DUMPSARENA

Associate VMware Digital Workspace

VMware 1V0-61.21

Version Demo

Total Demo Questions: 7

Total Premium Questions: 75

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, IT Architectures, Technologies, Standards	4
Topic 2, VMware Solutions	56
Topic 3, Install, Configure, Setup	11
Topic 4, Troubleshooting and Repairing	4
Total	75

QUESTION NO: 1

Which two components provide end user access to virtual desktops and hosted applications? (Choose two.)

A. Horizon Client

B. vSphere Client

C. Horizon Console

D. HTML Client

E. Horizon Agent

ANSWER: A D

Explanation:

Horizon Client and HTML Client provide the end-user connection methods for VMware Horizon virtual desktops and published (hosted) applications. Horizon Client is the installable application available for supported endpoint operating systems and devices. It authenticates the user with the Horizon environment and establishes the appropriate remote-display connection to the entitled desktop or application. It is designed to provide a full featured user experience and supports Horizon display protocols such as Blast Extreme, subject to the Horizon deployment configuration.

HTML Client represents browser-based access, commonly documented by VMware as HTML Access. It enables an entitled user to sign in through a supported web browser and launch virtual desktops or published applications without installing the native Horizon Client on the endpoint. This is especially useful for managed or temporary devices where a local client installation is not desired. Both access methods present the resources assigned to the user after authentication and authorization, making them the components used directly by end users to open desktops and hosted applications. VMware's Horizon documentation describes connecting through either the Horizon Client application or HTML Access: VMware Horizon Client documentation and VMware Horizon HTML Access documentation.

QUESTION NO: 2

Where should an administrator deploy Unified Access Gateway to provide secure external access to internal Horizon resources?

A. DMZ

B. Active Directory domain

C. vCenter Server database

D. Desktop virtual machine network only

ANSWER: A

Explanation:

DMZ is correct because Unified Access Gateway is designed to operate as a hardened edge gateway between external clients and internal resources. Deploying Unified Access Gateway in a demilitarized zone enables remote users to access Horizon desktops and published applications without requiring direct inbound access to Horizon Connection Server instances or desktop workloads on the internal network.

The DMZ placement supports a layered security design. Firewall rules can be configured to allow only the required traffic between external clients, Unified Access Gateway, and internal Horizon infrastructure. See the Unified Access Gateway technical overview for deployment architecture guidance.

QUESTION NO: 3

An administrator wants to set the initial configuration state of applications using Application Profiler. Which VMware tool does the Application Profiler reside in?

A. App Volumes

B. Unified Access Gateway

C. Dynamic Environment Manager

D. Workspace ONE UEM

ANSWER: C

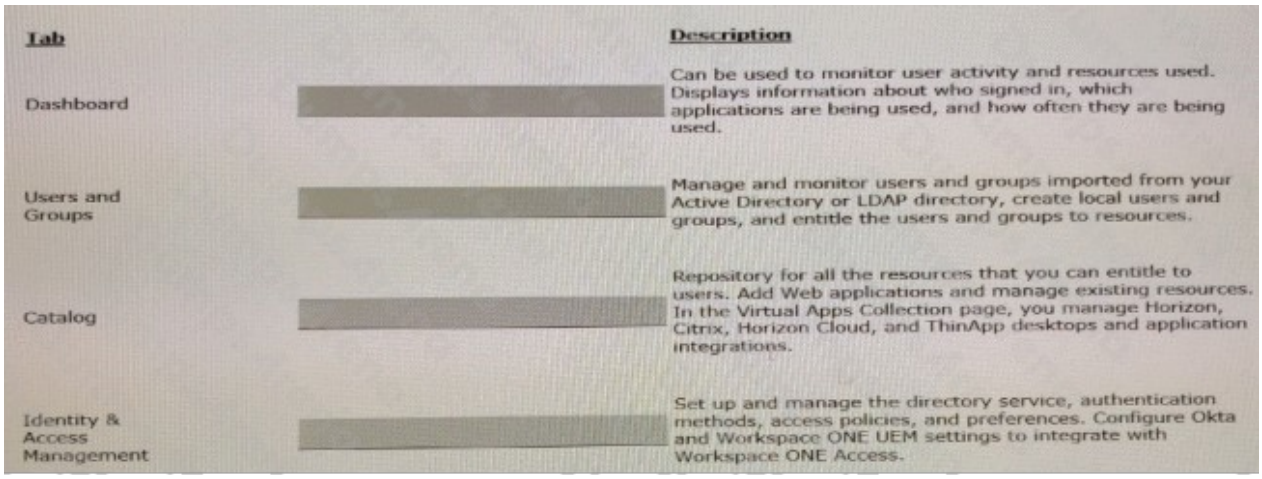
Explanation:

