PassQueen
a.k.a dumpsqueen.com

Dell PowerProtect Cyber Recovery Deploy v2 Exam

EMC D-PCR-DY-01

Version Demo

Total Demo Questions: 5

Total Premium Questions: 58

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, PowerProtect Cyber Recovery Concepts	22
Topic 2, PowerProtect Cyber Recovery Installation	18
Topic 3, PowerProtect Cyber Recovery Configuration	7
Topic 4, PowerProtect Cyber Recovery Administration	8
Topic 5, PowerProtect Cyber Recovery Troubleshooting	3
Total	58

QUESTION NO: 1

Before an upgrade window, an administrator runs the PowerProtect Cyber Recovery upgrade precheck to identify conditions that could prevent a supported upgrade.

Which three conditions are checked by the upgrade precheck? (Choose three.)

A. The crso user credentials are correct.

B. The Cyber Recovery registry service has a running status.

C. There is compatibility with upgrades from the current version.

D. No jobs are running in the production environment.

E. There is a minimum of 2 GB of free space.

ANSWER: A B C

Explanation:

The upgrade precheck validates that the **crso user credentials are correct**, that the **Cyber Recovery registry service is running**, and that the **installed version has a supported upgrade path**. These checks verify access, required service availability, and release compatibility before upgrade changes are made. Free-space and production-job conditions may be operational considerations, but they are not the specified checks in this precheck.

QUESTION NO: 2

Which is the best practice when securing PowerProtect Data Domain in Dell PowerProtect Cyber Recovery vault?

A. Disable HTTP access to all PowerProtect Data Domain network ports

B. Disable SSH access to all Dell PowerProtect Data Domain network ports except from help desk jump host

C. Disable port 2051 on all PowerProtect Data Domain network ports

D. Disable ports 80, 443, and 2049 on the PowerProtect Data Domain

ANSWER: B

Explanation:

Disable SSH access to all Dell PowerProtect Data Domain network ports except from help desk jump host is the appropriate best practice because it limits administrative access to a tightly controlled, auditable management path. In a Cyber Recovery vault, the Data Domain system contains protected recovery copies and must be isolated from routine production administration. Allowing SSH only through a designated jump host reduces the attack surface and lets the organization apply additional controls at one access point, such as multifactor authentication, privileged-access workflows, session logging, source-IP restrictions, and enhanced monitoring. The jump host should itself be hardened, monitored, and accessible only to authorized administrators. This approach supports the Cyber Recovery security model of minimizing connectivity to vault assets while preserving secure access for essential support and operational tasks. Dell's Cyber Recovery documentation emphasizes isolated vault infrastructure and controlled administrative access, while Data Domain security guidance supports restricting management services and access sources. See the Dell PowerProtect Cyber Recovery documentation and the Dell PowerProtect Data Domain security guidance.

QUESTION NO: 3

Before starting a Dell NetWorker recovery, the administrator needs to verify that the DDBoost user is correctly configured in both the production and Dell PowerProtect Cyber Recovery environments.

What must be confirmed about the DDBoost user to ensure a successful Dell NetWorker recovery?

A. The DDBoost user is different in the vault and production environments.

B. The DDBoost user is configured with read-only access.

C. The DDBoost user has administrative privileges.

D. The DDBoost user is the same UID in both the vault and production environments.

ANSWER: D

Explanation:

The DDBoost user must be the same UID in both the vault and production environments. During Cyber Recovery operations, NetWorker must be able to use the DD Boost credentials and associated user identity consistently when accessing the PowerProtect DD system and its protected storage. Matching the user ID preserves the identity expected by the DD Boost configuration when recovery assets are brought into, or used from, the vault environment. This consistency is particularly important because the Cyber Recovery vault is intentionally isolated from production and recovery workflows depend on preconfigured relationships among NetWorker, PowerProtect DD, and the DD Boost user. Administrators should therefore verify the numeric UID, not merely that similarly named users exist, before initiating recovery. The UID should correspond to the DD Boost account that NetWorker uses for the relevant device and storage-unit access. This validation supports a successful recovery workflow by ensuring that the vault-side configuration recognizes the same DD Boost user identity used in production. Dell documentation for the product and its deployment guides is available through the PowerProtect Cyber Recovery documentation portal; NetWorker documentation is available from the Dell NetWorker documentation portal.

