DUMPSBOSS.

Citrix Virtual Apps and Desktops 7 Assessment Design and Advanced Configurations

Citrix 1Y0-403

Version Demo

Total Demo Questions: 14

Total Premium Questions: 146

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Assessing and Designing a Citrix Virtual Apps and Desktops 7 Solution	120
Topic 2, Configuring a Citrix Virtual Apps and Desktops 7 Solution	26
Total	146

QUESTION NO: 1

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. While assessing the existing infrastructure, the architect determined that a number of users utilize legacy USB print devices that they will continue to need locally and within HDX sessions. The current HDX-optimized print virtual channel will NOT support these devices, so the architect decides that the Generic USB redirection channel should be used.

Which two factors must the architect consider when using Generic USB redirection? (Choose two.)

A. It requires more network bandwidth compared to standard HDX virtual channels.

B. Local access to printers will be lost until the HDX sessions is disconnected or ended.

C. Manufacturer printer drivers will need to be installed on user workstations.

D. The Citrix Virtual Channel Software Development Kit (VCSDK) will be required.

E. It is supported for only USB 3.0 devices and features.

ANSWER: A B

Explanation:

Generic USB redirection sends the USB device's traffic from Citrix Workspace app to the virtual desktop or application as if the peripheral were physically attached to the session host. Because this transports low-level USB protocol traffic rather than using a purpose-built, device-aware HDX printing channel, it can consume substantially more network bandwidth. The precise impact depends on the device's behavior, print-job size, protocol chatter, latency, and available bandwidth, so the architect should assess network capacity and user experience before relying on it for printing.

When a USB printer is redirected generically, Citrix Workspace app gives the remote session exclusive control of that USB device. Therefore, the endpoint operating system cannot use the redirected printer locally while the HDX session owns it. Local access becomes available again when the device is released, typically after the user disconnects from or ends the HDX session. This exclusivity is an important operational consideration where users need to alternate between local and hosted printing. Citrix documents that USB redirection redirects devices for use in the session and that redirected devices are unavailable to the local client while connected. See Citrix Workspace app USB device redirection and Citrix Virtual Apps and Desktops USB redirection documentation.

QUESTION NO: 2

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. The architect ' s objective is to create a configuration to automatically reroute network traffic to the second NIC within the bond. The goal is to avoid a loss of productivity should the primary Citrix Hypervisor host NIC fail. Each hypervisor currently consists of a single, active 10 GB NIC and a second, dormant 1 GB NIC.

Which two network interface configurations should the architect implement? (Choose two.)

A. Active-passive

B. Active-active (SLB)

C. NIC teaming-bonding

D. Active-active (LACP)

ANSWER: A C

Explanation:

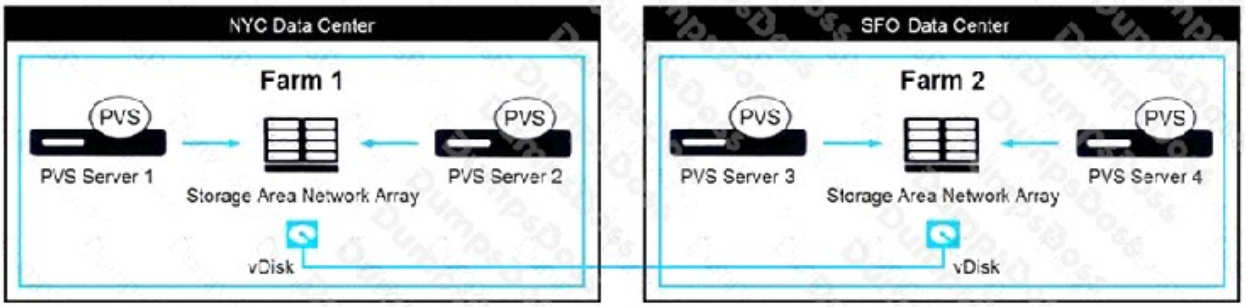
Active-passive and **NIC teaming-bonding** provide the required host-network resiliency. A Citrix Hypervisor NIC bond combines the physical 10 GB and 1 GB adapters into one logical network interface, so the management and VM networking configuration can continue to use a consistent network connection rather than requiring manual reconfiguration after a physical NIC failure. In active-passive mode, one bonded interface is designated as the active link while the other remains available as the standby link. If the active 10 GB NIC or its path fails, Citrix Hypervisor detects the link failure and transfers

