be able to handle the data from an RSS feed **and** an ATOM-based site. Click the Exhibit button to view an excerpt of the existing configuration.



What should the architect do to meet these requirements?

A. Modify existing profile settings and disable the setting ' Enable Form Tagging ' .

B. Create a new basic profile and use pre-existing HTML settings.

C. Modify existing profile settings, change HTML settings, and ensure to exclude uploaded files from security chec k s.

D. Modify existing profile settings and change HTML settings to use an HTML error object.

ANSWER: D

Explanation:

Modify existing profile settings and change HTML settings to use an HTML error object. The existing Application Firewall profile already contains the relevant HTML protections, including Form-Field consistency. With form tagging enabled, the ADC can insert tags into form responses and retain the expected form-field information so that it can validate a later client submission before forwarding it to the protected application. This directly supports the required response-to-request consistency validation.

An HTML error object supplies the customized HTML response returned when a request is blocked. Associating that error object with the profile allows blocked traffic to receive the organization's preconfigured informational page rather than a generic response. The HTML settings must also be adjusted to recognize the relevant RSS and Atom content types. RSS and Atom are XML-based formats, and configuring the applicable content types ensures the profile processes this application data appropriately while retaining the existing protections and error handling.

Citrix Application Firewall documentation describes profile-level security checks, including form-field consistency and form tagging, as well as configurable response behavior for blocked requests. See Citrix ADC Application Firewall documentation and Application Firewall protection checks.

QUESTION NO: 13

A Citrix Architect can execute a configuration job using a DeployMasterConfiguration template on a Citrix ADC____deployed_____. (Choose the correct option to complete sentence:

A. MPX; In high availability

B. CPX: without partitions

C. CPX; In high availability

D. MPX; as a cluster Instance

E. SDX; with more than 6 partitions

ANSWER: A

Explanation:

MPX; In high availability correctly completes the statement. Citrix Application Delivery Management configuration jobs can use templates to deploy and manage configuration consistently on supported Citrix ADC instances. For an MPX appliance configured as a high-availability pair, the active node is the configuration point for the appliance pair. Citrix ADC synchronizes the running configuration from the primary node to the secondary node, allowing the configuration job to be applied in a manner that preserves the intended HA operating model rather than treating the two nodes as unrelated appliances. This is important for repeatable deployment because the template-based job establishes the desired ADC configuration while HA supplies appliance redundancy and configuration synchronization.

Citrix documents HA as a paired Citrix ADC deployment in which one node operates as primary and the peer serves as the secondary node, with synchronization supporting continuity if a failover occurs. Citrix ADM's configuration-job capability is intended to deploy configuration to managed instances through templates and controlled execution. See Citrix ADC high availability documentation and Citrix ADM configuration jobs documentation.

QUESTION NO: 14

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

A. Running Configuration

B. Target Instance

C. Saved Configuration

D. Source Instance

E. Configuration Source

ANSWER: B D

Explanation:

Source Instance and **Target Instance** are required to define a configuration-replication job. The source instance is the Citrix ADC appliance from which Citrix ADM obtains the selected configuration objects or commands. It establishes the authoritative appliance and configuration context from which the desired snippet is collected. The target instance parameter identifies the managed Citrix ADC appliances that will receive that selected configuration. Although the field is expressed in the singular, a configuration job can select multiple target appliances, allowing the same approved snippet to be consistently deployed to all intended instances.

