



**Free Questions for 5V0-61.22 by certsinside**

**Shared by Pope on 15-04-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

## Question 1

---

**Question Type:** MultipleChoice

---

An administrator is configuring authentication n VMware Workspace ONE Access and will be using an authentication method that will not require the use of VMware Workspace ONE Access Connector.

Which authentication method is being used?

**Options:**

---

- A- RSA SecurID
- B- Kerberos Auth service
- C- User Auth service
- D- VMware Verify

**Answer:**

---

D

## Question 2

---

**Question Type: MultipleChoice**

---

Which service of the VMware Workspace ONE Access Connector Server requires inbound connectivity?

**Options:**

---

- A- Directory Sync Service
- B- Virtual App Service
- C- User Auth Service
- D- Kerberos Auth Service

**Answer:**

---

C

## Question 3

---

**Question Type: MultipleChoice**

---

Which statement about VMware Workspace ONE Access with other VMware Workspace ONE product integrations is accurate?

### Options:

---

- A-** VMware Workspace ONE Trust Network includes several security solutions that can be integrated with VMware Workspace ONE Access, which can provide a consolidated view of all threats reported by the various security solutions
- B-** VMware Workspace ONE Assist can be integrated with VMware Workspace ONE Access to provide administrators the ability to seamlessly launch remote management sessions for eligible devices from the VMware Workspace ONE Access console
- C-** AirWatch Cloud connector can be integrated with VMware Workspace ONE Access to act as a proxy for users to access internal resources
- D-** VMware Workspace ONE Access can be integrated with VMware Workspace ONE Intelligence to provide insights on user logins and application launches

### Answer:

---

D

## Question 4

---

### Question Type: MultipleChoice

---

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

**Options:**

---

- 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

**Answer:**

---

D, E

## Question 5

---

**Question Type: MultipleChoice**

---

Which two virtual desktop infrastructures (VDI) are supported as an integration in VMware's Anywhere Workspace with the VMware Workspace ONE Access Connector v21.08+? (Choose two.)

**Options:**

---

- A- Citrix
- B- V2 Cloud
- C- Workspot
- D- ThinApp
- E- Horizon

**Answer:**

---

A, E

## Question 6

---

**Question Type:** MultipleChoice

---

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?

**Options:**

---

- A- Immediate and Instructive
- B- Actionable and Informational
- C- Informational and Immediate
- D- Instructive and Actionable

**Answer:**

---

D

## Question 7

---

**Question Type:** MultipleChoice

---

A company has applications deployed in separate networks/locations which are managed by different identities. The company needs a technology that can empower the admin to securely provide Single Sign-on (SSO) experience to end-users across the board among these applications.

Which technology should be recommended?

**Options:**

---

- A- Delegated Authentication
- B- Basic Authentication
- C- Legacy Authentication
- D- Claims-Based Authentication

**Answer:**

---

D

## Question 8

---

**Question Type:** MultipleChoice

---

An administrator is attempting to create a magic link in VMware Workspace ONE Access for day zero onboarding. After building the REST API request, the administrator receives the following status code:

409 - token.auth.token.already.exists

How should the administrator interpret this error?

**Options:**

---



- A- The request served successfully
- B- The user does not belong to the AD group that was configured for the token
- C- A user could not be identified using the parameters passed in the body
- D- A token was already generated for the user, so a fresh one cannot be generated

**Answer:**

---

D

## Question 9

---

**Question Type:** MultipleChoice

---

An administrator is setting up a new integration between VMware Workspace ONE UEM and VMware Workspace ONE Access.

Which settings need to be configured in the VMware Workspace ONE UEM console?

**Options:**

---

- A- Kerberos admin key, import the Kerberos Admin account, and the admin auth certificate for VMware Workspace ONE Access

- B-** REST API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access
- C-** SOAP API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access
- D-** Certificate API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access

**Answer:**

---

B

## Question 10

---

**Question Type:** MultipleChoice

---

Which category setting of Citrix-published resources is supported in VMware Workspace ONE Access?

**Options:**

---

- A-** Syncing
- B-** Nested categories
- C-** StoreFront Filtering
- D-** Tagging

**Answer:**

---

C

## Question 11

---

**Question Type:** MultipleChoice

---

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 in the Last Compromised Scan compliance policy should be used?

**Options:**

---

- 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 12

---

**Question Type: MultipleChoice**

---

A customer has asked for recommendations around a disaster recovery architecture design for VMware Workspace ONE Access. The customer has an extremely aggressive recovery point objective and recovery time objective.

Which HA/DR design should be recommended, given the supported options?

**Options:**

---

**A-** Multi-datacenter design with two 3-node clusters, One 3-node cluster Datacenter 1 and the other 3-node cluster m Datacenter 2. The two 3-node clusters are setup in an active/passive configuration.

**B-** Multi-datacenter design with two 3-node clusters. One 3-node cluster Datacenter 1 and the other 3-node cluster m Datacenter 2. The two 3-node clusters are setup in an active/active configuration.

**C-** Multi datacenter design with two 3-node clusters, Both 3-node clusters are spanned across both datacenters, two nodes in one

datacenter and one in the other, respectively. The two 3-node clusters are setup in an active/active configuration.

**D-** Multi-datacenter design with two 3-node clusters, Both 3-node clusters are spanned across both datacenters, two nodes in one datacenter and one in the other, respectively. The two 3-node clusters are setup in an active/passive configuration.

**Answer:**

---

C

**To Get Premium Files for 5V0-61.22 Visit**

**<https://www.p2pexams.com/products/5v0-61.22>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/vmware/pdf/5v0-61.22>**

