DUMPSBOSS.

Citrix Virtual Apps and Desktops 7 Administration exam

Citrix 1Y0-204

Version Demo

Total Demo Questions: 25

Total Premium Questions: 255

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Initial Configuration	52
Topic 2, Citrix Virtual Apps and Desktops Site Configuration	22
Topic 3, Providing Access to Resources	68
Topic 4, Delivering App and Desktop Resources	31
Topic 5, Maintaining a Citrix Virtual Apps and Desktops Site	27
Topic 6, Troubleshooting Citrix Virtual Apps and Desktops	26
Topic 7, Mix Questions	29
Total	255

QUESTION NO: 1

Scenario: A Citrix Administrator is configuring load balancing on a Citrix ADC appliance for the company web servers. The administrator needs to create a custom monitor that will look for a specific keyword response from the website and will be used to keep the services in an UP state.

Which type of monitor can the administrator create to accomplish this scenario?

A. HTTP-ECV monitor with the keyword in the Special Parameters – Receive String field.

B. A HTTP monitor with the keyword in the Special Parameters – Response Codes field.

C. A TCP monitor with the keyword in the Special Parameters – Response Code field.

D. An UDP-ECV monitor with the keyword in the Special Parameters – Receive String field.

ANSWER: A

Explanation:

HTTP-ECV monitor with the keyword in the Special Parameters – Receive String field is correct because ECV (Extended Content Verification) monitors validate application content, rather than merely confirming that a network port is available or that an HTTP transaction completes. For an HTTP-ECV monitor, the Citrix ADC appliance sends an HTTP request to the monitored web service and evaluates the response against the configured receive string. When the expected keyword appears in the response, the monitor regards the service as healthy and can maintain its UP state for load-balancing decisions.

This is appropriate when the administrator needs to verify that the web application is returning a known page element, status text, or other expected content that demonstrates the site is functioning as intended. The receive string can be a literal text value or a regular expression, enabling checks ranging from a simple keyword to a more specific response pattern. Citrix ADC associates the monitor with the relevant service or service group, then uses its periodic probe results to determine service availability. Citrix documents ECV monitors and their receive-string content-validation capability in its load-balancing monitor documentation and provides monitor configuration guidance in CTX209292.

QUESTION NO: 2

Which layer can optionally be managed by Citrix Cloud, when designing Citrix Cloud architecture?

A. Access

B. Hardware

C. Resource

D. Control

ANSWER: A

Explanation:

The **Access** layer can optionally be managed by Citrix Cloud. This layer provides the secure user entry point to Citrix resources and commonly includes Citrix Workspace, StoreFront, and Citrix Gateway functionality. In a Citrix Cloud deployment, an organization can choose Citrix-managed access services, such as Citrix Workspace and Citrix Gateway service, rather than operating all access infrastructure itself. This reduces the need to deploy, maintain, patch, scale, and make externally available customer-managed Gateway and StoreFront components for supported use cases.

This is an architectural choice because organizations can also retain customer-managed access components where their network design, authentication requirements, security policy, or existing infrastructure calls for them. Citrix Cloud therefore supports flexibility at the user-access boundary while maintaining secure connectivity to resources through Cloud Connectors and resource locations. Citrix documents Citrix Gateway service as a cloud-hosted service that provides secure remote access without requiring a customer-managed Citrix Gateway appliance or virtual machine. Citrix Workspace also provides a cloud-hosted aggregation experience for users. See Citrix Gateway service documentation and Citrix Workspace documentation.

QUESTION NO: 3

Scenario: A Citrix Administrator is configuring a StoreFront store for users who connect from both the internal network and the Internet through Citrix Gateway.

Which two StoreFront beacon types should the administrator configure to allow Citrix Workspace app to detect whether users are internal or external? (Choose two.)

A. Internal beacons

B. External beacons

C. Secure Ticket Authority beacons

D. XML Service beacons

E. Delivery Controller beacons

ANSWER: A B

Explanation:

Internal beacons are addresses that Citrix Workspace app can reach only when the endpoint is connected to the internal corporate network. When an internal beacon can be contacted, Workspace app identifies the connection as internal and can use the internal access path.

External beacons are addresses that can be reached from outside the corporate network. When the internal beacon is not reachable but an external beacon is reachable, Workspace app identifies the connection as external and uses the configured Citrix Gateway access path. This detection helps ensure that users receive the appropriate connection method without manually selecting an internal or external store configuration.

Secure Ticket Authority and XML Service addresses are required for other parts of the Citrix access architecture, but they are not StoreFront beacon types. Citrix documents beacon configuration in the StoreFront beacon configuration documentation.

QUESTION NO: 4

A Citrix Administrator is in the process of installing Citrix Cloud Connector, but the installation fails.

