PassQueen
a.k.a dumpsqueen.com

Dell VxRail Deploy Exam

EMC D-VXR-DY-01

Version Demo

Total Demo Questions: 6

Total Premium Questions: 61

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, VxRail Concepts and Architecture	9
Topic 2, VxRail Planning	23
Topic 3, VxRail Installation	17
Topic 4, VxRail Post-Installation	12
Total	61

QUESTION NO: 1

When will local updates be the preferred option to update a VxRail cluster?

A. When using a customer provided vCenter.

B. When working at a dark site.

C. When a proxy server is required.

ANSWER: B

Explanation:

When working at a dark site is correct because a dark-site VxRail environment is isolated from, or tightly restricted from accessing, external networks and Dell online repositories. In this situation, the required VxRail composite bundle must be obtained through an approved connected system, transferred into the restricted environment according to the organization's security process, and uploaded locally for VxRail Manager to use during lifecycle management. This allows the cluster to remain on a Dell-validated software and firmware baseline while respecting air-gap, security, and compliance controls. Local update workflows are therefore essential for performing planned upgrades and applying supported platform updates where direct connectivity cannot be used. Before beginning the update, administrators should obtain the bundle that matches the cluster's supported upgrade path, verify bundle integrity, confirm the applicable release notes and prerequisites, and allow VxRail Manager prechecks to validate cluster readiness. Dell publishes VxRail documentation and release-specific lifecycle guidance through its VxRail support documentation portal and support site. See the Dell VxRail documentation page and Dell VxRail upgrade guidance.

QUESTION NO: 2

Refer to the exhibit.



Which selection in the VxRail deployment wizard leads to the displayed locked option?

A. Customer-managed vCenter Server

B. vSAN 2-Node Cluster

C. Stretched Cluster

D. VxRail-managed vCenter Server

ANSWER: A

Explanation:

Customer-managed vCenter Server is correct. Selecting this deployment model means the VxRail cluster will register with and be managed through an existing vCenter Server that is operated as part of the customer's environment. The deployment therefore depends on customer-provided infrastructure services, including DNS, to resolve the FQDNs required by VxRail hosts, vCenter components, and other management services.

For this architecture, the VxRail deployment wizard enforces use of an external DNS service rather than the internal DNS capability supplied by VxRail Manager. This is why the DNS selection shown in the exhibit is locked to *External*. The locked setting ensures that the cluster's name-resolution configuration is aligned with the external management environment from the beginning of deployment, which is essential for consistent service discovery and management-plane communication.

Dell's VxRail documentation describes customer-managed vCenter as a supported deployment topology and identifies the network and DNS prerequisites that must be satisfied during deployment. See the VxRail Support Matrix and Dell's VxRail product documentation for deployment guidance and current requirements.

QUESTION NO: 3

Which two types of key provider are supported in vSAN ESA using a VxRail-managed vCenter Server? (Choose two.)

A. Standard Key Provider with TPM 1.2 protected hosts

B. Native Key Provider with TPM 1.2 protected hosts

C. Native Key Provider

D. Standard Key Provider

ANSWER: C D

Explanation:

Native Key Provider and **Standard Key Provider** are the supported key-provider types for vSAN Express Storage Architecture when the cluster uses a VxRail-managed vCenter Server. vSAN encryption requires vCenter Server to provide and manage cryptographic keys through a configured key provider. The Native Key Provider is integrated into vCenter Server and enables vSAN encryption without requiring an external key-management server. It creates and maintains the necessary key material within the vCenter environment; its configuration includes taking and safely retaining a Native Key Provider backup.

The Standard Key Provider is used when an organization needs vCenter Server to obtain encryption keys from an external, KMIP-compliant key-management server. This model is appropriate where enterprise security policy, centralized key custody, separation of duties, or existing key-management infrastructure requires an external KMS. Once either supported provider type is configured and trusted by vCenter Server, it can be selected for vSAN encryption services for the ESA cluster. VMware documents both native and standard key-provider models in its vSphere key-management guidance and describes their use with vSAN encryption. See the vSphere Encryption and Key Management documentation and the vSAN Encryption documentation.

QUESTION NO: 4

A VxRail deployment will carry management, vSAN, vMotion, and virtual-machine traffic across the host uplinks. Which three switch-port preparations are appropriate on the ports connected to VxRail nodes? (Choose three.)

