PassQueen
a.k.a dumpsqueen.com

Deploy and Manage Citrix ADC 13 with Citrix Gateway

Citrix 1Y0-231

Version Demo

Total Demo Questions: 9

Total Premium Questions: 98

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Citrix ADC Platforms	9
Topic 2, Citrix ADC Traffic Management	25
Topic 3, Citrix ADC Security	13
Topic 4, Citrix ADC System Maintenance	19
Topic 5, Citrix Gateway	32
Total	98

QUESTION NO: 1

Scenario: A Citrix ADC MPX is using one of four available 10G ports. A Citrix Administrator discovers a traffic bottleneck at the Citrix ADC.

What can the administrator do to increase bandwidth on the Citrix ADC?

A. Add two more 10G Citrix ADC ports to the network and configure VLAN.

B. Add another 10G Citrix ADC port to the switch, and configure link aggregation control protocol (LACP).

C. Purchase another Citrix ADC MPX appliance.

D. Plug another 10G Citrix ADC port into the router.

ANSWER: B

Explanation:

Add another 10G Citrix ADC port to the switch, and configure link aggregation control protocol (LACP). This creates a link aggregation channel that combines multiple physical interfaces into one logical channel. With two 10-Gbps links in the channel, the Citrix ADC can distribute eligible traffic flows across both member interfaces, increasing the available aggregate bandwidth between the appliance and the connected switch while retaining a single logical network connection.

LACP is the standards-based protocol used to dynamically negotiate and maintain the aggregated link with the switch. It also provides resiliency: if one member link fails, traffic can continue over the remaining active member, subject to its available capacity. The switch ports must be configured as members of the same LACP port channel, and the Citrix ADC interfaces must be added to an LACP channel with compatible settings. Traffic distribution is flow-based, so an individual flow is normally carried by one member interface, while multiple concurrent flows can use the aggregate capacity.

Citrix documents link aggregation as a method for increasing bandwidth and providing network-interface redundancy on Citrix ADC appliances. See Citrix ADC documentation: Configuring link aggregation and Citrix ADC networking interfaces documentation.

QUESTION NO: 2

Which type of policy would a Citrix Administrator use to disable USB redirection?

A. Session

B. SmartControl

C. Auditing

D. Authorization

ANSWER: B

Explanation:

SmartControl is the correct policy type because Citrix Gateway SmartControl applies granular ICA-session restrictions according to contextual access decisions made at the Gateway. A SmartControl policy can be used to control Citrix Virtual Apps and Desktops session capabilities for users connecting through Citrix Gateway, including whether USB device redirection is available. This lets an administrator prevent endpoint USB devices from being redirected into the delivered application or desktop when a session meets the policy's assigned conditions, such as the user, group, client endpoint, or access scenario.

SmartControl is designed for this kind of fine-grained session security enforcement. Citrix Gateway communicates the applicable SmartControl settings as part of the ICA connection process, allowing the Citrix session to honor the restriction without requiring an administrator to create a separate desktop-delivery design solely for that access condition. Disabling USB redirection through SmartControl is therefore useful when organizations must protect sensitive resources from removable media and unmanaged peripheral devices while still providing authorized remote access. Citrix documents

SmartControl as a Citrix Gateway feature for applying ICA-proxy session controls: Configure SmartControl. Additional Citrix Gateway product documentation is available at Citrix Gateway documentation.

QUESTION NO: 3

A Citrix Administrator needs to provide access to Microsoft SharePoint through Citrix Gateway for users connecting from a web browser using the Citrix Gateway plug-in.

How can the administrator configure this?

A. Configure Citrix Gateway in ICA proxy mode.

B. Set clientless access to OFF.

C. Enable SSL bridge mode.

D. Set clientless access to ON.

ANSWER: D

Explanation:

Set clientless access to ON. Citrix Gateway clientless access is designed to publish internal web applications through the Gateway portal, allowing authenticated users to reach supported web resources such as Microsoft SharePoint from a web browser. When clientless access is enabled in the session profile or through the applicable session policy, Citrix Gateway presents the resources and proxies browser requests to the internal SharePoint site. This maintains the external user's connection through Citrix Gateway while avoiding a need to publish SharePoint as an ICA-delivered application.