What could be causing the Citrix Cloud Connector installation to fail on the machine?

A. It is in sync with UTC time instead of local time.

B. Enhanced Security Configuration (ESC) is set to 'off'.

C. It cannot run on a machine template cloned across multiple machines.

D. It is NOT joined to the domain.

ANSWER: D

Explanation:

It is NOT joined to the domain is correct because a Citrix Cloud Connector must be installed on a machine that is joined to an Active Directory domain. The connector acts as the secure communications channel between the Citrix Cloud control plane and resources in the customer-managed resource location, including Active Directory, Virtual Delivery Agents, and other infrastructure services. Domain membership enables the Connector to use the required domain context and to communicate properly with the Active Directory environment it supports.

Before installing the Connector, the administrator should confirm that the computer is joined to the intended domain, can resolve and communicate with the domain controllers, and is not itself a domain controller. The machine should also meet the supported operating-system and connectivity requirements, including outbound HTTPS access to Citrix Cloud endpoints.

Joining the server to the domain and verifying its domain trust and DNS configuration are therefore appropriate initial remediation steps when an installation fails under these circumstances.

Citrix documents the domain-joined-machine prerequisite in its Cloud Connector system requirements and provides installation guidance in the Cloud Connector installation documentation.

QUESTION NO: 5

What information from the Citrix License Server does a Citrix Administrator need in order to allocate the Citrix Virtual Desktops license file from the Citrix.com account?

A. IP address

B. FQDN

C. MAC address

D. Hostname

ANSWER: D

Explanation:

Hostname is the required License Server information when allocating a Citrix Virtual Desktops license file from the Citrix account. Citrix generates the license file for a specific License Server by associating the allocation with that server's hostname. The administrator obtains this value from the License Administration Console or directly from the server's operating system, then enters it during the allocation workflow in the Citrix licensing portal.

This hostname-based association is important because the downloaded license file is intended for the identified License Server. After allocation, the administrator installs the file on that server through the License Administration Console, allowing the License Server to make the entitled Citrix Virtual Desktops licenses available to the Citrix environment. Care should be taken to enter the hostname exactly as reported by the License Server, because a hostname change can require the license file to be reallocated or replaced. Citrix documents the process of obtaining and allocating license files, including the License Server details used by the portal, in its licensing documentation: Obtain a license file and Citrix Licensing documentation.

QUESTION NO: 6

A Citrix Engineer recently upgraded the environment from CVAD 2203 LTSR to CVAD 2402 LTSR and created multiple policy sets. How many policy sets can be assigned to a single Delivery Group?

A. One

B. None

C. Depends on the policy set type

D. Multiple

ANSWER: A

Explanation:

One is correct. In Citrix Virtual Apps and Desktops 2402 LTSR, policy sets provide a way to organize related Citrix policies and associate that collection with Delivery Groups. A policy set itself can be assigned to more than one Delivery Group, which helps administrators consistently apply a defined policy configuration across workloads. However, each individual Delivery Group can have only one policy set assigned to it. This creates a clear ownership relationship for the Delivery Group's policy-set assignment and avoids ambiguity when Citrix determines which grouped policy configuration applies.

Administrators can still use the policies contained in the assigned policy set to configure settings and can use normal Citrix policy processing concepts, such as policy priority and filters, when designing the effective configuration for users and machines. The limitation concerns the number of *policy sets* directly associated with a given Delivery Group, rather than the

number of individual policies that may be organized within that set. This behavior is documented in Citrix's policy-set administration guidance for the 2402 LTSR release. See Citrix policy configuration documentation and the CVAD 2402 LTSR documentation.

QUESTION NO: 7

What are three valid ways to configure Virtual Delivery Agent (VDA) registration? (Choose three.)

A. CONFI

B. Group Policy Object (GPO)

C. Organizational Unit (OU) based Controller discovery

D. DHCP Options

E. MCS-based PERSONALITY.INI

ANSWER: B C E

Explanation:

Group Policy Object (GPO), Organizational Unit (OU) based Controller discovery, and MCS-based PERSONALITY.INI are valid VDA registration configuration methods. A GPO can centrally apply the Controllers policy setting to VDAs, specifying the Delivery Controllers with which each VDA should register. This is a scalable approach because the policy can be managed through Active Directory and updated without manually editing each VDA.

OU-based Controller discovery is an Active Directory-based method in which VDAs discover the appropriate Controllers from the organizational unit structure. It is supported for environments that use this established Active Directory discovery design.

For Machine Creation Services deployments, the `PERSONALITY.INI` file is used during machine personalization. MCS can supply Controller registration information through this file as the cloned machine is initialized, allowing provisioned VDAs to obtain the correct registration configuration. These methods enable VDAs to locate and register with the Delivery Controller infrastructure used by the site. Citrix documents Controller discovery and registration configuration in its VDA registration documentation and covers MCS provisioning behavior in the Machine Creation Services documentation.