Dynamic Environment Manager is correct because Application Profiler is a component of the Dynamic Environment Manager Management Console. It lets an administrator launch an application and monitor the user-profile and registry changes that occur while the application is configured. The captured changes can then be used to create an application configuration definition, allowing Dynamic Environment Manager to save, restore, and apply the intended initial application settings for users.

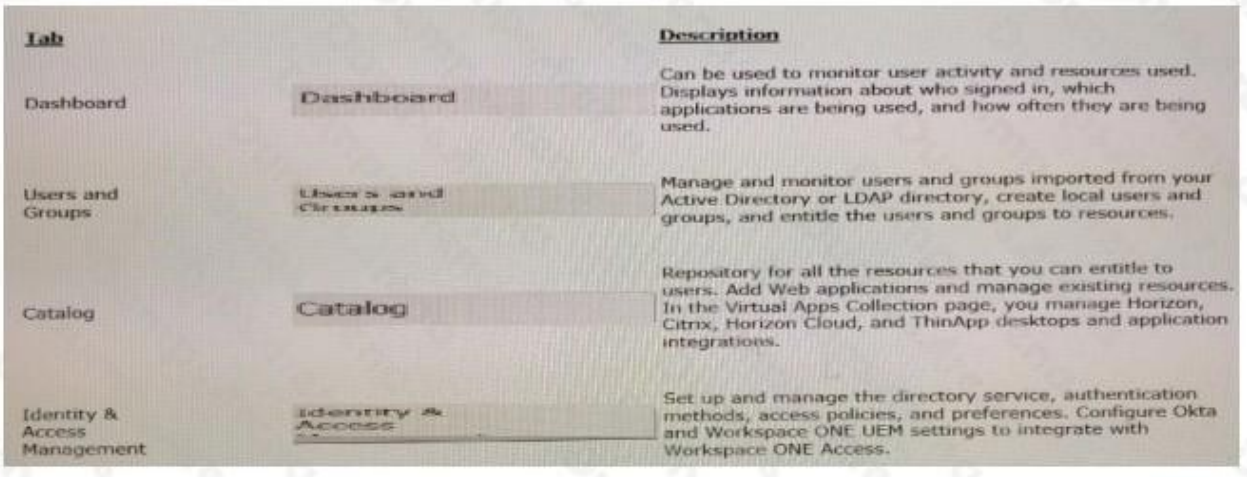
This capability supports consistent user experiences in virtual desktop and published-application environments without requiring administrators to manually identify every registry key and user-profile file associated with an application. Application Profiler is therefore used during configuration authoring: it observes the application's settings activity, presents the detected items for review, and helps build the configuration that Dynamic Environment Manager manages at logon, logoff, or application launch. VMware's Dynamic Environment Manager documentation describes Application Profiler as part of the Management Console workflow for creating application configurations. See the VMware Dynamic Environment Manager documentation and the VMware Dynamic Environment Manager resource page.

QUESTION NO: 4 - (DRAG DROP)

Match the Workspace ONE Access navigation tab on the left to Its description on the right by dragging the tab into the correct box.



ANSWER:



Tab		Description
Dashboard	Dashboard	Can be used to monitor user activity and resources used. Displays information about who signed in, which applications are being used, and how often they are being used.
Users and Groups	Users and Groups	Manage and monitor users and groups imported from your Active Directory or LDAP directory, create local users and groups, and entitle the users and groups to resources.
Catalog	Catalog	Repository for all the resources that you can entitle to users. Add Web applications and manage existing resources. In the Virtual Apps Collection page, you manage Horizon, Citrix, Horizon Cloud, and ThinApp desktops and application integrations.
Identity & Access Management	Identity & Access ...	Set up and manage the directory service, authentication methods, access policies, and preferences. Configure Okta and Workspace ONE UEM settings to integrate with Workspace ONE Access.

