DUMPSARENA

VMware Certified Advanced Professional 7 - Desktop and Mobility Design Exam

VMware 3V0-752

Version Demo

Total Demo Questions: 13

Total Premium Questions: 138

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

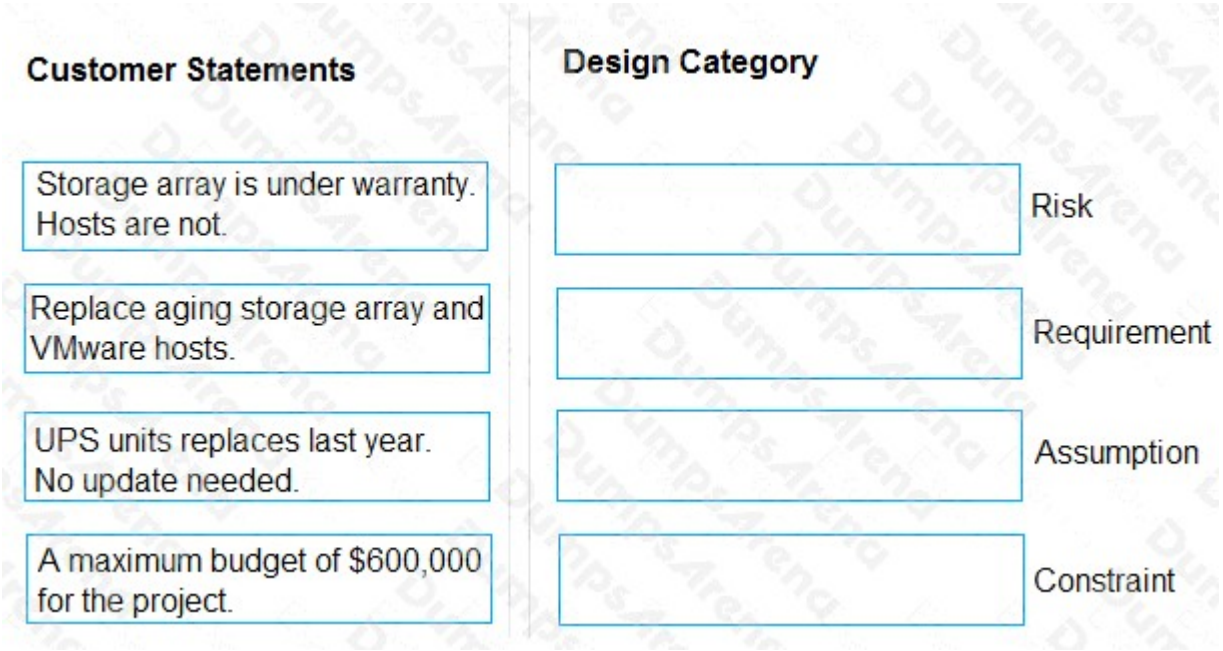
Topic Break Down

Topic	No. of Questions
Topic 1, Architectures and Technologies	5
Topic 2, VMware Products and Solutions	39
Topic 3, Planning and Designing	62
Topic 4, Installing, Configuring, and Setup	20
Topic 5, Performance-tuning, Optimization, and Upgrades	7
Topic 6, Troubleshooting and Repairing	5
Total	138

QUESTION NO: 1 - (SIMULATION)

A customer has an aging storage array that must be replaced. The array is used by VMware hosts in their data center. The storage array is under warranty, but the hosts are all out of warranty. The customer wants new hardware running Horizon 7, and is open to a hyperconverged solution. The project must take place with minimal-to-no disruption during normal business hours. The CIO states there is a maximum budget of $600, 000 for the project. The IT Director says their UPS units were replaced last year and they don't need to be updated. The existing racks are heavily populated, with limited rack units remaining and no additional datacenter floorspace for another rack.

Match the statements taken from the scenario with its correct design category.



ANSWER: See the explanation for the answer

Explanation:

Match the statements as follows:

Risk: `Storage array is under warranty. Hosts are not.`
The out-of-warranty hosts create a hardware-support/failure risk during the project.
Requirement: `Replace aging storage array and VMware hosts.`
This states the desired project outcome.
Assumption: `UPS units replaced last year. No update needed.`
The design assumes the existing UPS capacity and condition are adequate.
Constraint: `A maximum budget of $600,000 for the project.`
The budget is a fixed limitation on the solution.

