Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

COH-500 Exam Questions
COH-500 Practice Test
COH-500 Test Prep
COH-500 Questions & Answers
COH-500 Study Guide

PASS

killexams.com

Cohestity

COH-500

Cohesity Certified Architect Expert (CCAE)

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/COH-500

Question: 1023

A customer runs multiple retention policies on a single Cohesity cluster for different data types. Which scenario might cause issues that require architectural changes?

A. Retention of multiple years for archived compliance data alongside daily incremental backups
B. High snapshot frequency causing metadata database bloat
C. Simultaneous replication and archival jobs competing for node resources
D. Using the same node types across retention policies regardless of workload characteristics

Answer: B,C,D

Explanation: High snapshot frequency increases metadata size and can degrade performance. Concurrent replication and archival jobs strain cluster resources. Uniform node types may fail to optimize workload-specific performance needs. Long retention typically requires policy tuning but is supported.

Question: 1024

A ransomware attack compromises a 5TB file share. Which Cohesity features ensure rapid recovery?

A. Instant Mass Restore with fully hydrated snapshots
B. CyberScan to verify snapshot integrity
C. Manual restoration using file-level recovery
D. Helios anomaly detection for attack identification

Answer: A,B,D

Explanation: Instant Mass Restore enables rapid recovery of large datasets, CyberScan verifies snapshot integrity to avoid reinfection, and Helios anomaly detection identifies the attack timeline. Manual file-level recovery is too slow for a 5TB dataset.

Question: 1025

An administrator observes snapshot jobs failing in a multi-tenant cluster. Which troubleshooting steps are appropriate considering organization segregation?

A. Verify snapshot job ownership within the correct organization context

B. Check organization-specific quota limits affecting snapshot creation
C. Restart entire cluster nodes irrespective of tenant context
D. Review replication schedules globally without organization filters

Answer: A,B

Explanation: Snapshots belong to organizations; quota limits can prevent snapshots. Restarting whole cluster or ignoring organization context is inefficient.

Question: 1026

Your organization is deploying Cohesity Data Cloud in an AWS environment with EC2 instances and S3 buckets. You need to protect EC2 instances with automated snapshot-based backups and archive data to S3. Which AWS services and Cohesity settings must be configured?

A. Assign an IAM role with EC2 and S3 permissions to the Cohesity cluster
B. Configure Cohesity to use AWS KMS for encryption of archived data in S3
C. Enable AWS Snapshot Manager in Cohesity for EC2 instance backups
D. Set up an AWS Lambda function to trigger Cohesity backup jobs

Answer: A,B

Explanation: To protect EC2 instances and archive to S3, Cohesity requires an IAM role with permissions for EC2 (to manage snapshots) and S3 (for archiving), making A correct. Configuring AWS KMS in Cohesity ensures encrypted data archival to S3, making B correct. AWS Snapshot Manager is not a Cohesity feature; Cohesity directly manages EC2 snapshots. AWS Lambda is not required, as Cohesity's internal scheduling handles backup jobs.

Question: 1027

When sizing for a NAS-heavy environment storing 500 TB of active data with high change rates (~10% daily change), and assuming Cohesity compression of 2:1 and snapshot retention of 14 days, what is the optimal snapshot storage estimate for designing the platform?

A. 400 TB
B. 500 TB
C. 700 TB
D. 1000 TB

Answer: C

Explanation: Daily changed data is 10% of 500 TB = 50 TB. For 14 days, changed data totals 700 TB raw. With 2:1 compression, this is 350 TB. Including metadata and snapshot overhead, estimate around 700 TB is required to provision snapshots capacity safely.

Question: 1028

A Cohesity cluster reports a 500% spike in file modifications for an Oracle database backup. Which steps should you take to investigate?

A. Check the Security Center for IOC alerts
B. Run cohesity_threat --scan --workload oracle
C. Use cohesity_anomaly --details to analyze file change patterns
D. Update the backup policy to increase retention

Answer: A,B,C

Explanation: Checking the Security Center for IOC alerts identifies potential threats. Running cohesity_threat --scan --workload oracle scans the Oracle backup for malware. Using cohesity_anomaly --details analyzes file change patterns to confirm the anomaly. Updating the backup policy is unrelated to investigation.

Question: 1029

A Cohesity on-premises cluster uses a 6:2 erasure coding scheme. To tolerate 3 node failures in a 9-node setup, which configuration is needed?

A. Change to 6:3 erasure coding with RF=2
B. Change to 7:2 erasure coding with RF=3
C. Change to 7:3 erasure coding with RF=2
D. Change to 8:2 erasure coding with RF=3

Answer: C

Explanation: The 7:3 erasure coding scheme with RF=2 in a 9-node cluster tolerates 3 node failures. It splits data into 4 data fragments and 3 parity fragments, enabling recovery from 3 failures. RF=2 ensures sufficient redundancy while optimizing storage efficiency.