The setting is applied as part of the user session configuration, so the administrator should ensure that the session policy/profile bound to the relevant users has clientless access enabled and that the SharePoint resource is available through the configured portal or bookmark/resource configuration. Citrix Gateway can then enforce authentication and any associated authorization controls before users access SharePoint. Citrix documents clientless access as the Gateway capability for providing browser-based access to internal web applications and describes its configuration in the Gateway documentation: Configure clientless access. Additional Citrix Gateway configuration guidance is available at Citrix Gateway documentation.

QUESTION NO: 4

Which four steps should a Citrix Administrator take to configure SmartAccess? (Choose four.)

A. Execute "Set-BrokerSite -TrustRequestsSentToTheXMLServicePort $True" on any Citrix Delivery Controller in the Site.

B. Enable Citrix Workspace control within StoreFront.

C. Ensure that the SmartAccess filter name on the Delivery Group matches the name of the Citrix Gateway virtual server.

D. Ensure that the SmartAccess filter name on the Delivery Group matches the name of the Citrix Gateway policy.

E. Ensure that ICA Only is unchecked on the Citrix Gateway virtual server.

F. Ensure that the Callback URL is defined in the Citrix Gateway configuration within Store Front.

G. Ensure that ICA Only is checked on the Citrix Gateway virtual server.

ANSWER: A C E F

Explanation:

SmartAccess lets Citrix Virtual Apps and Desktops apply Delivery Group access-control filters based on the Citrix Gateway virtual server through which a user connected. The Delivery Controller must be configured to trust requests sent to the XML service port by running `Set-BrokerSite -TrustRequestsSentToTheXMLServicePort $True`. This permits the

Controller to accept the SmartAccess-related information supplied through the Gateway/XML integration. The SmartAccess filter configured for a Delivery Group must exactly match the Citrix Gateway virtual-server name, allowing the Delivery Group's access policy to identify the applicable Gateway connection.

The Citrix Gateway virtual server must have ICA Only cleared so that SmartAccess information can be passed with the connection rather than limiting the virtual server to ICA proxy behavior. StoreFront must also have the Citrix Gateway callback URL defined in its Gateway configuration. The callback mechanism enables StoreFront to communicate with Citrix Gateway for user-session validation and supports the required Gateway integration. Together, these settings establish the trusted XML communication, the Gateway identity used by Delivery Group filtering, and the StoreFront-to-Gateway callback path required for SmartAccess. See Citrix CTX227055 and Citrix SmartAccess documentation.

QUESTION NO: 5

A Citrix Administrator wants Citrix Application Delivery Management (ADM) to receive application-traffic information from a managed Citrix ADC instance by using AppFlow.

Which two Citrix ADC components should the administrator configure? (Choose two.)

A. An AppFlow collector that identifies Citrix ADM

B. An AppFlow action that references the collector

C. An SSL server certificate bound to each backend service

D. A GSLB site for the ADM instance

E. A traffic domain for AppFlow records

ANSWER: A B

Explanation:

An AppFlow collector that identifies Citrix ADM and **an AppFlow action that references the collector** are correct. The AppFlow collector specifies the destination to which the Citrix ADC exports AppFlow records. The AppFlow action uses that collector and defines the records or information to export.

After the action is associated with an AppFlow policy and the policy is bound at the appropriate traffic-processing point, Citrix ADC can export the configured data to ADM for analytics. The selected policy expression determines which traffic is exported. Citrix documents AppFlow configuration and its use with Citrix ADM in the Citrix ADC AppFlow documentation.

QUESTION NO: 6

Scenario: A Citrix Administrator needs to create local, limited-privilege user accounts for other administrators. The other administrators will require only:

- The ability to enable and disable services and servers
- Read-only access

Which built-in command policy permission level can the administrator use?

A. Read-only

B. Operator

C. Sysadmin

D. Network

ANSWER: B

Explanation:

Operator is the appropriate built-in command-policy permission level because it is intended for administrators who must perform limited operational tasks without receiving unrestricted configuration privileges. In particular, the operator role allows a user to enable and disable configured services and servers, which supports routine monitoring, maintenance, and incident-response work performed by operations staff. It also includes read-only access for viewing the appliance configuration and operational state, allowing those administrators to inspect relevant settings and status before taking an approved action.

