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

KILL EXAMS

CCPA COH100 Exam Questions
CCPA COH100 Practice Test
CCPA COH100 MCQs
CCPA COH100 Test Prep
CCPA COH100 PDF Questions

PASS

killexams.com

COHESITY

COH-100

Cohesity Certified Protection Associate - DataProtect (COH100)

ORDER FULL VERSION

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

Question: 503

A financial institution with strict regulatory requirements has deployed Cohesity DataProtect across multiple clusters, and during a quarterly audit, auditors flag inconsistent backup windows for Oracle databases. Which metrics displayed on the Cohesity performance dashboard are essential for the data protection team to review in order to validate that protection jobs are completing within defined SLAs and to prepare evidence for the audit? (Select Multiple Answers)

A. Cluster health score and posture advisor metrics
B. Data reduction ratios for each protection policy
C. Job duration versus SLA thresholds for database backups
D. Throughput rates for replication to remote sites

Answer: A, C

Explanation: For regulatory audits in a financial context, the cluster health score and posture advisor metrics on the dashboard offer a holistic view of system reliability and security posture, crucial for demonstrating overall compliance with data availability standards by highlighting any degraded states that could affect Oracle backup integrity. Additionally, job duration versus SLA thresholds specifically tracks how long database protection jobs take against predefined limits, allowing the team to correlate completion times with audit windows and implement policy tweaks, such as increasing parallelism, to ensure consistent performance and provide timestamped evidence of SLA adherence across multi-cluster deployments.

Question: 504

A backup admin needs to verify if incremental backup jobs for a large VM consistently completed within the SLA of 90 minutes last week. In Cohesity Data Cloud, which KPI metric should be monitored in the "Backup SLA Compliance" report for this?

A. Job Backlog
B. Changed Block Ratio
C. Job Duration
D. Job Throughput

Answer: C

Explanation: Job Duration is the key performance indicator to verify if jobs complete within the SLA time frame (90 minutes). Changed Block Ratio and Throughput relate to data change and transfer speed but do not confirm SLA adherence. Job Backlog indicates pending jobs, not completion times.

Question: 505

During a compliance review, a pharmaceutical firm analyzes Cohesity DataProtect policies for drug trial

data. In this regulated scenario involving global teams, which policy concepts ensure consistent application across distributed protection groups? (Select Multiple Answers)

A. Global deduplication scopes spanning multiple clusters
B. Log backup frequencies tied to transactional SLAs
C. Policy inheritance hierarchies for subgroup overrides
D. Snapshot consolidation intervals for storage optimization

Answer: B, D

Explanation: Log backup frequencies in policies are configured to align with transactional SLAs, capturing database changes at intervals like every 15 minutes to support trial data integrity across time zones. Snapshot consolidation intervals automatically merge deltas into base snapshots, optimizing storage in distributed setups without manual intervention. Global deduplication is a platform-wide feature, not a policy concept. Policy inheritance hierarchies do not exist in Cohesity; policies are directly assigned without cascading overrides.

Question: 506

Which Cohesity DataProtect protection policy component specifies on which schedule snapshots are created?

A. Retention duration
B. Replication target
C. Snapshot frequency
D. Agent installation profile

Answer: C

Explanation: Snapshot frequency defines how often snapshots are taken. Replication target defines where backup copies go, retention duration defines how long backups are kept, and agent installation profile relates to software install not snapshot scheduling.

Question: 507

During a scheduled backup operation, you notice some Protection Groups have the task state "Partially Failed." What does this status specifically indicate about the Protection Group's backup?
A. One or more individual objects or components within the Protection Group encountered failures, but some succeeded
B. The Protection Group backup was completely successful without any issues
C. The Protection Group backup task was canceled before completion
D. The Protection Group backup is currently running but stalled and incomplete

Answer: A

Explanation: The "Partially Failed" task state means that within the Protection Group, some components or objects failed during the backup process, while others completed successfully. This indicates partial success but highlights issues requiring investigation and remediation. It is not a complete success (which would be "Success"), nor an indication of cancellation or stalling.

