HIGHER QUALITY
BETTER SERVICE

CERTTREE

QUESTION & ANSWER

Provide One Year
Free Update!

https://www.certtree.com

Exam : **5V0-61.22**

Title : VMware Workspace ONE 21.X Advanced Integration Specialist

Version : DEMO

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

2.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,D,F

3.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?
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: B

4.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: C

5.An administrator has enabled and configured Kerberos in the VMware Workspace ONE Access console, but the connection test fails.
What is one reason this connection failed to authenticate?
A. The Linux machine on which the Kerberos Auth service is installed was not joined to the domain
B. The certificate was not enabled on VMware Workspace ONE UEM console
C. The Kerberos Auth service are incorrectly configured on the AirWatch Cloud Connector
D. The certificate is unsigned by a trusted SSL or public or internal certificate authority
Answer: A
Explanation:
For Kerberos authentication to work, the Linux machine hosting the Kerberos Auth service must be joined to the domain. Without domain membership, the Kerberos Auth service cannot authenticate users.