QUESTION NO: 8

Which Front-End Optimization (FEO) action can a Citrix Administrator use to achieve the results shown in the screenshots?

Cick the Exhibit button to view the screenshots.

A. Truncate CSS

B. Inline CSS

C. Move CSS to head

D. Rearrange CSS

ANSWER: B

Explanation:

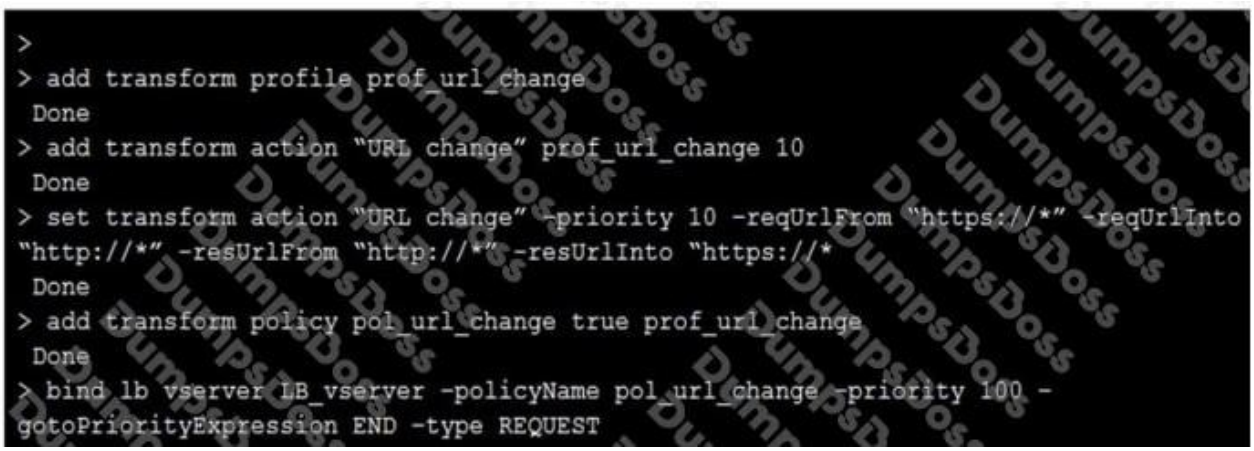
Inline CSS is the appropriate Front-End Optimization action when the desired result is to place style rules that were previously obtained through an external stylesheet directly into the HTML document. By embedding the CSS in a `<style>` block or applicable HTML elements, the browser can obtain the required styling as part of the initial page response instead of issuing a separate request for the stylesheet. This can reduce request overhead and help the browser render content sooner, particularly for small stylesheets or CSS needed immediately for the page's initial display.

Citrix ADC Front-End Optimization includes an Inline CSS action specifically for this purpose. The action rewrites eligible CSS references in server responses and inserts CSS content into the delivered page, subject to the configured FEO policy and the response being suitable for optimization. The visual difference shown by an external CSS resource being represented within the page source is therefore consistent with applying Inline CSS. Administrators should validate the result with browser developer tools and ensure that caching and page-size considerations are appropriate for the application. Citrix documents FEO configuration and its available optimization actions in the Citrix ADC Front-End Optimization documentation and the Citrix ADC optimization documentation.

QUESTION NO: 9

A Citrix Administrator has executed the commands in the screenshot on the Citrix ADC using the command-line interface.

Click on the 'Exhibit' button to view the screenshot of the command-line interface.



Which two replacements will be the outcome of executing these commands? (Choose two.)

A. https:// will be replaced by http:// in the HTTP REQUEST

B. http:// will be replaced by https:// in the HTTP REQUEST

C. http:// will be replaced by https:// in the HTTP RESPONSE

D. https:// will be replaced by http:// in the HTTP RESPONSE

ANSWER: A D

Explanation:

The commands create rewrite actions that operate in two different traffic-flow contexts: one action evaluates the HTTP request and the other evaluates the HTTP response. The request-side replacement searches the applicable request expression for the literal secure protocol prefix and substitutes the nonsecure protocol prefix. Consequently, text containing `https://` is changed to `http://` while Citrix ADC processes the HTTP request. The response-side replacement similarly applies its search-and-replace operation in the response context, changing occurrences of `https://` to `http://` in the HTTP response content selected by the configured expression. These outcomes follow from the direction-specific Citrix ADC advanced policy expressions used by rewrite actions: `HTTP.REQ` expressions inspect or modify client requests, whereas `HTTP.RES` expressions inspect or modify server responses. A rewrite action does not automatically perform the reverse conversion or apply the same action to both directions; its configured expression and replacement strings determine both the traffic direction and the exact substitution. Citrix documents rewrite policies and actions in its Application Delivery Management guidance at Citrix ADC Rewrite. The expression namespaces and HTTP request/response processing model are described in the Citrix ADC rewrite action API reference.