A. Configure the ports as VLAN trunk ports.

B. Allow the required VxRail VLANs on the trunks.

C. Configure the ports as Spanning Tree edge ports.

D. Configure the ports as single-VLAN access ports.

E. Require a dynamic LACP LAG for every VxRail deployment.

ANSWER: A B C

Explanation:

VxRail node-facing switch ports must carry the required VLAN-tagged traffic, so they should operate as trunk ports and permit the VLANs defined in the network plan. When Spanning Tree Protocol is used, host-facing interfaces should be configured as edge ports so they can transition to forwarding without normal switch-to-switch convergence delays.

Access mode permits only one VLAN and is unsuitable for a host uplink carrying multiple VxRail networks. A LAG is optional and depends on the selected network design; it is not a universal requirement for every VxRail node-facing port.

QUESTION NO: 5

What are three planning considerations when using a customer-supplied vCenter Server? (Choose three.)

A. Includes a standard vCenter license.

B. Requires an external DNS server.

C. Requires a separate vCenter license.

D. Uses customer-defined procedures for vCenter software upgrades.

E. Uses VxRail Lifecycle Management for vCenter software upgrades.

ANSWER: B C D

Explanation:

A customer-supplied vCenter Server is an external vCenter instance that is owned, operated, and licensed separately from the VxRail cluster. Therefore, the deployment requires a separate vCenter license. The vCenter entitlement bundled with a VxRail deployment is intended for the VxRail-managed vCenter deployment model and does not supply licensing for an independently provided vCenter Server.

The design also requires an external DNS server. Reliable forward and reverse DNS resolution is a prerequisite for the VxRail deployment workflow and for communication among the VxRail nodes, ESXi hosts, VxRail Manager, vCenter Server, and supporting services. DNS records should be planned and validated before deployment so that management components can resolve the required names and addresses consistently.

Finally, a customer-supplied vCenter Server uses customer-defined procedures for vCenter software upgrades. Because that vCenter instance is external to VxRail management, the customer plans, performs, and validates its vCenter lifecycle operations according to VMware guidance and their change-management process. VxRail lifecycle management continues to manage supported VxRail software and firmware components, while the external vCenter lifecycle remains a customer responsibility. Dell's VxRail documentation is available through the Dell VxRail documentation portal; VMware also documents vCenter Server administration in the vSphere documentation.

QUESTION NO: 6

What is a difference between vSAN Data-in-Transit Encryption and vSAN Data-At-Rest Encryption?

A. Data-In-Transit Encryption: Does not require a Key Management Server.Data-At-Rest Encryption: Requires a Key Management Server.

B. Data-In-Transit Encryption: Key Management Server must reside on the vSAN cluster.Data-At-Rest Encryption: Key Management Server can reside on the vSAN cluster.

C. Data-In-Transit Encryption: Encrypts data after it is written to the datastore.Data-At-Rest Encryption: Encrypts data as it moves between hosts.

D. Data-In-Transit Encryption: Encrypts traffic between VMs and the VxRail nodes.Data-At-Rest Encryption: Encrypts traffic between VxRail nodes only.

ANSWER: A

Explanation:

Data-In-Transit Encryption: Does not require a Key Management Server.

Data-At-Rest Encryption: Requires a Key Management Server. This accurately distinguishes the key-management requirements of the two vSAN encryption capabilities. Data-in-transit encryption protects vSAN traffic exchanged between ESXi hosts across the vSAN network. The hosts establish and use transient encryption keys for this host-to-host communication, so enabling this feature does not require deployment of an external KMS. It is intended to protect data while it is moving over the vSAN transport network, rather than to encrypt guest-to-host or general virtual-machine network traffic.

Data-at-rest encryption protects data persisted on vSAN storage devices, including data on cache and capacity devices. Because the encryption must remain recoverable after events such as host restarts or disk replacement, vSAN needs managed encryption keys. In traditional deployments, those keys are provided through a KMIP-compatible Key Management Server. Current vSphere releases can also use VMware Native Key Provider where supported, but the essential distinction tested is that data-at-rest encryption requires key-provider infrastructure, whereas data-in-transit encryption does not require an external KMS. Dell's VxRail documentation and VMware's vSAN encryption guidance describe these encryption models and their respective key-management behavior. See VMware vSAN Encryption and Dell VxRail Product Documentation.