Question: 1030

In the Cohesity sizing tool, to estimate cluster growth over five years with compound data growth and retention impacts, which modeling approach is most accurate?

A. Input linear growth rate annually with fixed retention period
B. Model year-over-year growth using compound growth formula in the retention input
C. Ignore growth for sizing; adjust cluster size later manually
D. Use default retention and growth without adjustment

Answer: B

Explanation: Compound growth calculation accounts for the accumulation of data year-over-year combined with retention impacts, providing accurate long-term sizing projections.

Question: 1031

Which command configures Cohesity Data Cloud to use Azure AD for authentication?

A. iris_cli auth add --type=azuread
B. cohesity ad integrate --azure
C. iris_cli cluster auth --azuread
D. cohesity auth setup --ad=azure

Answer: A

Explanation: The iris_cli auth add --type=azuread command integrates Azure AD for authentication in Cohesity Data Cloud. Other options are syntactically incorrect.

Question: 1032

Which SAML attribute must be configured in Azure AD to assign a Cohesity “Admin” role to a user group?

A. http://schemas.microsoft.com/identity/claims/displayname
B. http://schemas.xmlsoap.org/claims/Group
C. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
D. http://schemas.microsoft.com/identity/claims/objectidentifier

Answer: B

Explanation: The http://schemas.xmlsoap.org/claims/Group attribute in the SAML

assertion maps Azure AD groups to Cohesity roles, such as “Admin,” for proper RBAC assignment. Other attributes do not convey group or role information.

Question: 1033

During pre-install checks using Siren, you receive a validation failure stating “IP address validation failed on node.” Which potential configuration errors could cause this?

A. Duplicate IP addresses configured on cluster nodes
B. DHCP scope exhaustion causing IP conflicts during deployment
C. Incorrect subnet mask mismatch across cluster nodes
D. IP address reserved in firewall causing packet drops

Answer: A,B,C

Explanation: Duplicate IPs and DHCP scope exhaustion cause IP conflicts. Subnet mask mismatches cause network communication failures. Firewall reservation does not cause an IP validation failure at install.

Question: 1034

Scenario: A Cohesity DataProtect job for a 2 TB NAS filer fails due to snapshot inconsistency. Which setting ensures snapshot-consistent backups for NetApp NAS?

A. Enable quiescing of the NAS filer
B. Set snapshot consistency to crash-consistent
C. Use Cohesity's native snapshot integration
D. Disable deduplication for the NAS job

Answer: C

Explanation: Cohesity's native snapshot integration for NetApp NAS ensures snapshot-consistent backups without quiescing the filer, allowing continuous writes while protecting data. Quiescing disrupts operations, crash-consistent snapshots are less reliable, and disabling deduplication is unrelated to consistency.

Question: 1035

You are developing a custom workflow to automate Cohesity backup job scheduling using the REST API. The workflow must schedule a job to run every 6 hours with a 7-day retention. Which JSON payload is correct?

A. json
{"name":"HourlyBackup","schedules":[{"frequency":6,"unit":"Hours","startTime":"00:00:00","rete
B. json
{"name":"HourlyBackup","frequency":"6Hours","retentionDays":7}
C. json {"policy":"HourlyBackup","schedule":"6Hours","retention":7}
D. json
{"name":"HourlyBackup","dailySchedule":{"frequency":6,"retention":7}}

Answer: A

Explanation: The correct JSON payload specifies the schedule with a 6-hour frequency, start time, and 7-day retention in the correct format for the /v2/data-protect/policies endpoint. Other payloads use incorrect keys or structures.

Question: 1036

A Cohesity cluster with 8 nodes supports 1 PB with a target of 100,000 IOPS. Runtime metrics show 80,000 IOPS. The workload is 50% write-heavy. What is the most effective solution?

A. Add 2 nodes to the cluster
B. Disable deduplication for write-heavy workloads
C. Reconfigure to RAID 1
D. Upgrade to NVMe SSDs

Answer: A

Explanation: Adding 2 nodes increases IOPS capacity to meet the 100,000 target by distributing the workload. Disabling deduplication sacrifices efficiency without guaranteed IOPS gains. RAID 1 may help but isn't indicated as misconfigured. NVMe SSDs improve performance but are less cost-effective than adding nodes.

Question: 1037

Which parameters must be adjusted on a Cohesity cluster to support extremely high retention immutable backups without impacting production performance?

A. Increase metadata cache allocation per node
B. Enable deduplication inline for all backup jobs
C. Configure background snapshot pruning during low utilization windows
D. Disable encryption to reduce CPU load

Answer: A,C

Explanation: Metadata cache improves snapshot metadata access, pruning during low utilization reduces performance impact. Deduplication reduces storage but increases CPU. Disabling encryption is not recommended for security.

Question: 1038

A Cohesity engineer needs to script automated data recovery tasks across several clusters via Helios API. Which authentication method provides the most secure programmatic access?

A. Basic authentication using cluster admin credentials
B. OAuth 2.0 token-based authentication with refresh tokens
C. Static API keys with unrestricted access permissions
D. Anonymous read-only API access for monitoring

Answer: B

Explanation: OAuth 2.0 with token refresh is the most secure for programmatic operations, avoiding exposure of static credentials; basic auth and static keys are less secure; anonymous read-only access won't allow data recovery tasks.

Question: 1039

A Cohesity administrator wants to configure a multi-tenant FortKnox deployment. Which of the following settings are mandatory to support isolated tenant access?

A. Tenant-specific encryption keys with no cross-tenant sharing
B. Dedicated FortKnox vault per tenant with unique access policies
C. Unified tenant access auditing enabled on the central portal
D. Shared bucket configuration for cost-effective storage allocation

Answer: A,B,C

Explanation: Multi-tenant FortKnox requires tenant-specific encryption keys, dedicated vaults per tenant, and centralized audit logging. Shared buckets negate tenant isolation.

Question: 1040

A Cohesity cluster is configured with a retention policy for a 5 TB Oracle database, requiring daily incremental backups for 30 days and full backups retained for 6 months.

Which command sets this policy?

A. cohesity policy create --name oracle_policy --daily 30 --monthly 6 --full-backup
B. cohesity policy create --name oracle_policy --daily-retention 30d --monthly-retention 6m --incremental
C. cohesity policy create --name oracle_policy --daily 30d --monthly 6m --full
D. cohesity policy create --name oracle_policy --daily-retention 30 --monthly-retention 6 --incremental-backup

Answer: B

Explanation: The command cohesity policy create --name oracle_policy --daily-retention 30d --monthly-retention 6m --incremental configures daily incremental backups retained for 30 days and monthly full backups for 6 months. The --incremental flag ensures daily backups capture only changed data, while --monthly-retention 6m retains full backups for 6 months, aligning with the requirements.

Question: 1041

A Cohesity architect must validate the integrity of backups stored in immutable vaults after a security incident. Which methods are recommended?

A. Perform built-in checksum verification on vault snapshots
B. Use forensic tooling external to Cohesity for integrity check
C. Run automated backup verification jobs daily
D. Manually mount immutable snapshots and verify critical files

Answer: A,C

Explanation: Built-in checksum and automated verification jobs help quickly validate data integrity. External tooling and manual mounts are valid but time-consuming and less scalable.

Question: 1042

In a scenario where a cluster has multiple ransomware anomalies detected by Helios, what are the recommended immediate response actions?

A. Trigger legal hold on recent backup sets to preserve data
B. Initiate cluster-wide rollback to last known good snapshot
C. Disable snapshot creation temporarily to prevent corrupted data
D. Notify security team and quarantine affected cluster via Helios

Answer: A,D

Explanation: Legal hold prevents deleting potentially compromised backups, and notifying security for quarantine or investigation is critical. Rolling back or disabling snapshots without full understanding can cause data loss or missed detection.

Question: 1043

A Cohesity cluster is configured with DataLock for a VMware backup job. Which security features are automatically enforced when DataLock is enabled to protect against ransomware tampering?

A. AWS Object Lock integration for cloud snapshots
B. Granular Role-Based Access Control (RBAC)
C. Immutable snapshot filesystem
D. Multi-Factor Authentication (MFA)

Answer: B,C

Explanation: DataLock, Cohesity's WORM feature, enforces immutability through an immutable snapshot filesystem, preventing modification or deletion of backups. It integrates with granular RBAC to restrict unauthorized access. MFA and AWS Object Lock are separate security features not automatically enabled by DataLock.

Question: 1044

To create a custom RBAC role in Cohesity allowing users to generate reports but not modify backup jobs, which permissions are essential to include?

A. Read and execute permissions on report modules only
B. Write permission on backup job configurations
C. Admin privilege on export storage targets
D. Delete permission on backup job history

Answer: A

Explanation: Report generation requires read and execute access to reporting modules only. Backup configurations, admin rights, or delete permissions are unnecessary and risk privilege escalation.

Question: 1045

Which steps ensure Cohesity Data Cloud compliance with GDPR for data stored in AWS?

A. Enable encryption-at-rest with AWS KMS
B. Configure data retention policies in Cohesity Helios
C. Set up SpanFS audit logging for access tracking
D. Use public S3 buckets for data storage

Answer: A,B,C

Explanation: Encryption-at-rest with AWS KMS, retention policies in Helios, and SpanFS audit logging ensure GDPR compliance by securing data, enforcing retention, and tracking access. Public S3 buckets violate GDPR's data protection requirements.

KILLEXAMS.COM

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

***Actual Exam Questions**: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

***Exam Dumps**: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

***Practice Tests**: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

***Guaranteed Success**: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

***Updated Content:** Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

***Technical Support**: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*