DUMPSARENA

PowerProtect Cyber Recovery Exam

EMC DEP-3CR1

Version Demo

Total Demo Questions: 7

Total Premium Questions: 75

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

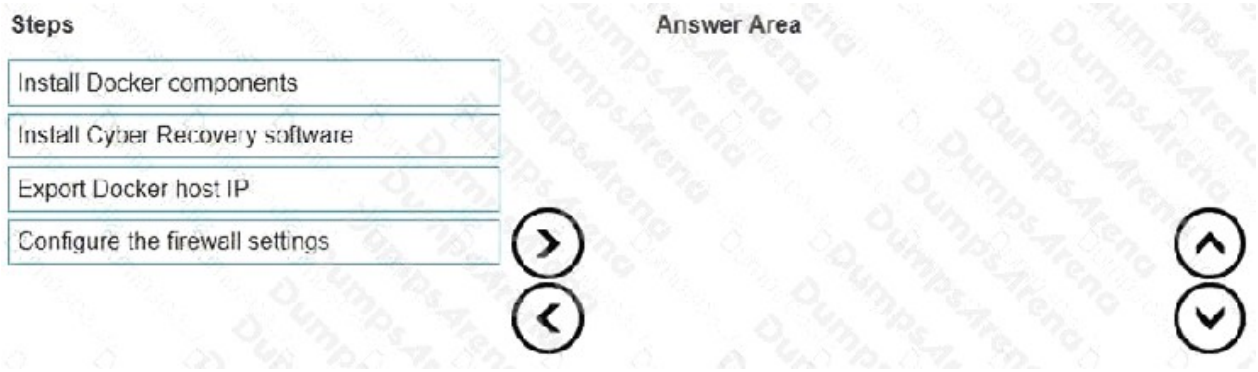
sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cyber Recovery Concepts	15
Topic 2, Cyber Recovery Solution Design	24
Topic 3, Cyber Recovery Solution Deployment	15
Topic 4, Cyber Recovery Solution Management	21
Total	75

QUESTION NO: 1 - (SIMULATION)

What is the correct sequence to install Cyber Recovery software on a physical host?



ANSWER: See the explanation for the answer

Explanation:

Correct sequence:

The firewall must permit the required Cyber Recovery communications. Docker must be installed before preparing the Docker host environment. Exporting the Docker host IP provides the required host-IP value to the Cyber Recovery installation, so it is performed before installing the Cyber Recovery software.

QUESTION NO: 2

What are the required components of a CR Vault Environment?

A. PowerProtect DD, Dedicated Network, and CR management host

B. NTP, Cyber Recovery management host, and DNS

C. Network connection, DNS, and PowerProtect DD

D. DNS, PowerProtect DD, and NTP

ANSWER: A

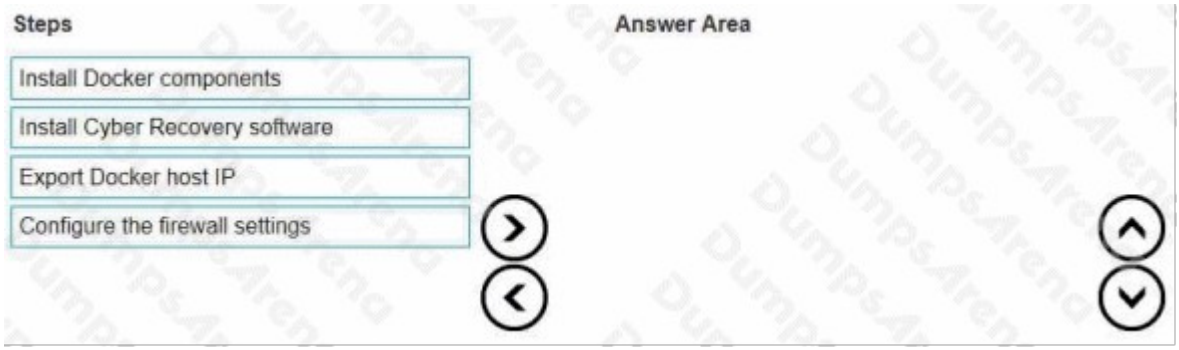
Explanation:

PowerProtect DD, Dedicated Network, and CR management host are the core components required to establish a PowerProtect Cyber Recovery vault environment. The PowerProtect DD system provides the protected storage platform in the vault and receives replicated backup data from the production environment. The dedicated network establishes the isolated vault connectivity needed for Cyber Recovery operations, helping segregate the vault from the production network and supporting the intended cyber-resilience design. The Cyber Recovery management host runs the Cyber Recovery software and provides the control plane used to configure policies, manage copies, orchestrate recovery workflows, monitor jobs, and support vault operations.