Explanation:

Workspace ONE Access organizes administrative tasks into navigation areas that align with the four descriptions shown. **Dashboard** is the administrative overview page, so it is used to monitor activity and resources and to see information about signed-in users, the applications they use, and how often they use them. This provides the operational visibility described in the prompt. VMware's Workspace ONE Access documentation describes the console as the place for administrators to manage the service and monitor its use; see the Workspace ONE Access documentation.

Users and Groups is the area for managing identities and group membership. It supports users and groups imported from Active Directory or LDAP and also supports local users and groups. Entitling users and groups to resources is part of this identity-management workflow. **Catalog** is the resource and application delivery area. It contains resources to which users can be entitled, supports web applications, and centralizes integrations with virtual-app and application sources such as Horizon, Citrix, Horizon Cloud, and ThinApp. This is why the resource repository and application-management description belongs to Catalog.

Identity & Access Management contains the service-wide identity and access configuration. It is where an administrator configures directory services, authentication methods, access policies, and related preferences. It also includes identity-provider and endpoint-management integration settings, including integration with Okta and Workspace ONE UEM. VMware's identity and access management guidance covers these administrative concepts. Therefore, each tab maps to the description matching its defined management function.

QUESTION NO: 5

Which operating system is workspace ONE Tunnel not currently available for?

A. iOS

B. Linux

C. Android

D. Windows

ANSWER: B

Explanation:

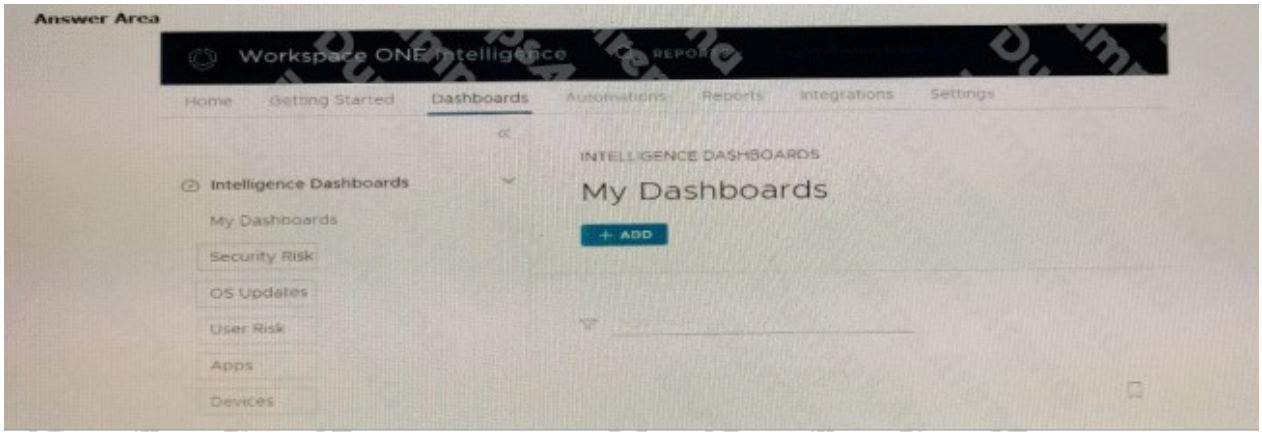
Linux is correct because Workspace ONE Tunnel is designed to provide managed mobile and desktop endpoints with secure, policy-controlled access to internal enterprise resources, but it does not provide a supported Tunnel client for Linux endpoints. The Tunnel service integrates with Workspace ONE Unified Endpoint Management and uses per-application VPN capabilities where supported, allowing managed applications to reach internal web, SaaS, and other protected resources without exposing those resources directly to the internet. VMware's Workspace ONE Tunnel documentation identifies the supported endpoint platforms and client deployment methods; Linux is absent from that supported-client scope. Therefore, an organization managing Linux devices cannot deploy Workspace ONE Tunnel as the endpoint Tunnel client in the same manner as the supported mobile and Windows platforms. Administrators should confirm platform support before designing an access architecture, especially when a workforce includes Linux devices, and use an alternative supported remote-

access or VPN solution for those endpoints. See the Workspace ONE Tunnel technical overview and the Workspace ONE Tunnel documentation for product architecture, deployment, and supported-client guidance.

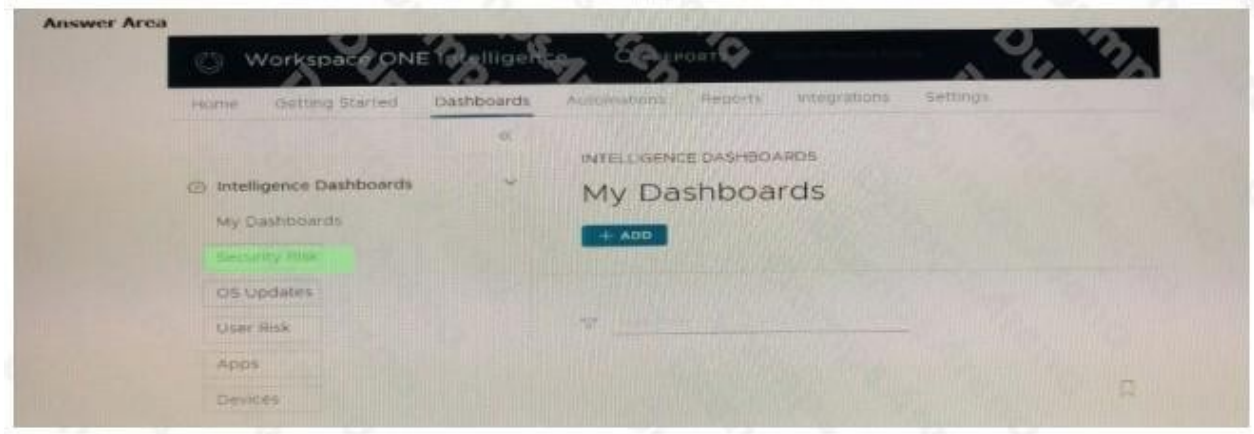
QUESTION NO: 6 - (HOTSPOT)

Click the appropriate dashboard button in the exhibit to answer the question.

Which button in the exhibit would you select to access the dashboard that can be used to view data concerning compromised devices, passcode risk, encryption status, and top risks?



ANSWER:



Explanation:

The correct selection is the **Security Risk** dashboard in the left-side Intelligence Dashboards menu. Workspace ONE Intelligence dashboards organize data by operational area, and the Security Risk dashboard is intended to provide a consolidated security posture view for managed devices. This is the appropriate place to review risk-oriented information such as compromised devices, passcode-related risk, device encryption status, and the most significant risks identified across the environment.

These metrics help an administrator quickly understand whether devices meet expected security controls and where remediation effort should be focused. A compromised-device indicator highlights devices whose integrity status may be unsafe, while passcode and encryption measures show whether important device-security requirements are being enforced. The top-risks information provides an at-a-glance prioritization of the issues affecting the fleet, making the dashboard useful for security monitoring and compliance review.

In the exhibit, click the text labeled **Security Risk**, which appears in the navigation pane on the left beneath the “Intelligence Dashboards” heading and directly under “My Dashboards.” VMware’s Workspace ONE Intelligence documentation describes dashboards as the interface for monitoring and analyzing workspace data, including security and risk-related insights. See the VMware Workspace ONE Intelligence documentation and the Workspace ONE Intelligence resource overview for additional dashboard and analytics context.

QUESTION NO: 7

Which two virtual application sources can be integrated with Workspace ONE Access by using a virtual-app collection? (Choose two.)

A. Horizon

B. Citrix

C. AirWatch Cloud Connector

D. Workspace ONE Assist

E. Apple Business Manager

ANSWER: A B

Explanation:

Horizon and **Citrix** are correct. Workspace ONE Access can integrate with Horizon environments to synchronize entitled virtual desktops and published applications into the Workspace ONE catalog. Users can then discover and launch those resources through the unified portal or Workspace ONE Intelligent Hub.

Workspace ONE Access can also integrate with supported Citrix environments through a Citrix virtual-app collection. The collection synchronizes applications and desktops available to entitled users and presents them in the Workspace ONE catalog. See the Workspace ONE Access virtual applications documentation for virtual-app collection guidance.