DUMPSARENA

VMware Workspace ONE 21.X Advanced Integration Specialist

VMware 5V0-61.22

Version Demo

Total Demo Questions: 10

Total Premium Questions: 60

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which two Workspace ONE UEM services require persistence on the load balancers to support an environment of 25,000 devices? (Choose two.)

A. Workspace ONE Intelligence

B. Secure Email Gateway

C. Device Services

D. AirWatch Cloud Connector

E. Dell Factory Provisioning

ANSWER: C D

QUESTION NO: 2

Which combination of authentication challenges does an integration of RSA SecurID in Workspace ONE Access provide to protect resources?

A. Password and PIN

B. Password, PIN, and biometrics

C. Password and biometrics

D. Password, email, and biometrics

ANSWER: B

QUESTION NO: 3

Which statement accurately describes modem claims-based identity management?

A. It supports multiple authentication methods except Single Sign-On

B. It doesn't support multiple providers

C. It requires the application to perform the authentication task

D. It makes account management easier by centralizing authentication

ANSWER: D

QUESTION NO: 4

Which two considerations should be noted when designing a Workspace ONE environment? (Choose two.)

A. Installing all product components

B. Testing environment

C. Involving stakeholders

D. Defining business drivers

E. Configuring integrations

ANSWER: C D

QUESTION NO: 5

Which two solutions needs to be integrated for an administrator to have conditional access with User Risk Score? (Choose two.)

A. Workspace ONE Hub Services

B. Workspace ONE SASE

C. Workspace ONE Assist

D. Workspace ONE Access

E. Workspace ONE Intelligence

ANSWER: D E

QUESTION NO: 6

Which three configurations are managed in the identity provider (IdP) settings in VMware Workspace ONE Access? (Choose three.)

A. Authentication Methods

B. Directory

C. Automation Methods

D. Group Attributes

E. Networks

F. User Attributes

ANSWER: A B F

QUESTION NO: 7

A VMware Workspace ONE administrator and the Information Security Officer reported that the Unified Access Gateway (UAG) front-end network is compromised. The compromised device was reconfigured to bypass the UAG.

Why did this action fail in a two-NIC deployment?

A. The UAG combines layer 5 firewall rules with layer 7 Unified Access Gateway security

B. The UAG combines layer 4 firewall rules with layer 7 Unified Access Gateway security

C. The UAG combines layer 3 firewall rules with layer 7 Unified Access Gateway security

D. The UAG combines layer 2 firewall rules with layer 7 Unified Access Gateway security

ANSWER: B

QUESTION NO: 8

An administrator of iOS supervised devices has noticed that devices are checking in regularly but are failing the Last Compromised Scan compliance policy. The administrator is fine with having slight disruptions to users but does not want any interaction from the user to be required.

The administrator decides to use an action in the Last Compromised Scan compliance policy that would force the device to report back the compromised status without requiring user input.

Which action m the Last Compromised Scan compliance policy should be used?

A. Assign a sensor to the device to request the compromised status

B. Assign the command to Request Device Check-In

C. Assign a push notification to the device to request the compromised status

D. Assign a compliance profile containing a single app payload for the Hub application

ANSWER: C

QUESTION NO: 9

Which feature limits the number of changes that can be made to Users and Groups when updating directories in VMware Workspace ONE Access?

A. UEM Security PIN

B. Default Action For Inactive Users

C. Conditional Group Sync

D. Directory Sync Safeguard

ANSWER: D

QUESTION NO: 10

Which two options are valid when managing directories m VMware Workspace ONE Access through the Manage > Directories page? (Choose two.)

A. Enable Password Recovery Assistant

B. Schedule the sync frequency

C. Configure Kerberos Auth Service

D. Change the mapped attributes list

E. Manage built-in identity provider for User Auth

ANSWER: B D