QUESTION NO: 2

A VDI Architect wants to optimize Blast Extreme protocol between 400 Horizon Windows clients and agents on an organization's LAN. No GPO currently makes Horizon settings to these clients or agents.

What GPO setting will improve performance of these systems?

A. Enable H264

B. Disable UDP Protocol

C. Enable UDP Protocol

D. Disable H264

ANSWER: D

Explanation:

Disable H264 is the appropriate setting for this large, LAN-based Horizon deployment. H.264 is a highly compressed video codec that is particularly valuable when bandwidth is constrained, such as across WAN links. Its compression and decompression work, however, adds processor overhead at the Horizon Agent and client. With 400 Windows clients and desktops communicating on the organization's LAN, available network bandwidth is generally less constrained than it would be over a WAN. Disabling H.264 allows Blast Extreme to use its alternative adaptive image-quality mechanisms without imposing unnecessary H.264 encode/decode processing on every session. Reducing that recurring CPU work can improve desktop responsiveness and help preserve host CPU capacity and desktop density when many sessions are active simultaneously. The policy should be applied consistently to the relevant Horizon clients and agents after validating the result with representative workloads, especially workloads involving video or rapidly changing graphics. VMware's Blast configuration guidance and its Blast Extreme optimization material describe the codec and transport tuning considerations for differing network conditions: Omnissa Horizon documentation: Configuring the Blast protocol and Omnissa Tech Zone: Blast Extreme Optimization Guide.

QUESTION NO: 3

A company has decided to implement Workspace One on premise.

- Workspace One portal will be used by end users to simplify access to web, mobile and Windows based applications.
- As part of the solution, the company is planning on using Horizon 7 Application Publishing. ▪ Published Applications will be used for applications frequently used by mobile users.

During a proof of concept (POC), users noted that it was too cumbersome to enter Active Directory username and password and RSA SecureID using mobile devices.

The Chief Security Officer (CSO) stated:

- Multi-factor is a requirement for a subset of the applications.
- End-users must have as seamless as possible authentication using mobile devices.

Which solution can satisfy the CSO's requirements?

A. Implement VMware Identity Manager with Mobile SSO. Configure Access Policies to require RSA SecureID authentication for the subset of applications and implement TrueSSO in Horizon.

B. Implement VMware Identity Manager with VMware Verify for easy authentication. Since VMware Verify offers two factors no extra access policies is needed.

C. Implement VMware Identity Manager with Mobile SSO. Configure Access Policies to require VMware Verify authentication for the subset of applications and implement TrueSSO in Horizon.

D. Implement VMware Identity Manager with SSO. Configure Access Policies to require VMware Verify authentication for the subset of applications.

ANSWER: C

Explanation:

Implement VMware Identity Manager with Mobile SSO. Configure Access Policies to require VMware Verify authentication for the subset of applications and implement TrueSSO in Horizon. This design applies the appropriate authentication method at the Workspace ONE access layer while maintaining a low-friction mobile experience. Mobile SSO allows enrolled mobile devices to authenticate to Workspace ONE using certificate-based authentication rather than repeatedly requiring users to enter Active Directory credentials. This directly addresses the usability concern associated with typing usernames, passwords, and token codes on a mobile device.

VMware Identity Manager access policies can be assigned to individual applications or groups of applications, enabling the organization to invoke VMware Verify multi-factor authentication only where the security requirement applies. The policy model therefore supports both ordinary seamless access and stronger authentication for the designated application subset.

For Horizon-published applications, True SSO extends the experience by obtaining short-lived certificates and allowing Horizon to authenticate users to the Windows resource without requiring the user's Active Directory password. Together, Mobile SSO, conditional VMware Verify challenges, and True SSO meet the stated security and usability objectives. See the Workspace ONE Access architecture guidance and True SSO architecture guidance.