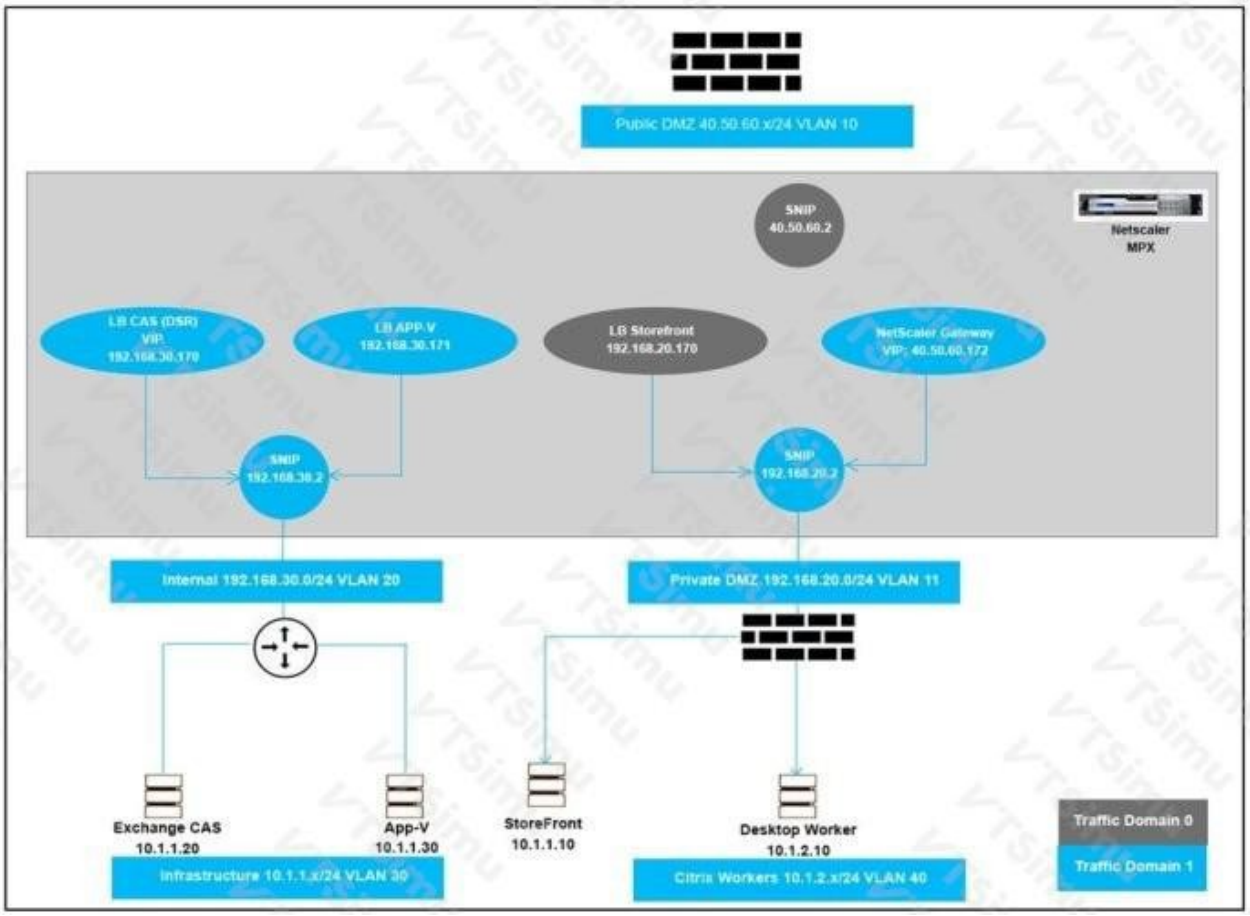
This source-to-target definition is fundamental to configuration jobs: ADM first uses the source appliance to select the relevant configuration entities, then applies the resulting job to the chosen target appliances. The administrator can choose whether to work from a running or saved configuration where supported, but that is a configuration-state selection rather than the pair of endpoint parameters needed to perform replication. Citrix documents configuration jobs as a mechanism for propagating configuration across managed instances; see Citrix ADM Configuration Jobs documentation and Citrix ADM instance management documentation.

QUESTION NO: 15

Scenario: A Citrix Architect and a team of Workspacelab members met to discuss a NetScaler design project. They captured the following requirements from this design discussion:

- A pair of NetScaler MPX appliances will be deployed in the DMZ network.
- High Availability will be accessible in the NetScaler MPX in the DMZ Network.
- Load balancing should be performed for the internal network services like Microsoft Exchange Client Access Services and Microsoft App-V.
- The load balancing should be performed for StoreFront.
- The NetScaler Gateway virtual server will be utilizing the StoreFront load-balancing virtual server.
- The NetScaler Gateway virtual server and StoreFront.
- The NetScaler Gateway virtual service and StoreFront and load-balancing services are publicly accessible.
- The traffic for internal and external services must be isolated.

Click the Exhibit button to review the logical network diagram.



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

A. LB StoreFront bound to traffic Domain 0

B. NetScaler Gateway VIP bound to Traffic Domain 1

C. LB APP-V bound to Traffic Domain 1

D. SNIP 192.168.20.2 bound to Traffic Domain 1

ANSWER: A C

Explanation:

"LB StoreFront bound to traffic Domain 0" is an incorrect design decision because the StoreFront load-balancing virtual server is consumed by the externally accessible NetScaler Gateway deployment. To meet the stated isolation requirement, the public Gateway and its associated StoreFront load-balancing endpoint must be placed in the traffic domain assigned to the external/DMZ service path, rather than the internal traffic domain. This maintains a distinct routing and address context for public-facing services while still allowing the ADC to load balance StoreFront.

