Welcome to Cert007 - Your Ultimate IT Certification Partner

- Real Exam Questions
- Free Updates
- Expert Support
- Instant Access
- Money-Back Guarantee

Visit us at **https://www.cert007.com/** for more information

Exam : **3V0-12.26**

Title : VMware Certified Advanced Professional - VMware Cloud Foundation Architect

Version : DEMO

1.An Enterprise IT Strategist is designing a cyber recovery strategy for a healthcare organization. They must configure the VMware Live Cyber Recovery snapshot retention policies to align with business requirements.
Cyber Recovery Strategy Overview
Regulatory Requirement: 6 months immutable backups
Monthly Budget Cap: $50,000 USD
Workload Churn: 500GB daily delta (Patient Systems)
Assumed Threat Dwell Time: 90 Days
Which THREE design decisions provide the most appropriate trade-off to meet these constraints while providing a robust ransomware recovery posture? (Select all that apply.)
A. Exclude non-critical application logs and temporary development databases from the Live Recovery protection groups to reduce the cloud storage footprint.
B. Utilize the Live Recovery Cloud Connector to replicate the active vSAN ESA storage policies directly to the public cloud to maintain parity.
C. Configure a high-frequency hourly snapshot schedule with a strict 6-month retention lock for all patient data systems to ensure the most granular recovery points possible.
D. Implement a tiered retention policy: retain daily snapshots for 14 days, weekly snapshots for 3 months, and monthly snapshots up to 6 months.
E. Leverage VMware Live Cyber Recovery's inherent delta-based (incremental-forever) snapshot architecture to minimize the storage impact of the high daily churn.
Answer: A, D, E

2.A VCF Solutions Architect is documenting the disaster recovery procedures for the Management Domain. A catastrophic storage array failure destroys all three nodes of the NSX Manager cluster, though the vCenter Server and SDDC Manager survived on a separate datastore.
The architect must execute a restoration from the external SFTP backup server.
How must the architect structure the NSX Manager cluster recovery process?
[Hardware_Symptom_Report]
- NSX Node 1: Unrecoverable VMFS corruption.
- NSX Node 2: Unrecoverable VMFS corruption.
- NSX Node 3: Unrecoverable VMFS corruption.
A. Deploy a single new NSX Manager node, restore the cluster database from the SFTP backup to this single node, and then scale out the cluster by joining two additional fresh nodes.
B. Restore the three original NSX Manager virtual machines from hypervisor-level snapshot backups and execute the nsxcli cluster re-init command to force a new quorum.
C. Deploy three fresh NSX Manager virtual appliances simultaneously via the SDDC Manager UI and point all three to the SFTP server to trigger a parallel distributed restore.
D. Deploy a single NSX Manager node, manually recreate the Tier-0 gateway, and then initiate an "Import Configuration" task from the SDDC Manager to synchronize the remaining state.
Answer: A

3.A Cloud Operations Engineer is troubleshooting access issues following the successful configuration of Identity Provider (IdP) Federation (using Okta via OIDC) for the vCenter Server.
[Authentication_Failure_Report]

- User A (Okta) successfully logs in via web browser, but has 0 permissions.
- User B attempts an API script execution and fails to authenticate.
- Administrator cannot run SDDC Manager host commissioning workflows.

Which THREE statements accurately describe the underlying token handling, RBAC mapping, and troubleshooting realities of vCenter Identity Federation? (Select all that apply.)

A. Disabling the native vsphere.local domain is a required security step once an external Identity Provider is successfully federated and configured.

B. If the LDAPS certificate on the Active Directory server is renewed and changes, vCenter SSO will automatically accept the new certificate via the 'Trust on First Use' (TOFU) protocol without administrative intervention.

C. If the external Identity Provider (e.g., Okta) becomes unreachable, administrators can still authenticate using the local administrator@vsphere.local account, as it is evaluated natively by vCenter SSO.

D. SDDC Manager workflows (like host commissioning) will fail if the internal vCenter SSO STS (Security Token Service) certificate is expired, as SDDC Manager relies heavily on internal STS tokens for API authentication, regardless of the external IdP.

E. When using Identity Federation (OIDC/SAML), the external IdP handles the authentication challenge, but vCenter Server still internally maps the returned user claims (groups) to local vSphere RBAC permissions; User A likely lacks a vSphere role mapping.

Answer: C, D, E

4.An NSX Network Engineer is reviewing the automated configurations applied by SDDC Manager immediately after the successful completion of a "Stretch Cluster" workflow. The cluster was stretched from Site A to Site B.

Which TWO specific configurations does SDDC Manager automatically apply to the vSphere/vCenter environment to ensure proper virtual machine placement and fault domain isolation? (Choose 2.)

A. It creates vSphere DRS Host Groups (one for Site A hosts, one for Site B hosts) and corresponding "Should Run" VM/Host affinity rules to enforce localized compute execution.

B. It configures a dedicated vSphere Replication appliance on the Site B hosts to asynchronously mirror the virtual machine RAM state back to Site

A. C. It creates two active vSAN Fault Domains ("Preferred" for Site A and "Secondary" for Site B) and places the respective ESXi hosts into them.

D. It automatically deletes the localized NSX Tier-1 gateways and replaces them with a singular Global Tier-0 gateway spanning both sites.

E. It automatically alters the NSX Distributed Firewall "Default Deny" rule to allow synchronous storage traffic between the two vSAN Fault Domains.

Answer: A, C

5.A Cloud Operations Engineer is provisioning a storage policy for a new set of mission-critical databases within a 16-node vSAN cluster. The ESXi hosts are physically distributed evenly across 4 racks (4 hosts per rack). The business requirement mandates that the databases must remain accessible even if an entire physical rack loses power.

Review the proposed vSAN storage policy configuration:

[Storage_Policy: Mission_Critical_DB]

Site disaster tolerance: None - standard cluster
Failures to tolerate (FTT): 1 failure - RAID-1 (Mirroring)
Number of disk stripes per object: 1
Flash Read Cache reservation: 0%
Force provisioning: False
Assuming the 4 physical racks are correctly configured as 4 distinct vSAN fault domains, what is the architectural outcome of applying this policy to the databases?
A. The database becomes inaccessible during a rack failure because, in vSAN storage policies, RAID-1 mirroring with FTT=1 does not leverage explicit fault domain awareness; this capability activates only when configured with FTT=2 or higher.
B. The database survives a single rack failure because vSAN places two replicas and a witness component across three distinct fault domains.
C. The policy guarantees survival against two simultaneous rack failures due to the cluster's size of 16 hosts, which significantly exceeds the minimum host requirement of 3 for an FTT=1 configuration.
D. The policy application fails because an FTT=1 configuration with explicit fault domains in vSAN requires a minimum of 5 fault domains to properly place the witness component and maintain quorum.
Answer: B