QUESTION NO: 4 - (DRAG DROP)

DRAG DROP

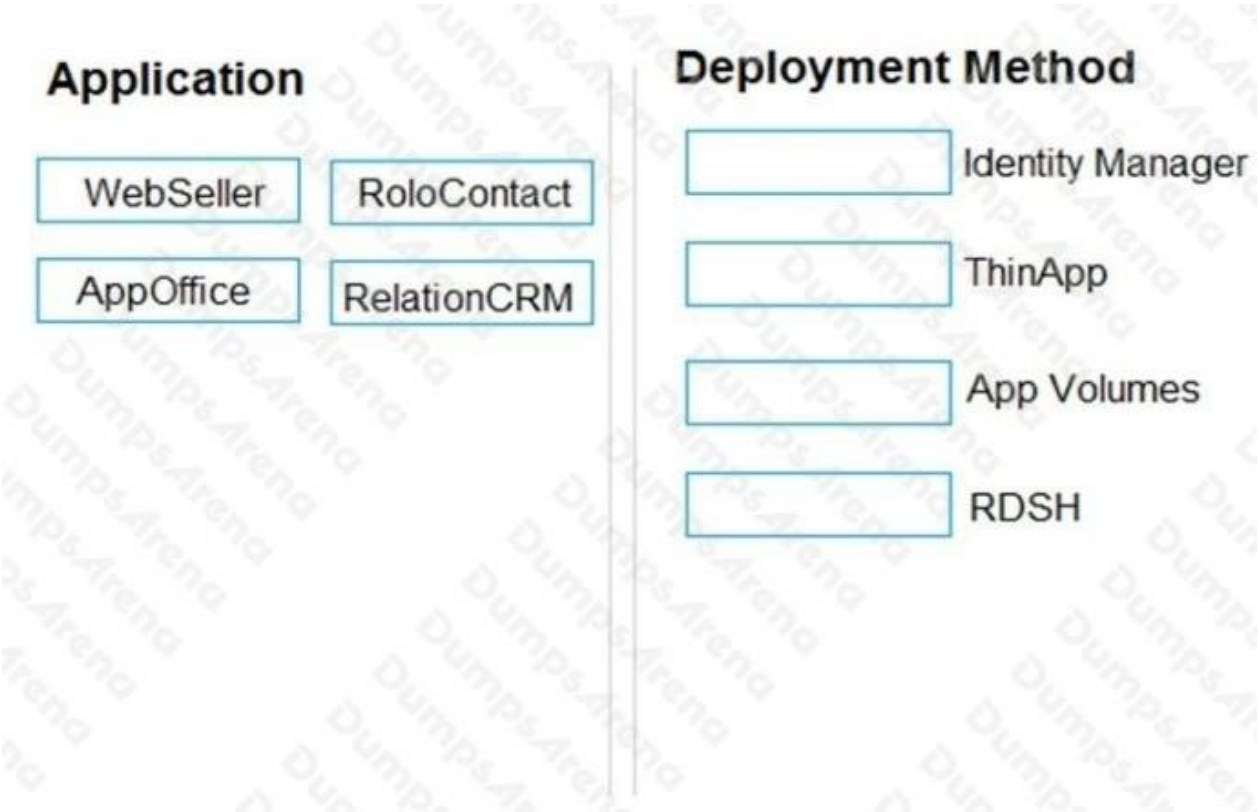
A company has several applications that are being moved to a Horizon environment. An architect has been given several application types and is designing an environment to accommodate all of the applications.

List of applications:

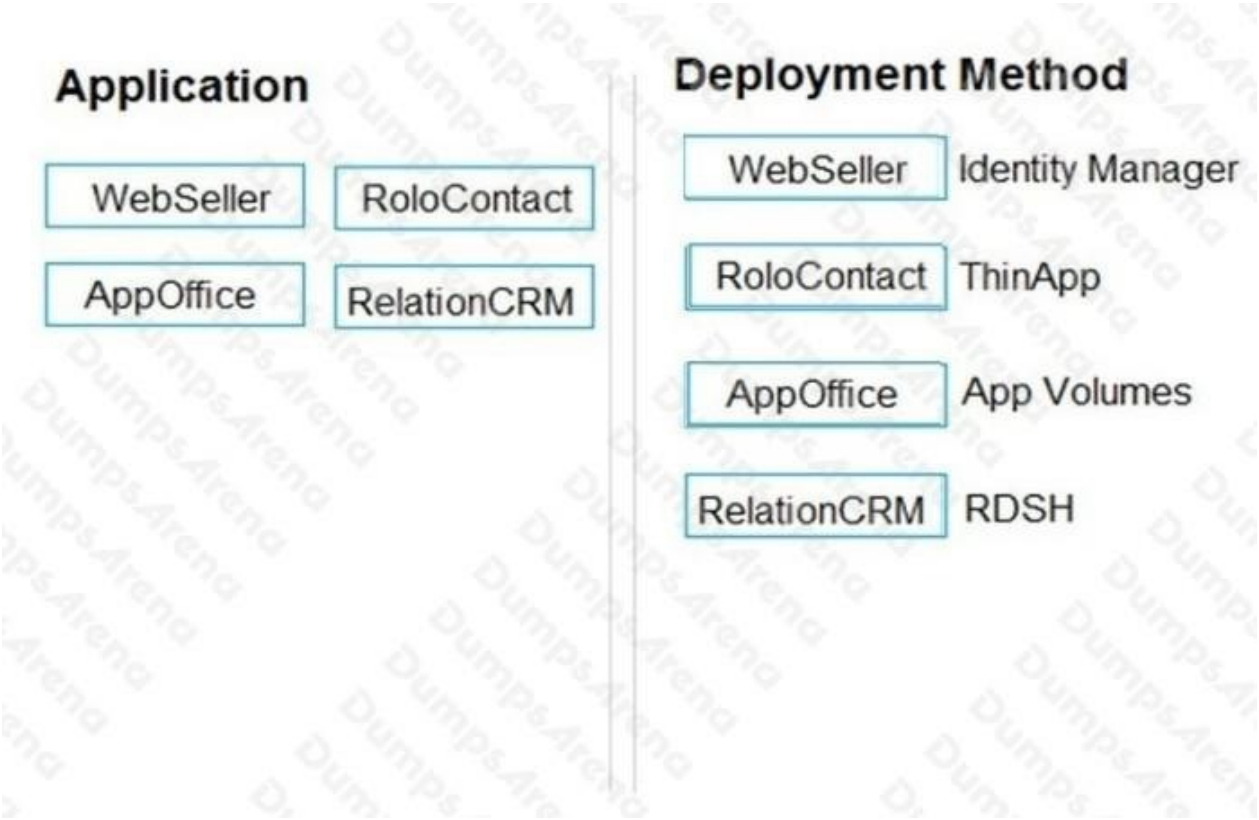
- WebSeller – a cloud-based application that is single sign-on capable.
- RoloContact – a Windows application that utilizes an Internet Explorer 6 and an IE plugin, but needs to be deployed to Windows 8 desktops.
- AppOffice – a group of Windows based application that needs to be deployed together to an existing View linked clone desktop pool for the remote sales team.
- RelationCRM – a server-based application that is currently accessed via RDP.

Match each application with its appropriate deployment method.

Select and Place:



ANSWER:



Explanation:

WebSeller belongs with Identity Manager because the application is cloud based and supports single sign-on. VMware Identity Manager is designed to provide a unified application catalog and federated access experience, allowing entitled users to launch SaaS and web applications through a centrally managed identity service. This directly supports the stated need without installing the application inside a desktop image.

RoloContact belongs with ThinApp because ThinApp packages an application into an isolated virtualized package. That isolation is useful when an older application requires Internet Explorer 6 behavior and a specific browser plug-in but must be made available on a newer Windows 8 desktop. The application can retain its required application environment rather than imposing those legacy dependencies directly on the operating system. VMware describes ThinApp application virtualization and isolation in its ThinApp packaging guidance.

AppOffice belongs with App Volumes because App Volumes delivers applications independently of the desktop image through attachable application packages. A package can contain the related applications that the remote sales users need and be assigned to the existing linked-clone pool, keeping the base image streamlined while ensuring the applications arrive together when entitled users log in. This is the intended model for managing and delivering applications dynamically to Horizon desktops, as covered in VMware's App Volumes documentation.

RelationCRM belongs with RDSH because it is already a server-based application accessed through RDP. Horizon can publish applications from Remote Desktop Session Host servers, providing users application access through Horizon while the software executes centrally on the RDSH host. VMware's published applications documentation describes this delivery model.

QUESTION NO: 5

An architect for Company A is working on implementing a VMware Horizon solution.

- Company A will be acquiring Company B in the coming months.

- Company B has an existing Active Directory structure and there are NO plans to move those users over to Company A's Active Directory structure - However, users from Company B need to be able to use VDI desktops running in Company A.