"LB APP-V bound to Traffic Domain 1" is also incorrect because App-V is identified as an internal service. Its load-balancing virtual server must be associated with the internal traffic domain, alongside the internal service network and the appropriate internal source IP address. Citrix ADC traffic domains provide separate routing domains and allow the appliance to isolate network contexts, including cases involving overlapping addressing. Correctly assigning the public StoreFront/Gateway path and the internal App-V path to their respective traffic domains is therefore fundamental to the required segmentation. Citrix documents traffic-domain behavior at Citrix ADC Traffic Domains and describes load-balancing configuration concepts at Citrix ADC Load Balancing.

QUESTION NO: 16

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

ANSWER: A D E

Explanation:

SAML, **WEBAUTH**, and **LDAP** can be used when Citrix ADC authenticates a user before providing Kerberos impersonation-based single sign-on to a load-balanced application. LDAP authentication allows the appliance to validate the user against a directory and obtain the authenticated user identity from Active Directory. Web authentication supports a custom web-based authentication exchange, enabling Citrix ADC to receive and validate the user information required for the authenticated session. SAML authentication allows Citrix ADC to consume a trusted identity assertion from a SAML identity provider and use the asserted user identity for the session.

For Kerberos impersonation, the essential outcome is a trusted, authenticated user principal that Citrix ADC can associate with the target Active Directory domain. Citrix ADC then uses its configured Kerberos delegation/impersonation settings and service identity to request access to the backend service on behalf of that authenticated principal. This provides seamless access to the application while the application server continues to receive a Kerberos-authenticated user context. Citrix ADC documents its supported AAA authentication mechanisms and their use with traffic-management integrations in the AAA-TM documentation and describes backend application delivery features in the load balancing documentation.

QUESTION NO: 17

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

A. URLHash

B. Least response time

C. Least Packets

D. Least Connection

E. LRTM

F. Least bandwidth

G. SRCIPSRCPORTHash

ANSWER: B D E F

Explanation:

Citrix ADC virtual server-level Slow Start is supported with **Least response time**, **Least Connection**, **LRTM**, and **Least bandwidth** load-balancing methods. Slow Start gradually increases the proportion of new client connections sent to a newly enabled or recovered service. This lets the service warm up without immediately receiving its full calculated share of traffic, helping avoid overload while it establishes normal capacity and response behavior.

These supported methods are adaptive algorithms that use current service load or performance measurements when selecting a service. **Least Connection** considers active connections, **Least response time** incorporates response-time information, **LRTM** uses response-time and connection-load measurements, and **Least bandwidth** considers bandwidth consumption. Because each method can continuously evaluate service load, Citrix ADC can safely phase a recovering service into the selection process through the configured Slow Start interval. Citrix documents Slow Start as a load-balancing virtual-server setting and identifies its supported load-balancing methods in the virtual-server configuration guidance. See the Citrix ADC load-balancing advanced settings documentation and the Citrix ADC LB vServer command reference.

QUESTION NO: 18

Scenario: A Citrix Architect has deployed two MPX devices, 12.0.53.13 nc and MPX 11500 models, in a high availability (HA) pair for the Workspace labs team. The deployment method is two-arm. and the devices are installed behind a CISCO ASA 5585 firewall. The architect enables the following features on the Citrix ADC devices: Content Switching. SSL Offloading, Load Balancing, Citrix Gateway, Application Firewall in hybrid security, and Appflow. All are enabled to send monitoring information to Citrix Application Delivery Management 12.0.53.13 nc build. The architect is preparing to configure load balancing for Microsoft Exchange 2016 server.

The following requirements were discussed during the implementation:

All traffic needs to be segregated based on applications, and the fewest number of IP addresses should be utilized during the configuration.
All traffic should be secured, and any traffic coming into HTTP should be redirected to HTTPS.
Single Sign-on should be created for Microsoft Outlook web access (OWA).
Citrix ADC should recognize Uniform Resource Identifier (URI) and close the session to Citrix ADC, when users hit the Logoff button in Microsoft Outlook web access.
Users should be able to authenticate using user principal name (UPN).
The Layer 7 monitor should be configured to monitor the Microsoft Outlook web access servers, and the monitor probes must be sent on SSL.

Which Responder policy can be utilized to redirect the users from http://mail.citrix.com to https://mail.citrix.com/owa ?