QUESTION NO: 10

Which qualifier is used to configure the Content filter action to modify the HTTP header of an HTTP Request?

A. Corrupt

B. Forward

C. Add

D. Error Code

ANSWER: C

Explanation:

Add is the correct qualifier because the Citrix ADC content-filtering `ADD` action inserts a specified string into an HTTP request or response. When the inserted string is formatted as an HTTP header, the action modifies the request header before the request is sent onward to the target server. This is useful when a policy needs to add information such as a custom header, an identifier, or another header value that an upstream application requires.

Content filtering actions are configured with an action type and, for an insertion action, the string to add. The policy determines the traffic to which the action applies, while the `ADD` action supplies the header content that Citrix ADC inserts into the matching HTTP request. Header syntax must be valid, including the header name, colon, value, and appropriate line termination where required by the configuration context. Citrix documents `ADD` as an action type for inserting content in HTTP messages, including headers. See the Citrix ADC content-filtering action configuration documentation and the Citrix ADC HTTP header insertion documentation.

QUESTION NO: 11

A Delivery Group has been created to publish APP_A, APP_B, and APP_C to an Active Directory group called “HR.” There are 10 users in the group (HR1–HR10).

It was discovered that one specific user, **HR10** , should not be allowed to access **APP_A** .

How can the administrator ensure HR group members can access all assigned apps, but HR10 is excluded from APP_A?

A. Remove HR10 from the Delivery Group

B. Limit Visibility on APP_A to HR1–HR9

C. Remove APP_A from the Delivery Group

D. Limit visibility on APP_A to HR10

ANSWER: B

Explanation:

Limit Visibility on APP_A to HR1–HR9 is correct because Citrix Virtual Apps and Desktops supports restricting an individual published application to a subset of the users assigned to its Delivery Group. The Delivery Group can remain assigned to the existing HR Active Directory group, preserving access to the group’s other published resources, while APP_A receives a more specific visibility assignment. Configuring APP_A’s visibility for HR1 through HR9 means those users can enumerate and launch the application, whereas HR10 remains entitled to the Delivery Group but does not receive APP_A.

In Citrix Studio, application properties include user-visibility controls that allow administrators to limit an application to selected users or groups. In a production environment, the most maintainable implementation is often to use an Active Directory security group containing the intended APP_A users, rather than selecting numerous individual accounts. This provides a clear separation between Delivery Group entitlement and application-level entitlement, and future membership changes can be managed in Active Directory without redesigning the Delivery Group.

Citrix documents that applications can be assigned to users and groups associated with the Delivery Group and that visibility can be limited at the application level. See Citrix documentation: Manage applications and Citrix documentation: Delivery Groups.

QUESTION NO: 12

What are three valid ways to configure Virtual Delivery Agent (VDA) registration? (Choose three.)

A. CONFIG.XML file

B. Group Policy Object (GPO)

C. Organizational Unit (OU) based Controller discovery

D. DHCP Options

E. MCS-based PERSONALITY.INI

ANSWER: B C E

Explanation:

Group Policy Object (GPO), **Organizational Unit (OU) based Controller discovery**, and **MCS-based PERSONALITY.INI** are supported mechanisms for supplying a VDA with the information needed to locate and register with Delivery Controllers. A Citrix policy configured through a Group Policy Object can set the Controller list for applicable VDAs, providing centralized and consistent registration configuration. OU-based Controller discovery supports discovering Controllers associated with the Active Directory organizational-unit hierarchy, reducing the need to explicitly maintain Controller names on each VDA. For Machine Creation Services deployments, the PERSONALITY.INI file is generated and used during provisioning so that cloned machines receive deployment-specific registration information, including Controller details, when they start.

These mechanisms address distinct deployment and administration scenarios: policy-based configuration for centrally managed machines, Active Directory–based discovery for appropriate domain designs, and Machine Creation Services provisioning for pooled or catalog-created workloads. Citrix documents Controller discovery and VDA registration configuration, including policy, registry, and provisioning-related methods, in its VDA registration guidance. See Citrix VDA registration and Citrix VDA installation and configuration.

QUESTION NO: 13

Scenario: A Citrix Administrator has made changes to the master image used by an MCS machine catalog. The administrator needs the changes to be applied to the non-persistent machines in the catalog.

Which two actions should the administrator take? (Choose two.)