Which step could the architect take to meet requirements?

A. Use vdmadmin –T command to assign Administrator access.

B. Create a one-way or two-way forest trust relationship.

C. Create a new AD user account for Company B.

D. Set up a VMware Connection Server in Company B Domain.

ANSWER: B

Explanation:

Creating a one-way or two-way forest trust relationship enables Company B users to retain their existing Active Directory accounts while authenticating to and receiving entitled Horizon desktops hosted in Company A. Horizon Connection Server integrates with Active Directory to locate users and groups, authenticate users, and apply desktop or application entitlements. A trust permits the Company A Horizon environment to recognize security principals from Company B without requiring account migration, duplication, or a separate identity lifecycle for those users.

In this resource-access scenario, the trust direction should be designed so that the Company A forest, which hosts the Horizon resources, trusts identities in the Company B forest. A two-way forest trust can be used where mutual access requirements exist; otherwise, a one-way trust limits the scope to the required access path and supports least privilege. Forest trusts are appropriate when the organizations maintain separate AD forests and need cross-forest authentication and authorization. The architect can then add Company B users or groups to Horizon entitlements for the desktop pools hosted by Company A. See Microsoft's Active Directory trust overview and the VMware Horizon 7 documentation.

QUESTION NO: 6

Which are three default network ports that need to be allowed through a firewall for a Workspace One solution supporting Mobile Single-Sign on (SSO) for iOS and Android devices? (Choose three.)

A. TCP 5262

B. TCP/UDP 88

C. TCP 8443

D. TCP/UDP 1337

E. TCP 443

F. TCP 80

ANSWER: A B E

Explanation:

Mobile SSO for Workspace ONE relies on secure communication among managed mobile devices, Workspace ONE components, and Microsoft Active Directory services. **TCP 443** is required for HTTPS-based communication with Workspace ONE UEM and Workspace ONE Access services, including device enrollment, policy delivery, authentication workflows, and access to published resources. **TCP/UDP 88** is the standard Kerberos port. Mobile SSO uses Kerberos-based authentication to obtain and present tickets for integrated authentication to internal resources, so connectivity to the domain controller or key distribution center must be available on the applicable Kerberos transports. **TCP 5262** supports the XMPP federation communication used by Workspace ONE UEM messaging components. This communication enables service connectivity needed by the mobile-device management architecture and associated mobile SSO workflow. Firewall rules should permit these ports only between the relevant endpoints and should be combined with appropriate DNS resolution, certificate trust, and Active Directory connectivity. VMware/Omnissa's mobile SSO design guidance describes the use of Workspace ONE UEM, Workspace ONE Access, Kerberos, and the required supporting infrastructure. See the Mobile Single Sign-On with Workspace ONE guide and the Workspace ONE UEM network ports reference.

QUESTION NO: 7

An architect is asked to review a companyâ€™s plans to implement ThinApp packaged applications to its non-persistent Virtual Desktop Infrastructure (VDI). The applications must be assigned to users and not individual VDI desktops. All ThinApp packages are already available on a network share.

Which two options can the architect recommend to meet requirements? (Choose two.)

A. Using Microsoft Active Directory and Group Policy Objects, deploy the ThinApp MSI file upon login of the users.

B. In the Horizon Administration console, add the network share with the ThinApp packages. Entitle ThinApp packages using the Horizon Administration console.

C. Copy the Thinapped MSI to an App Volumes App Stack and assign the application via Active Directory.

D. Using thinreg.exe, add ThinApp packages registration and use the PermittedGroups option for the identified user groups.

E. Implement VMware Identity Manager, install the VMware Identity Manager for Windows on all VDI desktops and entitle the ThinApp packages using VMware Identity Manager.

ANSWER: B E

Explanation:

Using the Horizon Administration console to add the network share as a ThinApp repository and then entitle individual ThinApp applications is a supported Horizon delivery model. Horizon scans the repository for available packages and publishes selected applications to entitled Active Directory users and groups. Because entitlement is evaluated for the user at logon or application launch, it works appropriately with floating, non-persistent desktops; the application assignment does not depend on retaining a particular VDI machine.

VMware Identity Manager can also provide user-based ThinApp application delivery. With the VMware Identity Manager Windows component installed on the Windows VDI desktops, entitled users receive their ThinApp application catalog and can launch the packages from the configured network repository. This centralizes application entitlement around user or group identity and remains independent of the specific non-persistent desktop instance assigned during a session.