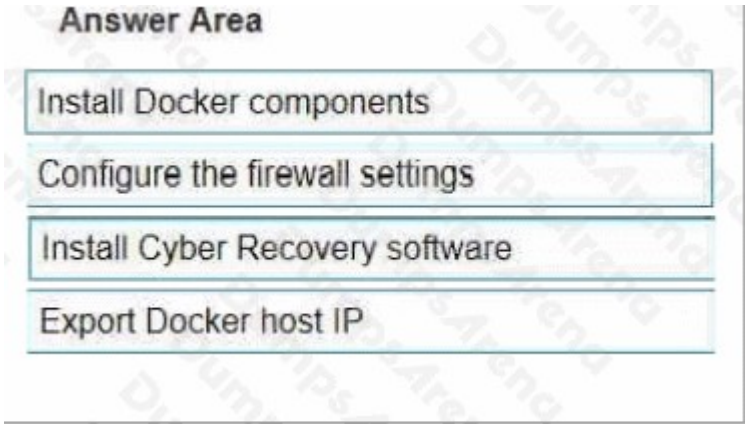
These components work together as a complete operational architecture: protected data is stored on PowerProtect DD, isolation and controlled communication are provided through the dedicated vault network, and lifecycle management is performed by the Cyber Recovery management host. Dell's Cyber Recovery documentation describes the deployment architecture, including the management host, PowerProtect DD storage, and networking requirements for vault deployments. Review the Dell PowerProtect Cyber Recovery product documentation and the PowerProtect Cyber Recovery documentation portal for the applicable release's installation and deployment guidance.

QUESTION NO: 3 - (DRAG DROP)

What is the correct sequence to install Cyber Recovery software on a physical host?



ANSWER:



Explanation:

The correct installation sequence prepares the physical operating-system host and its container platform before deploying the PowerProtect Cyber Recovery application. First, install the Docker components. Cyber Recovery on a physical host is deployed by using Docker containers, so Docker supplies the required container engine, networking, image handling, and runtime services on which the Cyber Recovery services operate.

Next, configure the firewall settings. This ensures that the physical host permits the ports and network paths required for administration, UI access, protected-storage communication, and communications among the Cyber Recovery components. Completing this host-level preparation before application deployment provides a supported and reachable environment for the Cyber Recovery installation.

After Docker and the network controls are ready, install the Cyber Recovery software. At this point, the installer can deploy the application's containerized services onto the prepared Docker host. The installation establishes the Cyber Recovery management environment that is used to create policies, run copies, and manage recovery workflows.

Finally, export the Docker host IP. Exporting this value completes the host-specific configuration used by the installed Cyber Recovery environment to identify and use the physical Docker host's address. This sequence follows the physical-host deployment workflow documented for Dell PowerProtect Cyber Recovery. Dell product documentation and installation materials are available through the Dell PowerProtect Cyber Recovery documentation portal.

QUESTION NO: 4

A customer is unable to deploy the CR Virtual Appliance. They currently use vCenter 6.5 and have 4 CPU, 8GB of memory, and 150GB of disk space available.

Why won't the virtual appliance deploy?

A. Insufficient disk space

B. Insufficient memory

C. Unsupported vCenter version

D. Insufficient CPU

ANSWER: A

Explanation:

Insufficient disk space is correct because the PowerProtect Cyber Recovery virtual appliance deployment requires more virtual-disk capacity than the 150 GB available in the stated environment. The appliance's virtual disks must be provisioned during OVA deployment, and the destination datastore must have sufficient free capacity for the complete appliance footprint. With only 150 GB available, deployment cannot reserve the required disk resources, so the OVA deployment cannot complete successfully.