A. Create a snapshot of the updated master image.

B. Update the machine catalog and select the new snapshot.

C. Create a new Delivery Group for the updated machines.

D. Delete and recreate the machine catalog.

E. Install a new Virtual Delivery Agent (VDA) on every catalog machine.

ANSWER: A B

Explanation:

The administrator should first **create a snapshot of the updated master image**. Machine Creation Services uses the selected snapshot as the source from which it creates or updates the catalog image. The snapshot provides a fixed, identifiable version of the master image that can be selected during the catalog update process.

The administrator must then **update the machine catalog and select the new snapshot**. Updating the catalog creates the required updated disks for the catalog machines and applies the image according to the selected rollout option. For non-persistent machines, the updated image is used after the machines are restarted or otherwise refreshed as part of the update process.

Creating a new Delivery Group or recreating the catalog is not required merely to deliver an updated master image. Citrix documents catalog image updates in the Machine Catalog update documentation.

QUESTION NO: 14

Scenario: A Citrix Administrator is configuring the Citrix Workspace app to allow users to access their applications and desktops. Management requires users to be logged on to the Citrix Workspace app without entering their credentials and for sessions to be pre-launched in the background for expedited application access.

Which experience does the administrator need to configure for users in this environment?

A. Citrix Workspace app for Windows

B. Citrix Workspace for Web

C. Citrix Workspace app for Universal Windows Platform

D. Citrix Workspace app for HTML5

ANSWER: A

Explanation:

Citrix Workspace app for Windows is correct because it supports both domain pass-through authentication and the prelaunch capability required by the scenario. Domain pass-through lets the Workspace app use the credentials from a user's Windows sign-in, so users can authenticate to Citrix resources without manually entering credentials again. This requires the appropriate Citrix Workspace app configuration, such as enabling pass-through authentication and configuring the relevant trusted sites, policies, and StoreFront or Gateway authentication settings.

The Windows Workspace app also supports prelaunch, which establishes a session before the user explicitly starts a published app or desktop. When the user subsequently opens an entitled resource, the existing prelaunched session can reduce perceived startup time. Administrators configure prelaunch through Citrix policies and must ensure that the published resources and delivery environment are configured to permit it. Citrix documents domain pass-through support in its Workspace app for Windows authentication documentation and describes session prelaunch configuration in its session prelaunch documentation.

QUESTION NO: 15

Scenario: A Citrix Administrator is configuring a Citrix ADC high availability (HA) pair with an existing Primary Citrix ADC with all resources configured. The administrator added the Secondary Citrix ADC in high availability and found that the configuration on the existing primary was removed. It is now the Secondary Citrix ADC in the HA pair. Which two configurations could the administrator have made to prevent this from happening? (Choose two.)

A. Enable HA monitoring on all the interfaces of the SECONDARY device.

B. Set the Secondary Citrix ADC to STAY SECONDARY in the Configure HA Node settings.

C. Set the Primary Citrix ADC to STAY PRIMARY in the Configure HA Node settings.

D. Enable HA monitoring on all the interfaces of the PRIMARY device.

ANSWER: B C

Explanation:

Setting the Primary Citrix ADC to STAY PRIMARY in the Configure HA Node settings explicitly pins the appliance that already contains the production configuration in the primary role. This avoids an unexpected role change during HA formation or subsequent HA state evaluation. The primary node is the authoritative source for configuration synchronization in an HA pair; therefore, preserving its primary role ensures that its existing configuration remains the configuration replicated to the peer rather than being replaced by a peer's configuration.

Setting the Secondary Citrix ADC to STAY SECONDARY in the Configure HA Node settings provides the complementary protection. It prevents the newly added appliance from assuming the primary role while the HA pair is being established. Using both role-persistence settings makes the intended authority explicit: the configured appliance remains primary and the newly introduced appliance remains secondary, allowing normal configuration synchronization from the established primary to the secondary node.

Citrix documents the *Stay Primary* HA setting as the mechanism for forcing the intended appliance to retain the primary role. The HA node configuration also supports setting the peer to remain secondary, which is appropriate when adding an unconfigured or nonauthoritative appliance to an existing deployment. See Citrix ADC: Force the primary node to stay primary and Citrix ADC high availability documentation.

QUESTION NO: 16

A customer is using Citrix Virtual Apps and Desktops 2402 LTSR. What will happen when a client-side printer is added or removed while a Citrix HDX session is active?

A. The session remains unaffected by changes to client-side printers

B. Users will need to manually update their printer list in the session

C. The system dynamically adjusts in-session auto-created printers to reflect the changes in client-side printers

D. The system will not adjust in-session auto-created printers based on client-side printer changes

ANSWER: C

Explanation:

The system dynamically adjusts in-session auto-created printers to reflect the changes in client-side printers. Citrix client printer redirection uses the HDX printing virtual channel to communicate printer information from the endpoint to the VDA. With dynamic printer discovery enabled, Citrix can detect a client-side printer that becomes available after the session has started and make it available as an auto-created printer in that active session. Likewise, when a redirected client printer is removed from the endpoint, Citrix updates the session's redirected-printer inventory accordingly. This behavior lets users work with current endpoint printer availability without needing to end and recreate the HDX session merely to obtain an updated printer list. The setting is especially useful for endpoints where printers are connected, disconnected, installed, or removed during the workday. Administrators can govern client-printer creation and related printing behavior through Citrix policies, so the effective result in a production deployment remains subject to the applicable printing policy configuration. Citrix documents the architecture and management of client printer redirection in its Printing documentation, and lists the configurable controls in the printing policy settings reference.

QUESTION NO: 17

Which three components have settings that a Citrix Administrator can configure using Citrix policies? **(Choose three.)**

A. Citrix Workspace app

B. Citrix Profile Management

C. StoreFront

D. Citrix License Server

E. Delivery Controller

ANSWER: A B E

Explanation:

Citrix policies centrally control user-session behavior and are processed as part of the Citrix Virtual Apps and Desktops brokering and session-launch workflow. **Citrix Workspace app** is covered by policy settings that govern the user device and ICA session experience, including client drive mapping, clipboard behavior, audio, USB redirection, graphics, and bandwidth-related features. These settings allow administrators to standardize how published resources interact with endpoint devices.

Citrix Profile Management is also configured through Citrix policy settings. Administrators can define profile-store locations, profile streaming behavior, synchronization, folder exclusions, and other user-profile processing controls. These settings can be configured in Citrix Studio or through Active Directory Group Policy, depending on the deployment's policy-management approach.

The **Delivery Controller** participates in applying Citrix policy during connection brokering. The Controller retrieves the applicable policies for the user and machine, evaluates policy priority and filtering, and provides the resulting settings for the launched session. Citrix policy configuration therefore includes settings whose delivery and enforcement depend on Controller-based brokering and communication with the Virtual Delivery Agent.

For details, see Citrix documentation on Citrix policies and Profile Management configuration.

QUESTION NO: 18

For which three components can Citrix Director capture utilization statistics? (Choose three.)

A. CPU

B. IOPS

C. Disk space

D. Network

E. Memory

ANSWER: A B E

Explanation:

Citrix Director can capture utilization statistics for CPU, IOPS, and memory on monitored machines. These measurements provide administrators with a machine-level view of resource consumption while investigating user-session performance or machine health. CPU utilization indicates how much processor capacity is being consumed; memory utilization identifies pressure on physical RAM; and IOPS measures disk input/output operations, helping identify storage activity that can contribute to slow application launches, logons, or session responsiveness.

These metrics are collected through the Citrix monitoring infrastructure and presented in Director when the relevant monitoring capability and machine configuration are available. They are useful for correlating resource demand with session behavior and for drilling into process-level resource use where supported. Citrix describes Director's CPU, memory, and disk I/O monitoring capabilities in its article on CPU, memory usage, and process information. Current Citrix monitoring documentation also describes Director as the console for viewing performance and resource-utilization information for Citrix Virtual Apps and Desktops environments: Citrix Director documentation.

QUESTION NO: 19

What two options are limitations of a typical Global Server Load Balancing (GSLB) setup? (Choose two.)

A. An administrator CANNOT define a backup for a backup Vserver in an active standby GSLB setup for a given GSLB domain

B. Apply spillover policies on a subset of GSLB services and the user CANNOT have a backup for a subset of GSLB services.

C. Restrict the selection of a GSLB service from a subset of GSLB services bound to a GSLB virtual server for the given domain.

D. Any given GSLB Vserver can load-balance only one FQDN.

ANSWER: A D

Explanation:

An administrator CANNOT define a backup for a backup Vserver in an active standby GSLB setup for a given GSLB domain is a limitation because GSLB backup virtual-server relationships do not support a chained backup hierarchy. A GSLB virtual server can designate a backup virtual server for continuity when its primary service set is unavailable, but that backup virtual server cannot itself have another backup virtual server. This limits traditional active-standby designs to a single backup level for the relevant GSLB domain.

Any given GSLB Vserver can load-balance only one FQDN describes another limitation of a typical, non-policy-based GSLB design. In that model, a GSLB virtual server is associated with one DNS domain name and its service-selection behavior applies to requests for that domain. Citrix introduced GSLB policies and related domain-based configuration capabilities to

support more granular behavior, including configurations involving multiple domains and differing service selections. Understanding this distinction is important when designing a GSLB deployment that must provide domain-specific traffic distribution or more complex failover behavior. Citrix documents GSLB concepts and virtual-server configuration in its Global Server Load Balancing documentation and describes supported GSLB virtual-server configuration in the GSLB virtual server command reference.

QUESTION NO: 20

Scenario: A Citrix Administrator configured the following policies in a Citrix Virtual Desktops Site environment, in descending priority order.

1. â€œMarketing Office Aâ€□ has a filter on Marketing users. 'Client Network Drives' is disabled; 'Client Fixed Drives' is enabled.

2. â€œMarketing Office Bâ€□ has a filter on Marketing users' internal IP. 'Client Network Drives' is disabled; 'Client Fixed Drives' is enabled.

3. â€œAccountingâ€□ has a filter on Accounting Users. 'Client Network Drives' is enabled; 'Client Fixed Drives' is NOT configured.

4. â€œBaselineâ€□ is configured without a filter. 'Client Network Drives' and 'Client Fixed Drives' are both disabled.

Based on these policies, what will Accounting users be able to access?

A. Client network drives only

B. Neither the client network drive nor the client fixed drive

C. Client fixed drives only

D. Client fixed and network drives

ANSWER: A

Explanation:

Client network drives only is correct. Citrix policies are evaluated according to priority, but policy precedence is applied independently for each individual setting. An Accounting user matches both the Accounting policy through its user filter and the unfiltered Baseline policy. The two Marketing policies do not apply because their filters target Marketing users, rather than Accounting users.

For the Client Network Drives setting, the Accounting policy explicitly enables access. Because it has higher priority than Baseline, its enabled value takes precedence over Baseline’s disabled value. The user can therefore access mapped network drives exposed from the endpoint during the session.

For Client Fixed Drives, the Accounting policy is not configured. An unconfigured setting does not override a value supplied by a lower-priority applicable policy. Consequently, the setting continues to be evaluated from the applicable Baseline policy, where Client Fixed Drives is disabled. The resulting effective policy permits client network-drive access while leaving client fixed-drive access disabled. Citrix documents that policies are prioritized and that the highest-priority applicable configured value for each setting is used. See Citrix policy documentation and Citrix policy settings documentation.

QUESTION NO: 21

A Citrix Administrator has disabled User Subscriptions (Mandatory Store) for the StoreFront internal store.

Which two experiences will users have when they authenticate to the Citrix Virtual Apps and Desktops Site through the internal store? (Choose two.)

A. Users can manually add additional StoreFront stores if desired.

B. Applications cannot be removed from Citrix Workspace app on the Favorites screen.

C. Users can choose which applications they would like to add to the desktop.

D. Applications will automatically be placed in the Start menu.

E. Users can choose which applications they would like to add to their Favorites.

ANSWER: B D

Explanation:

With User Subscriptions disabled, StoreFront operates as a mandatory store. In this mode, StoreFront automatically subscribes each authenticated user to every application and desktop that the user is entitled to access through the store. The user therefore does not manage an individual set of subscribed resources; the available resources are presented automatically based on entitlement.

Accordingly, **Applications cannot be removed from Citrix Workspace app on the Favorites screen.** Resources in a mandatory store are not user-managed subscriptions, so users cannot remove them from their displayed favorites/subscribed resources. Also, **Applications will automatically be placed in the Start menu.** For supported Citrix Workspace app for Windows integrations, automatically subscribed applications are integrated into the user's Start menu, allowing the published applications to be launched like locally installed applications.

This configuration is useful when administrators need a consistent, administrator-controlled application experience and want every entitled resource to be available without requiring users to opt in. StoreFront determines what is shown from the user's Citrix Virtual Apps and Desktops entitlement, while the mandatory-store setting prevents users from curating that resource list themselves. Citrix documents mandatory stores and user-subscription behavior in its StoreFront user access configuration documentation; Start menu integration is described in the Citrix Workspace app for Windows configuration documentation.

QUESTION NO: 22

Scenario:

A Citrix Administrator must implement new security standards to protect all internal users' username and password information within a Citrix Virtual Apps and Desktops environment. The solution must involve the **least administrative overhead** and **lowest cost**, while protecting authentication traffic inside the corporate network.

Which two certificates should the administrator deploy? **(Choose two.)**

A. A third-party SSL certificate on the StoreFront server(s)

B. A third-party SSL certificate on the Delivery Controller(s)

C. A **domain SSL certificate** on the StoreFront server(s)

D. A **domain SSL certificate** on the Delivery Controller(s)

ANSWER: C D

Explanation:

A **domain SSL certificate** on the StoreFront server(s) and a **domain SSL certificate** on the Delivery Controller(s) provide TLS protection for the internal authentication-related communications required in this scenario. StoreFront is the user-facing authentication and resource-enumeration component. Configuring HTTPS with a certificate issued by the organization's Active Directory-integrated certification authority encrypts client-to-StoreFront authentication traffic and presents a certificate that domain-joined internal clients already trust.

Delivery Controllers provide the XML service used by StoreFront for resource enumeration and launch-related requests. Enabling HTTPS for this Controller service and assigning a domain-issued certificate protects the StoreFront-to-Controller communication path. Consequently, credentials and other sensitive authentication or session-brokering data are protected while traversing the corporate network.