Both approaches use the existing network share rather than requiring the ThinApp packages to be installed permanently in the base image. They also support assigning access through directory-backed user and group entitlements, which directly satisfies the requirement. VMware's Horizon documentation is available at Omnissa Tech Zone: ThinApp Packaging and Deployment, and product documentation can be found at VMware Horizon Administration: ThinApp Applications.

QUESTION NO: 8

A customer has chosen vRealize Operations Manager for Horizon as its monitoring solution.

The customer's requirements are:

- Monitor the PCoIP metrics to address user experience complaints.
- Minimum required resources should be used for monitoring purposes.

Recent project updates include:

- vRealize Operations Manager is already in use for vSphere monitoring.
- All desktop templates are created with Horizon 7 View agent and Horizon deployment is at the final stage of completion.
- Existing vRealize Operations Manager capacity is already scaled out to meet the current requirements of Horizon 7 monitoring needs.

Which two additional components are required to make the monitoring systems ready? (Choose two.)

A. vRealize Operations Microsoft SQL Server plug in

B. vRealize Operations for Horizon Adapter

C. vRealize Operations for Horizon Desktop Agent

D. vRealize Operations Manager remote collector nodes

E. vRealize Operations for Horizon Broker Agent

ANSWER: B C

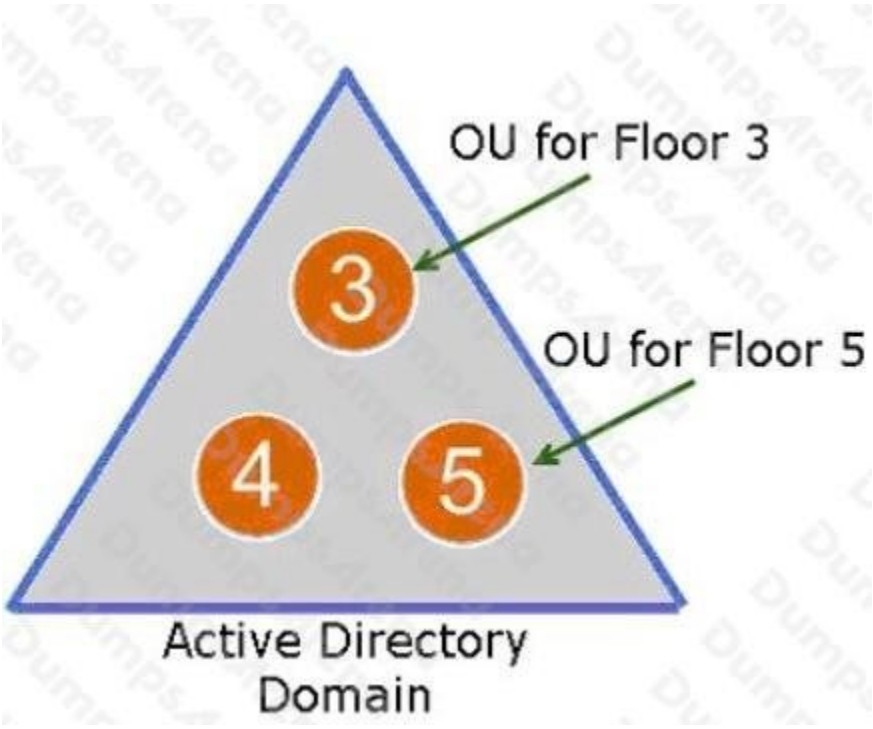
Explanation:

vRealize Operations for Horizon Adapter is required to extend the existing vRealize Operations Manager deployment with Horizon-specific collection, inventory, dashboards, alerts, and analytics. Because vRealize Operations Manager is already deployed and has adequate capacity, the Horizon adapter can be added to that platform without introducing a separate monitoring system or additional collector infrastructure. The adapter is the integration point through which Horizon monitoring data is processed and presented in vRealize Operations Manager.

vRealize Operations for Horizon Desktop Agent is required on the Horizon desktop images to collect the endpoint and protocol-performance data needed to investigate user-experience issues. In particular, PCoIP performance metrics are gathered from the desktop side and made available for Horizon monitoring and troubleshooting. Since the templates currently contain only the Horizon Agent, the Horizon Desktop Agent must be added before desktops are provisioned. This directly supports monitoring PCoIP quality while using the existing vRealize Operations Manager capacity efficiently. VMware describes Horizon monitoring integration and its Horizon-specific metrics in the Aria Operations Horizon monitoring documentation and the desktop-side agent's role in the Broadcom knowledge base.