QUESTION NO: 4

A customer deploying Dell PowerProtect Cyber Recovery software on Microsoft Azure.

Which two components does the ARM template create? (Choose two.)

A. Gateway

B. VNet Endpoint

C. Security Group

D. VPN

ANSWER: A C

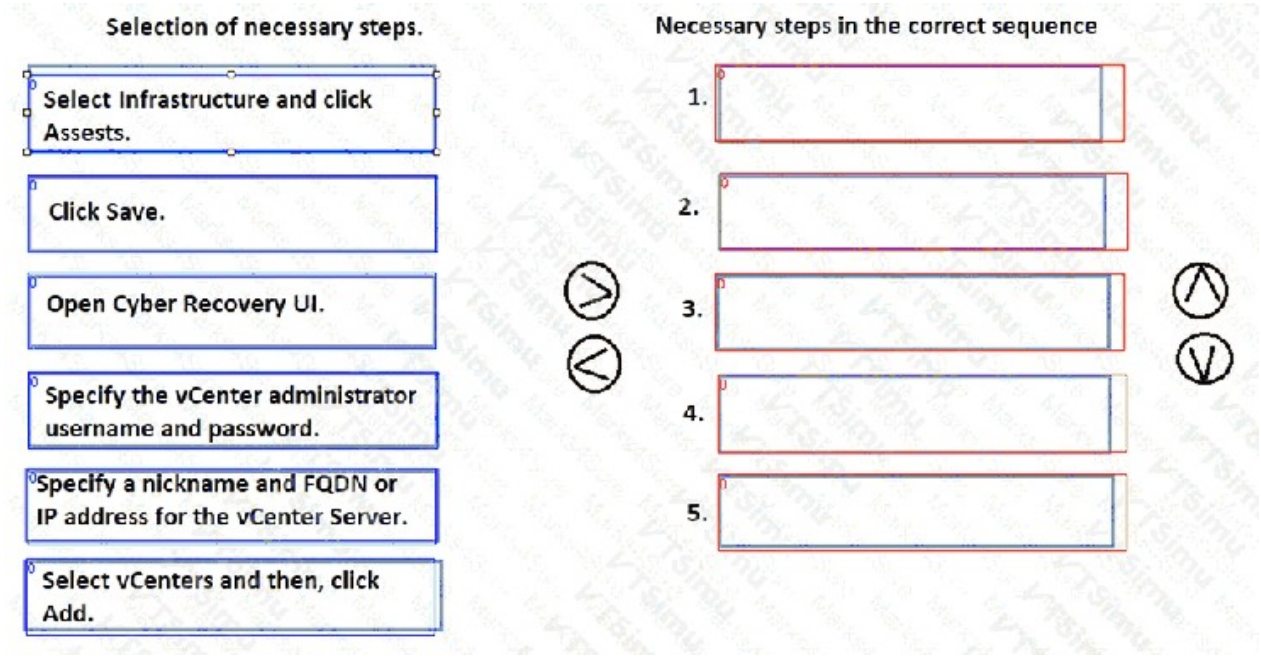
Explanation:

For a PowerProtect Cyber Recovery deployment in Microsoft Azure, the ARM template automates creation of the required Azure networking resources for the Cyber Recovery environment. The template creates the Gateway component used to provide the required controlled network connectivity for the deployment. It also creates the Security Group, which in Azure is implemented through network-security controls that define permitted inbound and outbound traffic for the Cyber Recovery resources. These resources provide a repeatable, standardized foundation for deploying the Cyber Recovery vault infrastructure rather than requiring the administrator to build the associated connectivity and security configuration manually. PowerProtect Cyber Recovery is designed to maintain an isolated recovery environment, so establishing managed network access and applying network-level security policy are essential parts of the Azure deployment workflow. Dell's PowerProtect Cyber Recovery product information is available at Dell PowerProtect Cyber Recovery. For background on the Azure deployment mechanism, see Azure Resource Manager template overview, which describes how ARM templates declaratively provision Azure infrastructure resources.