traffic to the remaining 1 GB NIC. This directly meets the stated requirement for automatic rerouting to a dormant secondary adapter and prioritizes availability during a primary-NIC outage. Because traffic normally uses only the active member, this design is appropriate for a standby interface with a lower link speed; the 1 GB adapter supplies continuity of service during the failure condition. Citrix Hypervisor documents NIC bonding as a mechanism for network redundancy and describes active-passive bonding as using one active interface with another interface available for failover. See the Citrix Hypervisor NIC bonding documentation and the networking documentation for configuration concepts and requirements.

QUESTION NO: 3

Scenario: A Citrix Architect is designing a multi-data center Citrix Virtual Apps and Desktops environment that will use Citrix Provisioning (PVS) to manage Virtual Delivery Agent (VDA) machine images. Each data center will have a separate PVS farm. During design discussions, the architect created a diagram to depict the way in which vDisk files will be replicated among PVS farms, based on the available storage for the vDisk stores.

Click the Exhibit button to view the diagram.



Overall, the customer has identified 3 objectives for the image-replication process:

Which method should the architect use to replicate vDisk files among data centers?

A. Manual copy

B. Scheduled RoboCopy commands

C. SAN replication

D. vDisk Replicator Utility

E. Microsoft Distributed File System Replication (DFSR) Namespaces

ANSWER: C

Explanation:

SAN replication is the appropriate method because the vDisk stores in the design are hosted on storage that can use the existing storage-array replication capability between data centers. Replication can be configured and operated through the storage platform, allowing storage administrators to manage the copy and synchronization workflow without needing Citrix Provisioning farm-administration rights. This aligns directly with the requirement to use established infrastructure and operational processes where possible.

For a vDisk store located on local storage, direct-attached storage, or a storage-area network, Citrix guidance recommends using replication to synchronize vDisks across locations. Storage-level replication also minimizes routine administrative effort: after the replication relationship and policy are established, changed vDisk files can be transferred according to the storage system's schedule or replication policy rather than requiring an administrator to perform a separate per-image process. The receiving location obtains a storage-consistent copy suitable for use by its independently managed Citrix Provisioning farm, while each farm can retain its own configuration and operational control. Citrix's virtual-apps-and-desktops design guidance discusses replication for vDisk stores, and the Citrix Provisioning documentation provides the relevant vDisk management context. See Citrix VDI best-practices design guidance and Citrix Provisioning documentation.

QUESTION NO: 4

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. Two Control Layer security requirements have been identified:

Secure XML traffic between StoreFront and the Delivery Controller using SSL.

Secure Ticket Authority (STA) traffic must be protected with SSL.

Which three tools can the architect use to ensure that all security requirements are met? (Choose three.)

A. Citrix Studio console

B. Internet Information Services (IIS)

C. Citrix Director console

D. Citrix StoreFront console

E. ' NETSH ' command line

ANSWER: B D E

Explanation:

Internet Information Services (IIS), the Citrix StoreFront console, and the `NETSH` command line can be used together to secure the required communications. On a Delivery Controller, the Citrix XML Service and the Secure Ticket Authority are exposed through the Controller's web-service infrastructure. IIS is used to install and manage the server certificate that establishes the Controller's HTTPS identity. The certificate must be trusted by StoreFront and must contain a name that StoreFront can use to reach the Controller securely.

The `NETSH` command-line utility is used to create or inspect the HTTP.SYS SSL certificate binding for the relevant HTTPS listener and port. This binding allows the Controller endpoint to present the intended certificate for incoming SSL/TLS connections. StoreFront is then configured in the Citrix StoreFront console to contact Delivery Controllers over HTTPS and to use secure STA URLs. This ensures that StoreFront uses TLS when communicating both with the XML service for resource enumeration and with the STA service for ticket validation. Citrix documents secure Delivery Controller and StoreFront integration at Citrix Delivery Controller installation and configuration and StoreFront Delivery Controller management.

QUESTION NO: 5

Scenario: A Citrix Architect is implementing a new Citrix Virtual Apps and Desktops environment. The IT team has purchased 1,000 Citrix Virtual Apps and Desktops Advanced licenses.

