



Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.



COH-100 Practice Questions
COH-100 Practice Test
COH-100 Practice Exam
COH-100 Exam Questions
COH-100 Study Guide



killexams.com

COHESITY

COH-100

Cohesity Certified Protection Associate - DataProtect (COH100)

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/COH-100>



Question: 1191

A company is using Cohesity to manage its data lifecycle. What is the primary function of the Cohesity CloudArchive feature?

- A. To provide real-time data access
- B. To replicate data across multiple sites
- C. To enable data deduplication
- D. To store data for long-term retention

Answer: D

Explanation: The primary function of Cohesity CloudArchive is to store data for long-term retention, allowing organizations to keep infrequently accessed data at a lower cost. The other options do not accurately describe the purpose of CloudArchive.

Question: 1192

A company is reviewing its backup service-level agreement (SLA) and wants to ensure it aligns with business needs. Which of the following best describes the purpose of a backup SLA in Cohesity DataProtect?

- A. To define the maximum amount of time allowed for a backup to complete
- B. To outline the responsibilities of the IT team in managing backups
- C. To specify the retention period for backup data
- D. To detail the acceptable recovery time objective (RTO) for all services

Answer: D

Explanation: A backup service-level agreement (SLA) specifies the acceptable recovery time objective (RTO) for services, ensuring that business continuity requirements are met. It is essential for aligning IT operations with business expectations regarding data recovery.

Question: 1193

When a Protection Group is in a 'Success' state, what additional information is available on the dashboard? (Select two)

- A. The historical trend of how long this particular task has taken to complete over time.
- B. Detailed metadata including the total size of the protected data and the number of files.
- C. The specific version of the Cohesity OS that was running at the time of the snapshot.
- D. The exact physical location of the data blocks on the underlying hardware drives.

Answer: A,B

Explanation: A successful backup status provides more than just confirmation; it reveals key data points such as the volume of data protected and the file count. Additionally, the platform tracks historical task duration, which is vital for detecting gradual performance degradation that might occur as the source dataset grows over time.

Question: 1194

You must register a new Windows Server source to the Cohesity cluster for backups. The server has strict firewall rules that allow outbound traffic only on ports 443 and 22. Which method and port combination should you use to successfully register this source?

- A. Use Cohesity agent installation over port 443
- B. Use remote script installation over port 8080
- C. Use SSH agent installation over port 22
- D. Use agentless registration over port 22

Answer: A

Explanation: Cohesity agent installation typically uses port 443 (HTTPS) for secure communications with the cluster. Given firewall restrictions allowing only ports 443 and 22, using the Cohesity agent over port 443 is the correct approach. SSH over port 22 is valid for Linux environments but not Windows Server agent installation. Ports 8080 and agentless registration on port 22 are not standard or supported for Windows source registration.

Question: 1195

An administrator is implementing a new protection policy and needs to ensure that all backups are compliant with regulatory requirements. What should the administrator prioritize in the configuration?

- A. The retention period of backups
- B. The encryption of backup data
- C. The frequency of backups
- D. The size of the backup storage

Answer: B

Explanation: To ensure compliance with regulatory requirements, the administrator should prioritize the encryption of backup data. This protects sensitive information and meets common regulatory standards for data protection, such as GDPR or HIPAA.

Question: 1196

An organization has implemented a Cohesity cluster to protect its multi-cloud hybrid environment. The infrastructure includes a Microsoft Azure subscription with several critical virtual machines. Which requirements must be met before Azure virtual machines can be registered as a source and protected? (Select two)

- A. The Cohesity Linux Agent must be manually injected into the Azure fabric management layer via an arm template extension.
- B. The Application ID, Directory (Tenant) ID, and a valid Client Secret or certificate must be provided during the source registration process in Cohesity.
- C. A local Cohesity physical hardware node must be colocated inside the public Azure data center to terminate ExpressRoute connections.
- D. An Azure Active Directory (Microsoft Entra ID) App Registration must be created with an assigned role that grants necessary compute and storage permissions.

Answer: B,D

Explanation: To register Microsoft Azure as a cloud source in Cohesity DataProtect, authentication and authorization must be established via Azure APIs. This requires creating an App Registration within Azure Active Directory (Microsoft Entra ID) and assigning it a custom or built-in role (such as Contributor or a tailored role) that

allows managing virtual machine disks and snapshots. During registration in the Cohesity interface, the administrator enters the corresponding Application (Client) ID, Tenant ID, and a Client Secret or certificate. Physical colocation of Cohesity hardware is not required, and the Cohesity agent is not injected into the native Azure fabric management layer.

Question: 1197

Which of the following best describes the sequence of operations in Cohesity VM protection workflow?

- A. Quiesce VM, create snapshot, transfer data, commit snapshot
- B. Create snapshot, quiesce VM, transfer data, commit snapshot
- C. Commit snapshot, quiesce VM, create snapshot, transfer data
- D. Transfer data, create snapshot, quiesce VM, commit snapshot

Answer: A

Explanation: The correct sequence is to quiesce VM I/O to ensure consistency, create the snapshot, transfer the snapshot data to Cohesity, and finally commit (delete) the snapshot on the hypervisor.

Question: 1198

A storage administrator wants to perform a file-level recovery from a virtual machine backup snapshot. The VM runs a Linux distribution utilizing an XFS file system inside an LVM (Logical Volume Manager) structure. The administrator opens the Cohesity DataProtect dashboard to locate and restore three specific configuration files. Which statements accurately describe Cohesity's native

capabilities regarding this scenario? (Select two)

- A. File-level recovery for Linux VMs always requires a separate external helper appliance to be deployed manually in vCenter for every individual restore task.
- B. Cohesity cannot parse Linux file systems from snapshots, requiring the administrator to restore the entire VMDK to an auxiliary VM to access the files.
- C. Cohesity natively understands and parses LVM structures and XFS file systems directly from the backup snapshot metadata, enabling granular file search and selection in the UI.
- D. Files can be restored either by downloading them directly through the web browser via the Cohesity UI or by pushing them back to the original target VM via the Cohesity Agent.

Answer: C,D

Explanation: Cohesity DataProtect possesses native indexing capabilities that can parse complex volume and file structures, including Linux LVM and XFS file systems, directly from backup snapshots without needing full restorations or manual helper appliance attachments. Once the files are located via the indexed search in the Cohesity UI, the administrator can download them via the browser or restore them directly to the target system using the Cohesity Agent.

Question: 1199

An organization wants to implement protection for its containerized and database environments. Which of the following workloads can be grouped and protected natively via Cohesity DataProtect? (Select three)

- A. SAP HANA running exclusively on specialized mainframe architectures
- B. Oracle Databases with RMAN integration capabilities
- C. Kubernetes persistent volumes and cluster configurations

D. Microsoft SQL Server databases running on physical or virtual hosts

Answer: B,C,D

Explanation: Cohesity DataProtect features wide support for enterprise data workloads. This includes Kubernetes persistent volumes and cluster configurations, Microsoft SQL Server databases running on physical or virtual hosts, and Oracle Databases with RMAN integration capabilities. It does not natively support SAP HANA running exclusively on specialized mainframe architectures; native SAP HANA support is targeted at specific supported Linux distributions on x86_64 systems or certified cloud infrastructure.

Question: 1200

When configuring protection groups in Cohesity DataProtect, an operator notices that a specific protected asset is labeled as a "Child Object." If the parent asset is an entire Microsoft SQL Server instance, which of the following represents a valid child object within this hierarchy?

- A. The virtual machine network interface card configuration file
- B. The physical operating system boot volume of the database host
- C. The storage domain pool holding the transaction log backups
- D. A single availability group database within that SQL instance

Answer: D

Explanation: In the Cohesity source-and-object hierarchy, a parent source or object can contain granular child objects. For a Microsoft SQL Server source, the instance is the parent object, and the individual databases hosted within that instance are the child objects, allowing administrators to protect them individually or collectively.

Question: 1201

An enterprise administrator needs to configure backup windows within Cohesity DataProtect to manage cluster resource consumption and ensure critical business workflows are not disrupted during peak operational hours. Which of the following statements accurately describe the behavior and enforcement of backup windows in Cohesity? (Select two)

- A. Backup windows only restrict the initiation of new protection runs but allow already active runs to continue until completion.
- B. Blackout windows completely prohibit both scheduled protection runs and manual user-triggered on-demand protection runs.
- C. Cohesity allows administrators to configure distinct backup windows for full backups and incremental backups within the same policy.
- D. Any active protection run that exceeds the defined backup window is automatically paused and resumes during the next window.

Answer: A,C

Explanation: Cohesity DataProtect backup windows provide granular control over when data protection activities can execute. Backup windows define the specific timeframes during which scheduled protection runs are permitted to start; if a run is already active when the backup window closes, Cohesity allows it to continue to completion rather than abruptly terminating or pausing it. Additionally, Cohesity DataProtect policies support the configuration of independent backup windows for full backups and incremental backups within a single policy metadata structure, enabling optimization of network and storage utilization based on expected data load. On-demand backups ignore configured backup windows, and runs are not paused to be resumed later.

Question: 1202

Your SLA requires a recovery time objective (RTO) of under 10 minutes. Which Cohesity protection feature directly impacts reducing RTO in backup configurations?

- A. Deduplication on the backup repository
- B. Increasing snapshot frequency to every 5 minutes
- C. Continuous data protection replication
- D. Instant mass restore using mountable backups for data availability

Answer: D

Explanation: Instant mass restore enables near-instant availability of data without lengthy full data restores, directly reducing RTO. Snapshot frequency affects RPO but does not necessarily reduce recovery time. Replication ensures data redundancy but not speed of recovery. Deduplication optimizes storage.

Question: 1203

A hospitality chain's Cohesity Data Cloud enforces SLAs for reservation system backups at 88% within 14-hour cycles, with reporting needed to correlate seasonal guest surges. Which tools facilitate surge-adjusted compliance verification? (Select Multiple Answers)

- A. Guest data privacy breach incidents
- B. Room occupancy forecasts

- C. Seasonal cycle compliance trendlines
- D. Surge-volume SLA adjustment dashboards

Answer: C,D

Explanation: Seasonal surges in hospitality challenge reservation SLAs, with surge-volume SLA adjustment dashboards in Cohesity Data Cloud dynamically recalibrating 88% metrics against traffic, ensuring accurate verification. Seasonal cycle compliance trendlines project and confirm adherence, supporting capacity planning for uninterrupted booking data across properties.

Question: 1204

A company is using Cohesity to manage its data lifecycle. Which of the following best describes the role of Cohesity's archival capabilities?

- A. To manage active data for immediate access
- B. To create real-time backups of data
- C. To store data that is no longer actively used but must be retained
- D. To replicate data across multiple sites

Answer: C

Explanation: Cohesity's archival capabilities are designed to store data that is infrequently accessed but still needs to be retained for compliance or historical reasons. The other options describe different functionalities that do not align with the purpose of archival.

Question: 1205

A Cohesity cluster admin identifies a need for rapid search across protected objects and file metadata. Which platform characteristic provides automated global indexing for this capability?

- A. Built-in global indexing engine across the Data Cloud for files, objects, and protected data
- B. External search appliance requirement
- C. Indexing limited to backup metadata only
- D. Manual indexing scripts per source

Answer: A

Explanation: The Cohesity platform includes automated global indexing of files and objects, enabling fast search, analytics, and granular recovery without additional tools.

Question: 1206

An administrator is conducting a recovery operation for a critical Oracle database. Due to a storage area network failure at the primary site, the database must be recovered onto a completely different server at a secondary data center. What requirements must be satisfied for Cohesity DataProtect to complete this multi-site recovery? (Select two)

- A. The target database instance must have identical or compatible Oracle database software versions and matching user privileges.
- B. The target Oracle server must have the Cohesity Agent installed and be registered as a source with the Cohesity cluster performing the restore.
- C. The Cohesity cluster must have a dedicated fiber channel connection routed

directly into the fabric switches of the secondary data center.

D. The source database must be maintained in an active, un-archived online state during the entire data transmission process.

Answer: A,B

Explanation: To recover an Oracle database onto an alternate server via Cohesity, the target server must have the Cohesity Agent installed and be registered as an environment source within the managing Cohesity cluster. Additionally, the target server must run an identical or compatible version of the Oracle database software, ensuring that configuration files and database structures reconcile properly.

Question: 1207

You are recovering an application on a virtualized environment and want to ensure the recovery does not consume excessive resources affecting other workloads. Which Cohesity feature specifically helps to control resource usage during recovery?

- A. Throttling Instant Mass Restore via cgroups and QoS settings
- B. Disabling deduplication for faster restore
- C. Running full volume backup before recovery
- D. Exporting backup to external tape for offline recovery

Answer: A

Explanation: Controlling resource consumption during recovery is achieved through throttling Instant Mass Restore using cgroups and quality of service (QoS) controls, ensuring other workloads are not negatively impacted.

Question: 1208

A media company generates large volumes of unstructured video and image files that need secure, scalable access via multiple protocols for both internal users and external applications. Which Cohesity SmartFiles use case is most appropriate?

- A. Configuring SmartFiles as a primary database storage solution replacing SAN arrays
- B. Using SmartFiles exclusively as a backup target for virtual machines with no direct file access
- C. Limiting SmartFiles to immutable archival of database transaction logs only
- D. Deploying SmartFiles as a unified multiprotocol (NFS, SMB, S3) file

Answer: D

Explanation: SmartFiles is designed for unified management of file and object workloads on the Cohesity Data Cloud. It supports native NFS, SMB, and S3 access, global deduplication/compression, immutable snapshots, and integrated apps for insights, making it ideal for consolidating unstructured data such as media repositories while providing security and scalability.

Question: 1209

You are investigating a Protection Group that has been consistently showing a "Pending" status for its backup tasks. What does this typically indicate?

- A. The task has completed successfully
- B. The backup task is currently running
- C. The backup task has been scheduled but not yet started

D. There is a critical error preventing the task from starting

Answer: C

Explanation: A "Pending" status means that the backup task has been scheduled and is awaiting execution. This status indicates that the task has not yet started, often due to resource availability or scheduling conflicts.

Question: 1210

To validate the health of data protection tasks at scale, you want to include metrics from Cohesity's "Job Success Rate" and "Average Recovery Point Objective" in your report. Which API endpoint would you use for automated data retrieval?

- A. /monitoring/v1/cluster/healthMetrics
- B. /jobs/v1/taskDetails
- C. /config/v1/slaPolicies
- D. /reporting/v1/backup/jobStatistics

Answer: D

Explanation: The endpoint /reporting/v1/backup/jobStatistics provides detailed job success, duration, and RPO statistics necessary for health reports. Cluster health metrics and SLA policy endpoints provide different types of information.

Question: 1211

An operator wants to perform a recovery validation test for a group of web applications protected by Cohesity. The test must ensure that the applications boot correctly, pass health checks, and can communicate with a database clone, all without creating IP conflicts on the production network. Which Cohesity features natively support this workflow? (Select two)

- A. Cohesity Site Continuity or orchestration playbooks configured for sandbox testing
- B. Automated recovery scripts combined with network isolation settings in the recovery wizard
- C. Total cluster isolation by disconnecting the Cohesity data network uplinks during the test
- D. Manual exporting of VMDKs to a separate standalone ESXi host with local vSwitches

Answer: A,B

Explanation: Cohesity natively supports non-disruptive validation testing through orchestration features like Site Continuity or built-in recovery playbooks that isolate workloads into a sandbox network. This allows administrators to combine automated validation scripts with isolated network configurations directly within the wizard. Disconnecting cluster uplinks or manually exporting VMDKs are disruptive, inefficient, and manual processes that bypass Cohesity's native automated workflows.

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllabus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.