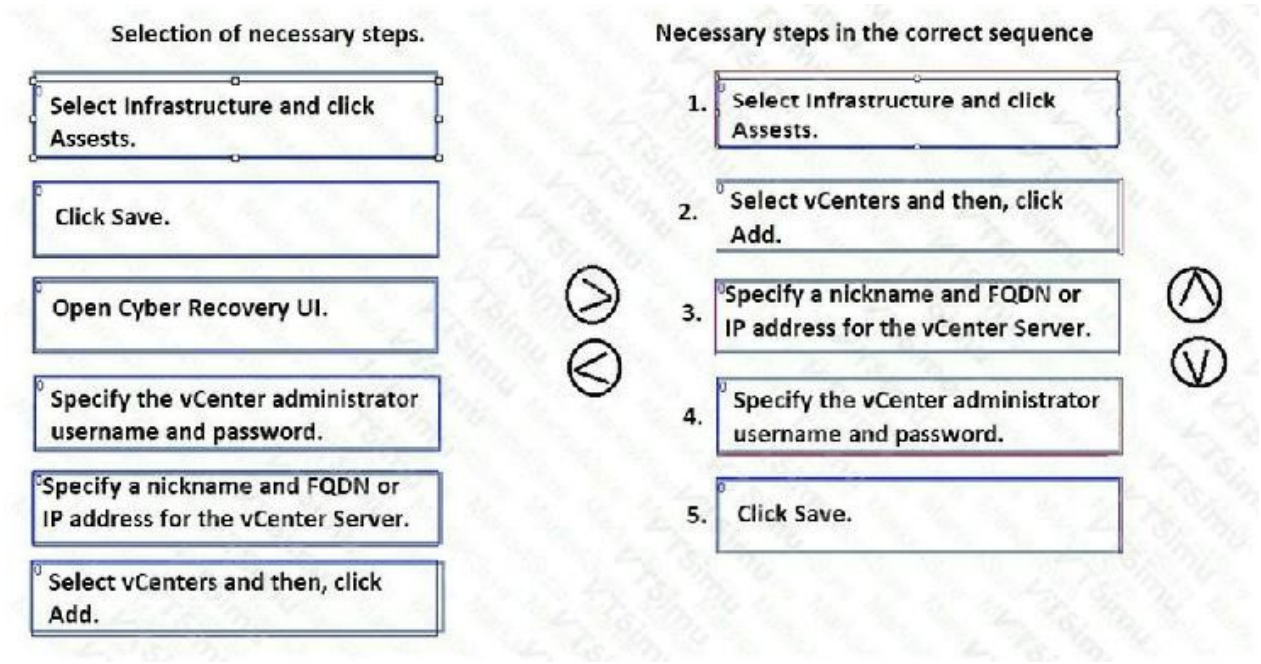
QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

When you install a vCenter Server in an on-premises Dell PowerProtect Cyber Recovery vault, you must register it with the PowerProtect Cyber Recovery software. Arrange the necessary steps in chronological order.



ANSWER:



Explanation:

Registering a vCenter Server in an on-premises PowerProtect Cyber Recovery vault is performed from the Cyber Recovery infrastructure asset-management workflow. The sequence starts by navigating to **Infrastructure** and opening **Assets**, since this is where Cyber Recovery manages the external infrastructure components it uses. Within Assets, selecting **vCenters** and clicking **Add** creates a new vCenter registration entry and opens the form for its connection settings.

The registration form first needs the identifying and network-location details: a nickname that makes the server recognizable in Cyber Recovery and the vCenter Server FQDN or IP address used to reach it. After that, the vCenter administrator username and password provide the credentials Cyber Recovery uses to authenticate to the vCenter Server and access the required inventory and operations. Selecting **Save** commits the supplied endpoint and credential information, completing the registration.

Opening the Cyber Recovery UI is naturally required before an administrator can perform the task, but it is not one of the five ordered registration actions represented by the available sequence positions. The ordered workflow therefore begins at the Infrastructure/Assets navigation point and finishes only when the new vCenter record is saved. Dell documentation identifies vCenter as an infrastructure asset managed through the Cyber Recovery UI; see the Dell PowerProtect Cyber Recovery

documentation and the PowerProtect Cyber Recovery Documentation Info Hub for the product's infrastructure and administration guidance.