Question: 508

In an automotive R&D facility using Red Hat OpenShift sources for simulation objects and Huawei Cloud OBS for CAD collaboration objects, a supply chain cyber incident has invalidated partial source certificates; which two source and object concepts in Cohesity DataProtect restore trust through certificate-agnostic protection and object-level auditing for R&D continuity? (Select Two)

A. Revoking and re-registering sources with quorum authentication for OpenShift simulations and Huawei OBS CAD objects, using data pools for audited object isolation during certificate invalidation
B. Applying global search with ML-powered certificate validation to audit simulation objects, enabling instant recovery of collaborative CAD data across incident-affected sources
C. Configuring protection policies with sliding-window deduplication for Huawei OBS objects to support RBAC-enforced auditing, integrated with automated source reconciliation
D. Utilizing federated source management via API extensibility to enforce WORM immutability on R&D objects, facilitating MFA-based trust restoration post-incident

Answer: A, D

Explanation: Cohesity DataProtect facilitates source revocation and re-registration with quorum authentication, ensuring secure reconnection of Red Hat OpenShift and Huawei Cloud OBS amid certificate invalidations from cyber incidents, while data pools provide audited isolation for simulation and CAD objects to maintain R&D continuity without data loss or exposure. This process rebuilds trust through multi-approver validation. Furthermore, federated source management leverages API extensibility to impose write-once-read-many (WORM) immutability across R&D objects, enabling multi-factor authentication (MFA)-driven trust restoration and comprehensive auditing trails; these concepts ensure resilient protection in automotive innovation pipelines, core to Cohesity's cyber-resilient architecture.

Question: 509

A media company with global content repositories on Cohesity DataProtect faces challenges in providing low-latency access to archived video files for post-production teams while complying with GDPR data residency rules. Which native Cohesity file services capabilities support geo-distributed, compliant access with intelligent caching? (Select Multiple Answers)

A. Intelligent tiering with edge caching for regional file views

B. S3-compatible object locking for immutable content archives
C. Kerberos authentication for secure multi-site SMB access
D. AI-driven data classification for automated residency enforcement

Answer: A, C

Explanation: Intelligent tiering with edge caching for regional file views enables low-latency access to archived videos by prefetching frequently used content to edge locations compliant with GDPR, automatically adjusting based on access patterns to balance performance and cost across global teams. Kerberos authentication for secure multi-site SMB access integrates with Active Directory for encrypted, ticket-based verification, ensuring post-production teams in different regions can mount shares securely without exposing credentials, thus upholding data residency by restricting cross-border transfers unless explicitly authorized.

Question: 510

An administrator needs to confirm that all backup jobs are running within their assigned SLA targets using Cohesity's reporting tool. The report must also show trends over the past 6 months. Which report best fits this requirement?
A. Backup Verification Status report with job integrity checks
B. SLA Compliance Trend report with Job Completion Time over 6 months
C. Data Protection Job History showing failure counts per week
D. Resource Utilization report listing CPU and Memory consumption trends

Answer: B

Explanation: The SLA Compliance Trend report tracks job completion times relative to SLAs and displays trends over time, ideal for verifying adherence over 6 months. Other reports either focus on integrity, failures, or resources rather than SLA compliance trends.

Question: 511

A gaming studio's Cohesity DataProtect dev/test pipeline recovers SQL databases to ephemeral Azure instances for load testing. Which workflows ensure data freshness without chain breaks? (Select Multiple Answers)

A. Enable incremental forever with log replays for PITR in tests
B. Integrate with Azure AD for seamless, masked data provisioning
C. Use RecoveryAgent blueprints for automated testbed orchestrations
D. Apply global dedup for zero-cost multi-spin copies in dev

Answer: C, D

Explanation: RecoveryAgent blueprints in Cohesity DataProtect automate dev/test orchestrations, including SQL PITR to Azure for load simulations without manual chain management. Global deduplication enables zero-cost spins of large databases, accelerating gaming asset tests with fresh, space-efficient copies.

Question: 512

Which Cohesity method is best for recovering a large number of small files quickly without negatively impacting production environment performance?

A. Use the Instant Mass Restore feature with selective file-level recovery
B. Perform full volume mounts for manual copying
C. Execute bare metal restore during maintenance window
D. Export backups to cloud archive for retrieval

Answer: A

Explanation: Instant Mass Restore enables parallelized file recovery, speeding up restore of large datasets with many files while minimizing production impact, unlike full volume restores or archive exports.

