5V0-61.22 Q&As

VMware Workspace ONE 21.X Advanced Integration Specialist

Pass VMware 5V0-61.22 Exam with 100% Guarantee

Following Questions and Answers are all new published by VMware Official Exam Center

QUESTION 1

Users are able to seamlessly log into VMware Workspace ONE Access with Kerberos and then launch Horizon apps without a prompt for credentials. What must be enabled to support this feature?

A. Certificate (Cloud Deployment)

B. Password Caching

C. True SSO

D. Identity Bridging

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-administration/GUID-2590854E-483F-4A26-AE56-D45BB948906C.html

---

QUESTION 2

An organization wants to allow users to connect to VMware Horizon desktop or application pools from a Horizon Pod deployed on their internal network by selecting the Horizon resources from the Unified Catalog of their Workspace ONE Access shared SaaS tenant.

Which setting must an organization administrator make to achieve this goal?

A. Set authentication method in VMware Horizon to ADFS Authenticator = Allowed on all Horizon Connection Servers in the Horizon Pod

B. Enable the Virtual App Service on all Unified Access Gateway systems that allow users to connect to Horizon pools from the Horizon Pod

C. Enable the VMware Tunnel on all Unified Access Gateway systems that allow users to connect to Horizon pools from the Horizon Pod

D. Set "Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)" to "Allowed" on all Horizon Connection Servers in the Horizon Pod

Correct Answer: D

Reference: https://techzone.vmware.com/resource/workspace-one-access-architecture

---

QUESTION 3

Which two actions are valid based on identified risk behaviors in VMware Workspace ONE Intelligence Risk Analytics? (Choose two.)

A. Add authentication methods to the user or device with VMware Workspace ONE Access integration

B. Delete all previous risk scoring for the user

C. Move the user to the "very high" risk category

D. Monitor the device or user

E. Add authentication methods to the user or device with VMware Workspace ONE UEM integration

Correct Answer: DE

QUESTION 4

An organization wants to prevent users from connecting to VMware Horizon desktop or application pools from a Horizon Pod deployed on their internal network unless the user selects the Horizon pool from the Unified Catalog of their Workspace ONE Access shared SaaS tenant.

Which additional setting must the organization administrator configure?

A. Enable the Virtual App Service on al Unified Access Gateway systems that allow users to connect to Horizon pools from the Horizon Pod

B. Configure the Workspace ONE Access tenant as a SAML 2.0 authenticator on all Horizon Connection Servers in the Horizon Pod

C. Enable the VMware Tunnel on all Unified Access Gateway systems that allow users to connect to Horizon pools from the Horizon Pod

D. Set "Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)" to "Allowed" on all Horizon Connection Servers in the Horizon Pod

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-Access/22.09/ws1-access-resources.pdf

QUESTION 5

A leadership team would like to enable VMware Workspace ONE Notifications with Hub Services so push notifications can occur to the end-user devices. Which types of notifications are sent?

A. Immediate and Instructive

B. Actionable and Informational

C. Informational and Immediate

D. Instructive and Actionable

Correct Answer: D