QUESTION NO: 9

Company M recently acquired Company T. All Company M employees work in the same office building. Company T has multiple buildings. Company T uses a single domain Active Directory (AD) structure as shown in the exhibit. They place end users in one of several AD groups in an OU based on the floor of the building where that user's office is located. Over the next six months, the IT team will be adding AD groups and user accounts for Company T employees.



The IT team decided to implement VMware Horizon and deploy all end user applications using Horizon RDS application pools. All users need access to all Horizon RDS applications.

After creating the Horizon RDS application pools, what task should the IT team perform to enable users access the applications with the least administrative effort?

A. Entitle each AD group to the Horizon RDS application pools.

B. Entitle each RDS Host to the Horizon RDS application pools.

C. Entitle the AD domain to the Horizon RDS application pools.

D. Entitle each OU to the Horizon RDS application pools.

E. Entitle all users to the Horizon RDS application pools.

ANSWER: E

Explanation:

Entitle all users to the Horizon RDS application pools. This is the lowest-administration approach because the stated access policy is universal: every user requires every published application. An all-users entitlement is evaluated without requiring administrators to maintain a separate entitlement for each floor-based Active Directory group, organizational unit, or subsequently created account. As Company T onboards employees and creates additional groups during the next six months, eligible authenticated users receive access through the existing entitlement automatically, so no recurring pool-entitlement updates are needed solely because of those directory changes.

In Horizon, entitlements are the mechanism that determines which users can see and launch a desktop or published application. Horizon Console supports assigning users and groups and provides an all-users entitlement for cases where access is intended for the entire Horizon user population. This design should be used only when the universal-access requirement is intentional; application-level authorization and least-privilege requirements should still be reviewed if the organization later introduces applications with restricted audiences. VMware's published-applications administration documentation describes managing application entitlements, and its Horizon architecture documentation explains Horizon's integration with Active Directory for user authentication and authorization. See VMware Horizon: Entitling Users and Groups to Published Desktops and Applications and VMware Horizon: Active Directory.

QUESTION NO: 10

A hospital is looking to introduce a new work model. Their goal is to allow doctors and nurses to access care applications more flexibly. An important task is that Android and iOS tablets be allowed for hospital staff. The IT department is faced with the task of executing on the requirements.

The current client environment is:

- Physical Windows 7 desktops and laptops
- 2500 Windows based applications
- 300 Web based applications, where 200 requires Internet Explorer ▪ Windows applications are managed using Microsoft SCCM

Any solution must be in production within 6 months. IT was approved to start building a non-optimized solution to get things started. At a later date, investments will be spent on optimizing the solution. There is no time for a proper application assessment and user segmentation, so the solution must support as broad a user base as possible.

The main priorities for the design are:

- Time to market
- Change as little as possible of existing management processes

What solution would support the main priorities?

A. Deploy Horizon 7 on vSAN ready nodes. Create full clones Windows 7 VDI desktops and manage applications using the existing Microsoft SCCM solution.

B. Deploy Horizon 7 on vSAN ready nodes. Create linked clones desktops based on Windows 10 and manage applications using App Volumes.

C. Deploy Horizon 7 on existing SAN and use Application Publishing to allow access to all Windows applications. Use VMware Identity Manager to allow access to all Web applications natively on the tablets.

D. Order a new physical SAN and deploy Horizon 7. Use Instant Clones Windows 7 VDI desktops to save SAN storage. Manage applications using Microsoft SCCM.

ANSWER: A

Explanation:

Deploy Horizon 7 on vSAN ready nodes. Create full clones Windows 7 VDI desktops and manage applications using the existing Microsoft SCCM solution.

This approach best supports rapid delivery while deliberately minimizing change to the hospital's current desktop and application-management model. Full-clone virtual desktops can use the existing Windows 7 desktop image and preserve the established Microsoft SCCM-based process for deploying, updating, and managing the large Windows application estate. This avoids requiring an immediate application-rationalization project, user-segmentation exercise, or broad conversion of applications into another delivery format. It also provides a familiar, complete Windows environment for the many applications and browser-dependent workflows that need Internet Explorer.