A. add responder action Act redirect "\"https://mail.citrix.com/owa/\"" -responseStatusCode 302
add responder policy pol "HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/\")" Act

B. add responder action Act redirect "\"https://mail.citrix.com/owa/\"" -responseStatusCode 307
add responder policy pol "HTTP.REQ.IS_NOTVALID" Act

C. add responder action Act redirect "\"http://mail.citrix.com/owa/\"" -responseStatusCode 302
add responder policy pol "HTTP.REQ.IS_NOTVALID" Act

D. add responder action Act redirect "\"http://mail.citrix.com/owa/\"" -responseStatusCode 302
add responder policy pol "HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/\")" Act

ANSWER: A

Explanation:

The responder configuration that redirects the root request to `https://mail.citrix.com/owa/` with an HTTP 302 response is correct. The responder policy expression `HTTP.REQ.URL.PATH_AND_QUERY.EQ("/")` matches a request for the site root. When this policy is bound to the HTTP virtual server that receives requests for `mail.citrix.com`, the matching request invokes the redirect action and sends the client to the HTTPS OWA path. This provides the required transition from the unsecured HTTP entry point to the secured HTTPS OWA endpoint while keeping the redirect narrowly scoped to users who browse to the root URL.

A responder action supports a redirect target and a configurable HTTP response status code. A 302 redirect is appropriate for this access redirection use case because the client is instructed to retrieve the requested resource from the specified HTTPS URL. The redirect target must explicitly use the `https` scheme and include `/owa/`, ensuring that users reach the Outlook on the web application rather than merely changing protocol at the root path. Citrix documents responder actions and policies, including redirect actions and request-expression evaluation, at Citrix ADC Responder documentation and Citrix ADC policy infrastructure documentation.

QUESTION NO: 19

Scenario: A Citrix Architect needs to conduct a capabilities assessment for an organization that wants to create a new Citrix ADC deployment. One of the

organization's core business drivers is to ensure that key applications are always available to users.

Which capabilities must the architect verify to assess if the requirement is feasible with the current infrastructure?

A. Undocumented environment

B. issues image management processes

C. Disaster recovery and implementation

D. Training and certification of support staff and end users

E. Current Active Directory and DNS environment

ANSWER: C

Explanation:

Disaster recovery and implementation is correct because continuous application availability requires the architect to establish whether the existing infrastructure can support resilient Citrix ADC service delivery during both localized failures and wider site-level outages. The assessment should determine whether a workable recovery design can be implemented, including the availability of alternate sites, adequate network connectivity between sites, appropriate routing and DNS capabilities, and operational processes for failover and recovery. Citrix ADC high availability provides redundancy for an appliance or instance failure within a deployment, while Global Server Load Balancing can direct users to healthy application services across geographically separate data centers. These capabilities depend on the surrounding infrastructure being able to support the required health monitoring, traffic steering, state synchronization, and recovery design. Verifying disaster-recovery readiness and the practical ability to implement the design therefore directly tests whether the organization can meet its stated availability objective, rather than merely defining a desired architecture. Citrix documents high-availability behavior and requirements at Citrix ADC high availability, and describes cross-site application availability with GSLB at Citrix ADC Global Server Load Balancing.

QUESTION NO: 20

Scenario: A Citrix Architect has setup 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 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 **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?

A. Configure HTML SQL injection check on Application Firewall and enable Transform SQL special characters.

B. Configure signatures manually and apply them to the Application Firewall profile.

C. Configure HTML SQL Injection check on Application Firewall and enable Block SQLSplCharANDKeyword.

D. Configure HTML cross-Site scripting and enable Check Request headers.

ANSWER: A

Explanation:

Configure HTML SQL injection check on Application Firewall and enable Transform SQL special characters. is correct because it directly addresses the stated requirement to handle SQL-significant characters before potentially malicious input reaches backend servers. Citrix ADC Application Firewall's SQL injection protection inspects request components, including HTML form fields, URL query parameters, cookies, and headers, for SQL injection patterns. When the HTML SQL injection check is enabled, the appliance can apply the configured SQL-injection protections to HTML-form input. Enabling transformation of SQL special characters causes characters commonly used in SQL-injection payloads, such as quotation marks, backslashes, and semicolons, to be safely transformed rather than passed unchanged to the protected application. This provides an appropriate control when the requirement explicitly permits transforming, blocking, or dropping these characters on requests sent to the backend. The check operates as part of the Application Firewall profile associated with the protected virtual server, allowing the policy to be applied consistently to inbound web traffic. Citrix documents SQL injection checks and actions, including transformation of SQL special characters, in its Application Firewall guidance: Citrix ADC SQL injection protection. Additional Application Firewall configuration context is available in the Citrix ADC Application Firewall documentation.