The listed processor and memory resources match the baseline sizing commonly specified for the Cyber Recovery virtual appliance in the applicable deployment documentation, and vCenter Server 6.5 is within the supported VMware environment range for the relevant Cyber Recovery releases. The limiting condition in this scenario is therefore datastore capacity, not the available compute resources or the vCenter version. Before retrying deployment, the customer should select or prepare a datastore with enough free space for the appliance's required virtual disks and account for any local vSphere datastore overhead or organizational capacity reserve. Dell publishes version-specific deployment prerequisites and virtual-appliance requirements in the PowerProtect Cyber Recovery documentation. VMware also documents how datastore capacity is consumed when deploying OVF and OVA templates in the vSphere Virtual Machine Administration guide.

QUESTION NO: 5

What are the possible connection states of the CR Vault?

A. Acked, Unlocked, Unknown, Secured, and Downgraded

B. Open, Locked, Secured, Promoted, and Unknown

C. Degraded, Down, Up, Running, and Maintenance

D. Locked, Unlocked, Unknown, Secured, and Degraded

ANSWER: D

Explanation:

Locked, Unlocked, Unknown, Secured, and Degraded is correct because these are the connection states used by PowerProtect Cyber Recovery to represent the Cyber Recovery vault's connectivity and isolation condition. The vault design relies on controlled network isolation, allowing the recovery environment to remain separated from production except during explicitly managed operations. Cyber Recovery reports whether the vault connection is locked or unlocked, identifies a secured condition, and surfaces unknown or degraded conditions when the system cannot fully determine or maintain the expected connectivity state. These states provide administrators with an operational view of the vault's cyber-isolation posture and help them verify that the environment is in the required condition before carrying out protection, recovery, or validation activities. Monitoring this status is an important part of maintaining an air-gapped recovery workflow and confirming that vault access is controlled as intended. Dell's PowerProtect Cyber Recovery documentation and product-documentation resources describe the vault architecture, isolation model, and operational monitoring concepts: Dell PowerProtect Cyber Recovery product documentation and Dell PowerProtect Cyber Recovery overview.

QUESTION NO: 6

What must be considered when planning and implementing a secure Cyber Recovery Vault solution?

A. Production environment can use resources from Vault environment

B. Production environment is used to run the Cyber Recovery Management Host

C. Vault and Production infrastructure must be managed by NOC

D. Vault infrastructure is completely isolated from the Production infrastructure

ANSWER: D

Explanation:

Vault infrastructure is completely isolated from the Production infrastructure is correct because isolation is a fundamental design principle of Dell PowerProtect Cyber Recovery. The Cyber Recovery vault is intended to provide a protected, separate environment for copies of critical data that can be used for recovery after a cyberattack compromises production systems. This separation includes the vault network, management components, and protected storage, with tightly controlled and limited connectivity used only when required for replication and operational workflows. Cyber Recovery uses an automated retention-lock mechanism, known as the Cyber Recovery lock, to help ensure that vault copies remain inaccessible to an attacker who has gained control of the production environment. Planning must therefore account for a distinct security boundary, restricted administrative access, segmentation, and procedures for securely recovering data from the vault. Dell describes Cyber Recovery as isolating critical data from the production environment to preserve an immutable recovery copy and support a clean recovery. A completely isolated vault reduces the attack surface and helps prevent ransomware, compromised credentials, or destructive commands in production from reaching protected recovery assets. See Dell's PowerProtect Cyber Recovery overview and the PowerProtect Cyber Recovery documentation for architecture and deployment guidance.

QUESTION NO: 7

A Cyber Recovery policy has completed a Copy action successfully.

Which action should be used to protect the resulting copy from deletion until the configured retention period expires?

A. Lock

B. Sync

C. Analyze

D. Recover

ANSWER: A

Explanation:

Lock is correct because the Lock action applies retention protection to an eligible point-in-time copy in the Cyber Recovery vault. Retention locking helps preserve the recovery copy for its configured retention interval and strengthens protection against accidental or malicious deletion. A Sync action refreshes the source inventory, and a Copy action creates the vault copy, but neither action alone applies the configured retention lock. See the PowerProtect Data Domain overview and the Dell PowerProtect Cyber Recovery documentation.