Horizon provides remote access to virtual desktops through Horizon Client on supported Android and iOS devices, so clinicians can use tablets while the applications and desktop workload remain centrally hosted and controlled. vSAN Ready Nodes provide prevalidated server hardware configurations for vSAN, helping the organization establish the Horizon infrastructure without designing a separate storage platform from scratch. The organization can subsequently optimize desktops, application delivery, and personas after the initial service is in production. VMware's Horizon architecture guidance is available at Horizon Architecture Planning, and vSAN Ready Node guidance is available at VMware vSAN Ready Nodes.

QUESTION NO: 11

A customer is designing a Horizon published-application service using an automated RDS farm. The design must continue providing application access when one RDS host is unavailable and must prevent new sessions from being directed to a host that is undergoing maintenance.

Which two design decisions meet the requirements? (Choose two.)

A. Deploy multiple RDS hosts in the automated farm.

B. Place an RDS host in maintenance mode before performing maintenance.

C. Create one dedicated application pool for every RDS host.

D. Configure each RDS host to use a separate Horizon Connection Server.

E. Disable Horizon load balancing for the farm.

ANSWER: A B

Explanation:

Deploying **multiple RDS hosts in the farm** provides capacity and availability when an individual RDS host becomes unavailable. Horizon can direct new application sessions to another eligible host in the same farm, provided that sufficient capacity remains available.

Placing a host in **maintenance mode** prevents Horizon from sending new sessions to that host while allowing the administrator to drain or manage existing sessions according to the selected maintenance behavior. This supports planned maintenance without removing the published application pool or disrupting the remaining healthy RDS hosts. See the Horizon documentation for managing RDS hosts.

QUESTION NO: 12

A company has two Horizon pods in separate data centers. Both pods contain an RDS farm that publishes the same accounting application. Users must see one application entitlement, be directed to their preferred site when available, and retain access if the preferred site cannot provide the application.

Which Horizon feature should be configured?

A. A local application entitlement

B. A Global Application Entitlement

C. A Global Desktop Entitlement

D. An App Volumes entitlement

ANSWER: B

Explanation:

A Global Application Entitlement should be configured. In a Cloud Pod Architecture environment, a global application entitlement combines published application pools from multiple pods into one user-facing entitlement. It can use site assignments and home-site behavior to direct users toward the preferred site while allowing Horizon to use another entitled site when necessary.

A local application entitlement is limited to resources in one pod. A global desktop entitlement is used for desktop pools rather than published applications. An App Volumes entitlement controls application package assignment but does not broker users between RDS farms in separate Horizon pods. See the Horizon Cloud Pod Architecture documentation.

QUESTION NO: 13

In a local design, a company selected one database instance to be shared by Horizon View Composer database, vCenter external database, and Horizon AppVolumes database. The design must provide High Availability for all databases.

Which two database server options should be selected during physical design creation? (Choose two.)

A. Oracle 10g

B. Microsoft SQL Server 2014

C. Oracle 11g

D. Microsoft SQL Server 2012

ANSWER: B C

Explanation:

Microsoft SQL Server 2014 and **Oracle 11g** are suitable common external database platforms for this design because they are supported across the Horizon View Composer, vCenter Server external database, and App Volumes roles applicable to this Horizon generation. Selecting one of these common platforms allows the physical design to standardize database operations, connection configuration, backup processes, and database-administration skills while keeping the individual product databases logically separate.

Both platforms also provide mature database-layer high-availability capabilities. SQL Server 2014 can be designed with mechanisms such as Failover Cluster Instances or Always On Availability Groups, while Oracle 11g can use Oracle Real Application Clusters or Data Guard-based designs. The application components should connect through the database service name, listener, virtual name, or other stable endpoint so that a database failover does not require each Horizon or vCenter component to be manually reconfigured. High availability must include the database nodes, storage, network paths, and tested recovery/failover procedures; merely placing several product databases on one standalone database host would not meet the requirement. VMware compatibility must also be validated against the exact Horizon, vCenter, App Volumes, database edition, and patch levels being deployed. See the Broadcom VMware Product Interoperability Matrix and the VMware Horizon installation documentation.