Moving forward, the company requires the IT team to produce a report of all unsuccessful connections of Citrix Virtual Apps during the previous 12 months.

Which two actions does the architect need to take to support these requirements? (Choose two.)

A. Configure 'GroomSessionsRetentionDays' to 365 days.

B. Upgrade to Citrix Virtual Apps and Desktops Premium licenses.

C. Configure 'GroomFailuresRetentionDays' to 365 days.

D. Upgrade to Citrix Gateway Universal licenses.

E. Implement Citrix Application Delivery Management.

ANSWER: B C

Explanation:

The environment must retain connection-failure records for the full reporting period and have the required monitoring entitlement. Configuring `GroomFailuresRetentionDays` to 365 days ensures that Citrix Monitor does not groom

connection-failure data before it can be included in a twelve-month report. This setting specifically controls the retention period for failed connection records in the Monitor database, making it the appropriate setting for a report focused on unsuccessful launches or connections.

Upgrading to Citrix Virtual Apps and Desktops Premium provides the licensing level needed for the enhanced monitoring and historical reporting capabilities required by this design. Licensing must be evaluated alongside database retention: retaining data alone does not satisfy a reporting requirement if the deployed edition does not provide the necessary monitoring capabilities. The architect should also size, protect, and maintain the Monitor database appropriately because increasing the retention period substantially increases the amount of historical monitoring data stored.

Citrix documents Monitor database grooming and retention configuration in its Monitor data grooming documentation. Product edition capabilities and licensing are described in the Citrix Virtual Apps and Desktops feature matrix.

QUESTION NO: 6

Scenario: A Citrix Architect is designing a pod-based architecture in a Citrix Virtual Apps and Desktops environment. The plan is to create three pods for different Resource Layer types:

- Windows 10 VDI (non-persistent)

- Windows Server 2016 hosted shared desktops (non-persistent) - Windows 10 VDI (persistent)

Which three components can be shared between the three pods? (Choose three.)

A. Citrix Delivery Controller

B. Citrix StoreFront

C. Citrix License Server

D. Citrix Director

E. Citrix Site Database

ANSWER: B C D

Explanation:

Citrix StoreFront, **Citrix License Server**, and **Citrix Director** can be shared by separate Citrix Virtual Apps and Desktops pods (Sites). StoreFront is designed to aggregate resources from multiple Citrix Sites and present the applications and desktops available to an authenticated user through a unified store. This permits each resource layer to remain independently managed while users access their entitled resources from one access interface.

A License Server can serve multiple Sites because licensing is centrally administered and the individual Delivery Controllers communicate with the configured License Server to obtain the required license capacity. Centralizing this service simplifies license management and avoids maintaining a separate licensing deployment for every pod.

Director can also be shared because it supports monitoring and help-desk operations across multiple Sites when those Sites are added to its configuration. This gives operations staff a consolidated view for session monitoring, troubleshooting, and user support, while each pod retains its independent Site-specific brokering and database functions. Citrix describes the Site as the core management unit and documents StoreFront's support for multiple Sites. See Citrix Virtual Apps and Desktops technical overview and Citrix StoreFront store configuration documentation.

QUESTION NO: 7

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. The customer previously installed all applications locally on managed laptops and desktops, but is willing to evaluate other application delivery methods as part of the new deployment. The environment will be standardized on Windows 10 for the Virtual Delivery Agent (VDA) machines.

As part of an application analysis performed earlier in the project, the information in the exhibit was collected regarding 1 of the required applications.

Click the Exhibit button to view the information.

Category	Detail
Application Name	Visual Studio
Description	The application is used to develop computer programs, websites, web apps, web services, and mobile apps.
Usage	The application will be used by developers working in the organization.
OS Compatibility	The application is compatible with the target operating systems.
Special Considerations	The users are internal and external contractors, third-party collaborators, and other provisional team members who do NOT require offline access to the application. The application contains a number of Windows services.

The customer's security policies mandate that all development software must run within the corporate data center, but should appear to the user as if it is running locally on the virtual machine (VM).

How should the architect recommend deploying the application?

A. Use Desktop OS machines to deliver VM hosted applications.

B. Install it directly on the endpoint devices, and include it in a virtual desktop session using the Local App Access feature.

C. Install it in an Application Layer using Citrix App Layering, then present it to users as an Elastic Layer during a virtual a virtual desktop session.