Question: 513

A defense contractor's Cohesity DataProtect recovery for physical servers post-DDoS involves alternate host mounts. The process must include error-continued volume browsing. Which steps facilitate secure path alternates? (Select Multiple Answers)

A. Disable Recover to Original Path and specify alternate Recover To field
B. Browse snapshot content and select volumes/files for Next progression
C. Enable Continue on Error in options for resilient multi-volume tasks
D. Monitor progress in Activity with Download Files post-completion

Answer: A, C

Explanation: Disabling Recover to Original Path and specifying an alternate in Cohesity DataProtect directs physical server recoveries to secure hosts, isolating DDoS-affected systems. Enabling Continue on Error ensures volume-level failures don't halt the task, allowing partial restores in defense-critical multi-host environments.

Question: 514

An administrator is looking at a graphical Cohesity performance dashboard showing backup job durations and notices a steady upward trend over the past 3 weeks. Which action is the best approach to

investigate this?
A. Drill down on job logs and check for increased Changed Block Ratio or resource contention
B. Increase snapshot retention to offload older backups
C. Add additional nodes to the cluster immediately
D. Reset all backup jobs to run sequentially instead of concurrent

Answer: A

Explanation: Investigating job logs for changed data amounts or resource contention helps identify why durations are increasing. Other options are premature without understanding root causes.

Question: 515

A creative agency collaborating on campaigns uses Cohesity SmartFiles SMB views for asset editing and object services for client deliverables, facing version conflicts in remote edits; which two SmartFiles use cases resolve conflicts via snapshot versioning and collaborative locking? (Select Two)

A. Leveraging SmartFiles for content management with unlimited versioning snapshots for SMB assets, enabling collaborative locking on object deliverables to prevent conflicts
B. Utilizing SmartFiles as a corporate audio/video repository with ML-based conflict resolution for edits, supporting global access for remote teams
C. Implementing SmartFiles as a backup target with WORM for client files, integrated with quota enforcement for asset shares
D. Configuring SmartFiles for secure digital storage to apply RBAC on SMB views, facilitating MFA for deliverable objects

Answer: A, B

Explanation: In Cohesity SmartFiles, the content management use case offers unlimited, performance-neutral versioning snapshots for SMB editing assets, paired with fine-grained locking on object-based client deliverables to eliminate remote edit conflicts, streamlining agency collaborations. This versioning preserves creative history. Additionally, the corporate audio/video repository use case integrates machine learning (ML)-based resolution to auto-merge or flag edit discrepancies, enhancing global team productivity; these use cases boost efficiency in dynamic creative settings.

Question: 516

In a scenario where VM backups must be offloaded to cloud storage after 7 days, which SLA or Protection Group feature handles this tiering?
A. Backup Window adjusted for cloud transfer
B. Retention policy with cloud archival tier enabled
C. Backup job concurrent limits
D. Recovery Time Objective scheduling

Answer: B

Explanation: Retention policies linked with cloud archival tier enable automated movement of backup data to lower-cost cloud storage after the specified period.

Question: 517

Following a data center migration to Cohesity DataProtect, an insurance company's dashboard indicates fluctuating throughput for NAS file shares, risking 8-hour SLA breaches for archival data. Which performance measurements should be analyzed to determine if the fluctuations are from metadata overhead or cross-vCenter traffic patterns? (Select Multiple Answers)

A. Metadata processing latency for file indexing
B. Throughput averages for vMotion-integrated jobs
C. Total encrypted data volume post-migration
D. Alert resolution times for minor warnings

Answer: A, B

Explanation: Migration-induced fluctuations in NAS backups stem from metadata processing latency for file indexing, which the dashboard tracks to identify overhead in large share catalogs, prompting indexing optimizations for SLA adherence. Throughput averages for vMotion-integrated jobs further expose cross-vCenter traffic inefficiencies, allowing VLAN adjustments or policy refinements to stabilize performance and ensure archival data availability for insurance claims processing.

Question: 518

During a storage domain configuration on Cohesity, which parameter optimizes the write performance for SSD-backed storage domains?

A. Set the block size to 1MB and disable read caching
B. Set the block size to 512KB and disable write caching
C. Set the block size to 4MB and enable write caching
D. Set the block size to 128KB and enable compression

Answer: C

Explanation: Larger block sizes like 4MB combined with write caching optimize throughput and write performance on SSD storage domains. Write caching aggressively speeds up writes that would otherwise be latency-bound on SSDs. