DUMPSQUEEN

VMware Professional Workspace ONE Exam 2019

VMware 2V0-61.19

Version Demo

Total Demo Questions: 10

Total Premium Questions: 107

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

QUESTION NO: 1

Which three occur on an Android device when it goes through Adaptive Management and becomes Workspace ONE Managed? (Choose three.)

A. The Android for Work version of VMware Workspace ONE app gets activated.

B. The Android device immediately goes through Android OS update.

C. The original VMware Workspace ONE app gets de-activated.

D. The Work folder gets created on the Android device.

E. The Android device prompts user to backup internal storage to Google Cloud.

ANSWER: A B D

QUESTION NO: 2

A topology, which includes placement of Workspace ONE service applications within layered internal networks, as well as communication workflows of requesting and receiving services, is an example of what kind of architectural design?

A. Conceptual

B. Logical

C. Virtual

D. Physical

ANSWER: B

Explanation:

Reference: https://techzone.vmware.com/resource/workspace-one-and-horizon-reference-architecture#sec14-sub3

QUESTION NO: 3

What additional permissions may be required to successfully run a telnet command across domains?

A. Membership in the local System Account group, or equivalent.

B. Domain User Membership group, or equivalent.

C. Domain Computer Membership, or equivalent.

D. Membership in the local Administrators group, or equivalent.

ANSWER: B

QUESTION NO: 4

Which are the key functionalities of Workspace ONE Intelligence? (Choose three.)

A. Content Insights

B. App Analytics

C. Mobile Analytics

D. Powerful Automation

E. Email Automation

F. Integrated Insights

ANSWER: B D F

Explanation:

Reference: https://www.vmware.com/products/workspace-one/intelligence.html

QUESTION NO: 5

Which are the two device enrollment modes in the Workspace ONE UEM console? (Choose two.)

A. Device Enrollment Program

B. Active Directory Authentication

C. Registered Devices

D. Open Enrollment

E. Token Enrollment

ANSWER: C D

QUESTION NO: 6

A customer has Office 365 that is accessible to all devices for both OWA and Active Sync. The customer wishes to restrict email access so that email is only allowed on Workspace One Managed Devices.

What are two VMware Recommended technologies to achieve this? (Choose two.)

A. VMware Secure Email Gateway

B. VMware Identity Manager

C. AirWatch Cloud Connector

D. VMware Tunnel

E. PowerShell Integration

ANSWER: A E

QUESTION NO: 7

Which Unified Access Gateway (UAG) component can use an AirWatch generated certificate for inbound SSL traffic?

A. VMware Tunnel

B. Content Gateway

C. AirWatch Cloud Connector

D. VMware Secure Email Gateway

ANSWER: B

Explanation:

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.7/content-gateway-to-unified-access-gateway-migration-guide.pdf

QUESTION NO: 8

Which two are valid options for activating a Windows VMware Identity Connector? (Choose two.)

A. Through Workspace ONE UEM

B. Through PowerShell

C. Through Installer

D. Through browser

E. Through API

ANSWER: C D

Explanation:

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/3.2/com.vmware.aw-enterpriseSystemsConn/GUID-D4BA6C74-BE9A-4249-9975A67C53282B4D.html

QUESTION NO: 9

What step is required to configure the VMware Identity Manager Connector for outbound mode?

A. Deploy VMware Unified Access Gateway and configure Reverse Proxy.

B. Ensure the connector has a valid certificate signed by a public Certificate Authority.

C. Add a built-in IdP and associate it with the connector.

D. Configure firewall rule to allow inbound TCP 443 from the Identity Manager Service.

ANSWER: C

Explanation:

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/3.1/com.vmware.aw-enterpriseSystemsConn/GUID-C97A4D37-8F1F-4B24-9A971A25A0033999.html

QUESTION NO: 10

Which is correct step to prevent unmanaged devices from accessing email through Office 365 using SEG?

A. Federate O365 with Workspace One and use access policies in Workspace One to allow only managed devices.

B. Run PowerShell commands to manually block devices.

C. Configure IP whitelisting in O365 admin console to allow only SEG's IP address and block everything else.

D. Change the default access policy in O365 to quarantine and whitelist devices enrolled in Workspace One UEM.

ANSWER: B

Explanation:

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.4/vmware-airwatch-mobile-email-management-guide.pdf