D. Stream it to a VDA machine using Microsoft App-V, and access it through a virtual desktop session.

E. Push it to users with a Workspace Environment Management (WEM) action option.

ANSWER: D

Explanation:

Stream it to a VDA machine using Microsoft App-V, and access it through a virtual desktop session. This approach keeps the application execution environment inside the corporate data center because the App-V client and the streamed application run on the Windows 10 VDA. The user interacts with the application through the Citrix virtual desktop, so it is presented within the desktop session and has the expected local-application experience from the user's perspective, while corporate controls over the VDA, application content, and data remain centralized.

Microsoft App-V separates an application from the base operating-system image by packaging it into a virtualized application package and delivering that package to managed clients. In this design, the VDA is the managed client. This is particularly useful for an application that should not be installed permanently into every base image, while still needing to be available inside the hosted Windows 10 desktop. Citrix Virtual Apps and Desktops supports integrating App-V applications with VDA-based workloads, allowing the architect to preserve centralized delivery and lifecycle management without placing the development software on endpoint devices. See Microsoft's App-V overview and Citrix's App-V integration documentation.

QUESTION NO: 8

Scenario: A Citrix Architect must update a Citrix Provisioning vDisk used by a production device collection. The architect needs to install application updates and validate the revised image before making it available to production target devices.

Which two actions should the architect perform before promoting the revised vDisk version to production? (Choose two.)

A. Create a Maintenance version of the vDisk.

B. Assign a maintenance target device to boot from the Maintenance version.

C. Change the existing Production version to private image mode.

D. Delete all previous vDisk versions before installing updates.

E. Configure the vDisk as a personal vDisk.

ANSWER: A B

Explanation:

The architect should first create a new **Maintenance** version of the vDisk. A maintenance version is writable and is intended for image updates, allowing the existing production version to remain available to users.

A maintenance target device should then be assigned to boot from the maintenance version. The architect can install updates, test application functionality, and validate the revised image on that device. After validation, the version can be promoted through the Test and Production stages according to the organization's vDisk update process.

QUESTION NO: 9

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. Management has requested dynamic distribution of users between the primary and backup data centers to ensure that all available hardware is utilized during normal operations.

What is the biggest risk the architect should highlight to the customer when designing the profile strategy?

A. Scale-Out File Servers are required to support active-active profile deployments

B. Using Microsoft Distributed File System Replication (DFSR) to replicate user profiles requires significant bandwidth

C. Replicating profiles between the 2 data centers will double storage costs

D. Roaming profiles are NOT supported in active-active Microsoft Distributed File System Replication (DFSR) deployments

ANSWER: D

Explanation:

Roaming profiles are NOT supported in active-active Microsoft Distributed File System Replication (DFSR) deployments. In an active-active design, the same user can be directed to either data center on different sessions or after a failover. Profile data is mutable and is commonly updated at logoff, so independently writable copies in separate sites create a multi-master replication problem. DFSR replicates changes asynchronously; it does not provide coordinated locking or transaction-aware profile synchronization across the two profile copies. If concurrent or overlapping changes occur, DFSR conflict handling can result in one version winning while another is moved to ConflictAndDeleted, leaving the user with missing or inconsistent profile settings. This is a data-integrity and user-experience risk, rather than merely a capacity-planning issue.

The profile design therefore needs a supported method that presents a single authoritative user-store location, or a profile solution specifically designed for multi-site availability and failover. Citrix Profile Management guidance should be considered alongside the storage and namespace design, and Microsoft's DFS Replication behavior and conflict-handling limitations must be accounted for before using it with user-profile data. See Microsoft DFS Replication overview and Citrix Profile Management documentation.

QUESTION NO: 10

Scenario: A Citrix Architect is designing a new 2,000-user Citrix Virtual Apps and Desktops environment. The environment will use Windows Server 2016 for all Site infrastructure components (Delivery Controllers, StoreFront servers, and Citrix Director). Machine Creation Services (MCS) will be used to provision Virtual Delivery Agent (VDA) machines. The environment will include 2 primary use cases:

- Windows Server 2016 VDA machines providing hosted applications
- Windows 10 VDA machines providing random, non-persistent VDI

The IT team has NOT yet purchased the hardware that will be used for the environment, and will build the Hardware Layer components based on the architect's recommendations.