This role follows least-privilege administration: it grants access needed to operate existing load-balancing objects while avoiding the broad administrative control associated with full system administration. A Citrix ADC administrator can create a local user, assign the built-in operator command policy, and thereby provide a consistent permission set without individually defining every permitted command. Citrix ADC authorization is based on command policies, and built-in policies provide predefined levels for common administrative responsibilities. See the Citrix documentation on user configurations and authorization and the configuration of local users.

QUESTION NO: 7

In a single-hop deployment, a Citrix Administrator needs to use a client's IP address as the source IP address for Citrix ADC-to-server connections.

Which Citrix ADC mode can the administrator use to meet this requirement?

A. USIP

B. USNIP

C. Layer 2

D. Layer 3

ANSWER: A

Explanation:

USIP is the appropriate Citrix ADC mode because it instructs the appliance to use the original client IP address as the source address for connections that it opens to backend servers. In a single-hop topology, the servers can route responses back through the Citrix ADC, allowing the appliance to remain in the traffic path while the backend application sees the actual client address at the network layer. This is useful when an application, server-side access-control list, or audit process requires the client IP address rather than a Citrix ADC-owned address as the connection source.

USIP is enabled globally through the Citrix ADC command-line interface with the `set ns mode USIP ON` command. Because source-address preservation affects server return traffic, the administrator should ensure that the relevant backend-server routing design supports return packets traversing the appliance. Citrix documents USIP as a mode in which the appliance uses the client IP address for connections to servers, and its direct-routing guidance describes the associated traffic-flow and routing considerations. See the Citrix ADC modes of operation documentation and Citrix guidance for load balancing with direct routing.

QUESTION NO: 8

A Citrix Administrator wants to configure a secure SSL profile for an Internet-facing load-balancing virtual server.

Which two configuration changes improve the security of the virtual server? (Choose two.)

A. Disable TLSv1.

B. Bind a cipher group containing approved strong ciphers.

C. Enable SSLv3.

D. Enable RC4 cipher suites.

E. Use a self-signed certificate for public users.

ANSWER: A B

Explanation:

Disable TLSv1 and **bind a cipher group containing approved strong ciphers** are correct. Disabling TLSv1 removes an obsolete protocol version from client negotiation. A cipher group allows the administrator to define and apply an approved set of cryptographic ciphers consistently to the virtual server.

SSL profiles provide reusable settings for protocol versions, cipher groups, and other SSL parameters. The administrator should validate required client compatibility before disabling older protocols. See the Citrix ADC SSL profiles documentation.

QUESTION NO: 9

A Citrix Administrator is configuring Citrix Gateway for ICA proxy access to a Citrix Virtual Apps and Desktops deployment.

Which two configurations are required for StoreFront and Citrix Gateway to communicate with the Secure Ticket Authority (STA)? (Choose two.)

A. Configure the same STA server URLs in StoreFront.

B. Bind the STA servers to the Citrix Gateway virtual server.

C. Bind the StoreFront server certificate as a client certificate on Citrix Gateway.

D. Enable clientless access in the Citrix Gateway session profile.

E. Configure a RADIUS server as the Citrix Gateway authentication server.

ANSWER: A B

Explanation:

Configure the same STA server URLs in StoreFront and **bind the STA servers to the Citrix Gateway virtual server** are correct. StoreFront requests STA tickets during resource launch, and Citrix Gateway validates those tickets when the user establishes the ICA connection. Both components must reference the same STA servers so that tickets issued by StoreFront can be validated by Citrix Gateway.

The STA URLs normally identify the Citrix Virtual Apps and Desktops Delivery Controllers that provide the STA service. The URLs must be reachable from the relevant components and configured consistently. A callback URL supports specific Gateway and StoreFront integration scenarios, but it does not replace the STA configuration required for ICA proxy ticket validation. See the StoreFront and Citrix Gateway integration documentation and the Citrix Gateway ICA proxy documentation.