Internal CA-issued certificates are appropriate for this requirement because domain members can automatically trust the issuing CA through Active Directory policy, which avoids manual trust-distribution work and external certificate procurement.

Citrix documents TLS configuration for StoreFront and Controller communications in its security guidance. See Citrix StoreFront security documentation and Citrix TLS security documentation.

QUESTION NO: 23

Scenario: A Citrix Administrator must prevent users from copying data between their endpoint devices and published applications.

Which two Citrix policy settings should the administrator configure? (Choose two.)

A. Client clipboard redirection

B. Server clipboard redirection

C. Client drive mapping

D. Auto-create client printers

E. Client audio redirection

ANSWER: A B

Explanation:

Client clipboard redirection controls clipboard data copied from the endpoint into a Citrix session. Configuring this setting to prohibit redirection prevents users from pasting endpoint clipboard content into published applications or desktops.

Server clipboard redirection controls clipboard data copied from the Citrix session to the endpoint. Configuring it to prohibit redirection prevents users from copying data from a published application or desktop and pasting it into a local application. Configuring both settings restricts clipboard transfer in both directions.

Drive mapping and client printer redirection govern different endpoint redirection capabilities and do not prevent clipboard data transfer. Citrix documents these controls in the client devices policy settings reference.

QUESTION NO: 24

Which step does a Citrix Administrator need to take to enable Citrix XML Service trust for user access within a Citrix Virtual Apps and Desktops infrastructure?

A. Enable XML Service trust using the StoreFront console.

B. Run the Set-BrokerSite -TrustRequestsSentToTheXMLServicePort $true PowerShell command from within a Virtual Delivery Agent (VDA) machine.

C. Run the Set-BrokerSite -TrustRequestsSentToTheXMLServicePort $true PowerShell command from within a Controller.

D. Configure the appropriate XML Service trust settings using HDX policy within Citrix Studio.

ANSWER: C

Explanation:

Run the Set-BrokerSite -TrustRequestsSentToTheXMLServicePort $true PowerShell command from within a Controller. This setting is a site-wide Citrix Virtual Apps and Desktops broker configuration, so it must be changed through the Citrix PowerShell SDK on a Delivery Controller, where the Broker Service management components are installed and can modify the site database configuration.

Enabling XML Service trust allows the XML Service to trust user credentials supplied in requests from StoreFront rather than requiring the XML Service to authenticate those credentials itself. This configuration is commonly used when StoreFront performs user authentication and then requests resource enumeration or launch information from the Delivery Controller.

Because it changes how authentication requests are trusted, it should be enabled only when StoreFront and the Controllers are deployed in an appropriately secured, trusted environment.

Citrix documents the BrokerSite setting through the Set-BrokerSite cmdlet reference. Citrix also describes XML Service trust and the associated StoreFront authentication planning considerations in its StoreFront user authentication documentation.

QUESTION NO: 25

Scenario: A Citrix Administrator is required to maximize the usage of the Citrix Virtual Apps and Desktops Site by enabling users to access the Site from external devices and reducing the cost and the effort required to maintain the infrastructure. The desktops for the users are provisioned using Citrix Provisioning.

Which set of resources will enable the administrator to achieve the objective?

A. Citrix Virtual Apps and Desktops service, Citrix Gateway service, on-premises resources

B. Citrix Virtual Apps and Desktops service, Citrix Gateway, public cloud

C. Citrix Virtual Apps and Desktops service, Citrix Gateway, on-premises resources

D. Citrix Virtual Apps and Desktops service, Citrix Gateway service, public cloud

ANSWER: A

Explanation:

Citrix Virtual Apps and Desktops service, Citrix Gateway service, on-premises resources is the appropriate resource set because it combines Citrix-managed cloud control-plane and external-access services with the existing local infrastructure needed for Citrix Provisioning. Citrix Virtual Apps and Desktops service (Citrix DaaS) reduces administrative effort because Citrix operates and maintains the cloud management components, including the control plane, rather than requiring the organization to maintain equivalent on-premises management infrastructure.

Citrix Gateway service provides secure remote access for users connecting from external devices. It is a Citrix-managed cloud service and removes the need to deploy, patch, scale, and maintain a customer-managed Citrix Gateway appliance or virtual machine for this access path. The on-premises resource location remains suitable because Citrix Provisioning components, such as Provisioning servers and their associated image and streaming infrastructure, can continue operating close to the hosted desktop workloads and local network resources. Cloud Connectors in the resource location securely connect those resources to the Citrix-managed service.

Citrix documents the resource-location architecture at Citrix DaaS Resource locations and describes secure remote connectivity through the Citrix Gateway service.