How should the architect design the Citrix Hypervisor resource pools based on Citrix leading practices?

A. Windows Server 2016 VDA machines should be placed in 1 resource pool, Windows 10 machines should be placed in a second resource pool, and the infrastructure servers should be placed in a third resource pool.

B. Windows Server 2016 machines should be placed in 1 resource pool, and all Windows 10 machines should be placed in a second resource pool.

C. The infrastructure servers and all VDA machines should be located in 1 resource pool.

D. The infrastructure servers should be placed in 1 resource pool, and the VDA machines should be placed in a second resource pool.

ANSWER: D

Explanation:

The infrastructure servers should be placed in 1 resource pool, and the VDA machines should be placed in a second resource pool. This design separates the control-plane services that users depend on for brokering, authentication, application enumeration, and monitoring from the comparatively large and variable compute workload generated by hosted-application and pooled-VDI sessions. The infrastructure pool can consequently be sized and protected for predictable availability, while the VDA pool can be scaled according to aggregate user-session demand and the MCS provisioning capacity required for the 2,000-user environment.

A Citrix Hypervisor resource pool is a set of compatible hosts managed together, allowing workload placement and high-availability behavior within that pool. Keeping infrastructure and VDA workloads in distinct pools establishes a meaningful resource and failure-domain boundary: VDA growth, maintenance, or contention is less likely to consume the host capacity needed by Delivery Controllers, StoreFront, and Director. Within the VDA resource pool, both the Windows Server hosted-app machines and random non-persistent Windows 10 desktops can use the same pooled compute capacity, provided the hosts are appropriately sized for the combined workload. This aligns the hardware-layer design to workload roles rather than unnecessarily isolating each VDA operating-system type.

See Citrix guidance on managing Citrix Hypervisor resource pools and the Citrix Virtual Apps and Desktops architecture overview.

QUESTION NO: 11

Which access component will support anonymous access within a new environment?

A. Citrix StoreFront

B. Citrix Gateway Service

C. Citrix ADC

D. Citrix Workspace

ANSWER: A

Explanation:

Citrix StoreFront is the access component that supports anonymous access for Citrix Virtual Apps and Desktops resources. StoreFront can be configured to present a Receiver for Web site that does not require users to supply Active Directory credentials. Instead, it obtains and uses anonymous credentials that are configured for the associated Delivery Group. This is useful for scenarios such as kiosks, shared public devices, training rooms, or applications intended for unauthenticated users, while still allowing Citrix to broker and launch the published resources.

Anonymous access requires coordinated configuration: the Delivery Group must permit anonymous users and have suitable applications assigned, and StoreFront must have anonymous access enabled for the relevant store or Receiver for Web site. StoreFront is therefore the component that provides the anonymous user entry experience and passes the anonymous identity through the resource-enumeration and launch workflow. Citrix documents anonymous access configuration as a StoreFront capability and describes enabling anonymous users when configuring Delivery Groups. See Citrix StoreFront: Configure anonymous access and Citrix Virtual Apps and Desktops: Create a Delivery Group.

QUESTION NO: 12

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. The architect has identified the Resource Layer requirements shown in the exhibit.

Click the Exhibit button to view the requirements.

User Group	Persistent User Settings Required?	Assigned FlexCast Model	Access to Profile Folders Required?	Additional Requirements
Accountants	Yes	Hosted VDI – Static/Persistent	No	None
Executives	Yes	Remote PC	Yes, the following folders should be available: • Contacts • Desktop • Downloads • Favorites • My Documents	Profile data should be preserved even if the resource machine fails. Solution must NOT require additional software to be installed on remote PCs.
Graphic Designers	Yes	Published Apps that use vGPU	Yes, the following folders should be available: • Contacts • Desktop • Favorites • My Documents • My Pictures • My Videos	The application reads and writes a high volume of data to and from the AppData folder.
Customer Service	No	Published Desktop (Server OS)	No	None

Which feature of Citrix Profile Management could help the architect address the Graphic Designers Group requirements while minimizing login time?

A. Profile streaming

B. Active write back

C. Folder redirection

D. File exclusions

ANSWER: A

Explanation:

Profile streaming is the appropriate Citrix Profile Management feature for graphic designers when their user profiles contain large amounts of data but they still require fast sign-ins. With profile streaming enabled, Profile Management does not need to copy the entire profile from the user-store location to the endpoint before the session begins. Instead, it brings down the minimum profile content needed for logon and retrieves additional files from the user store on demand as the user or applications access them.

This behavior is particularly useful for design users because their profiles can include large application settings, caches, and other files that may not all be needed immediately at session startup. By avoiding a full up-front profile download, profile streaming reduces the amount of data that must be processed during logon and therefore helps minimize login time. Files that are accessed are cached locally during the session, allowing the user to work with required profile content while the remainder is obtained only when necessary. Citrix documents profile streaming as a way to improve logon performance for large profiles, while requiring reliable connectivity to the profile store throughout the session.

See Citrix's Profile streaming documentation and the Citrix Profile Management documentation for configuration and operational guidance.

QUESTION NO: 13

Scenario: A Citrix Architect is designing a new Citrix Virtual Apps and Desktops environment. The environment consists of 4 Citrix Hypervisor hosts, each running 10 virtual machines (VMs). To meet company security standards for the environment, the IT team will need to perform routine VM snapshots, data backups, and threat scans.

Which two matters should the architect consider when securing a backup plan for the company? (Choose two.)

A. Administrative access to the storage location that maintains backups and archived data should be monitored

B. There are various delegated administrator roles that will have permissions to perform VM snapshots

C. RAID technology is supported for secure VM backups and snapshots when using local host storage

D. VM snapshots and data backups are NOT required for backup purposes if an enterprise-grade, geo-replicated, high-security storage solution is deployed

E. Running simultaneous security scans on different VMs can reduce host resource utilization

ANSWER: A B

Explanation:

Administrative access to the storage location that maintains backups and archived data should be monitored because backup repositories contain highly sensitive copies of production workloads. A secure backup design requires access auditing so the organization can identify who viewed, changed, deleted, or restored backup data. Monitoring also supports incident investigation and helps detect unauthorized activity, including attempts to alter recovery points before or during a ransomware event. Access should be limited to authorized backup administrators and protected through appropriate authentication and authorization controls.

There are various delegated administrator roles that will have permissions to perform VM snapshots because Citrix Hypervisor uses role-based access control to delegate administrative capabilities without granting every administrator unrestricted control of the environment. The architect should define which teams and roles can create, manage, revert, or remove snapshots, ensuring that snapshot operations used by backup procedures are assigned according to least-privilege principles. This helps protect workload integrity while allowing operational teams to carry out approved recovery and maintenance tasks. Citrix documents built-in roles and the permissions assigned to them, which should be reviewed when designing administrative separation of duties. See Citrix Hypervisor role-based access control and Citrix Hypervisor backup guidance.

QUESTION NO: 14

Scenario: A Citrix Architect is creating a conceptual architecture for a Citrix Virtual Apps and Desktops environment. Based on some initial discussions around the companyâ€™s business goals and objectives, the architect collected the information shown in the exhibit.

Click the Exhibit button to view the information.

Which delivery model should the architect recommend?

A. Single-Site in Citrix Cloud, with resources hosted in public cloud

B. Single-Site, single-zone, and single on-premises data center

C. Multi-Site, and single on-premises data center

D. Multi-Site in Citrix Cloud, with resources hosted in public cloud

ANSWER: D

Explanation:

Multi-Site in Citrix Cloud, with resources hosted in public cloud is the appropriate delivery model when the conceptual design must support separate locations while using public-cloud-hosted workloads. Citrix Cloud provides the service-

management plane, reducing the customer-managed infrastructure required for components such as Delivery Controllers and the management consoles. The architect can then deploy Cloud Connectors within each public-cloud resource location, allowing the Citrix Cloud control plane to securely broker access to the workloads and services in those locations.

A multi-site design is appropriate where business requirements call for distinct locations, such as geographically separated operations, regional workload placement, independent resource administration, or resiliency boundaries. Hosting the application and desktop resources in public cloud also aligns the resource layer with a cloud-first model, enabling workloads to be located in the cloud regions that best meet organizational and user-access requirements. Citrix documents that resource locations are the places where workloads and resources are hosted, while Cloud Connectors provide the communication path from those locations to Citrix Cloud. See Citrix DaaS resource locations documentation and Citrix Cloud Connector documentation.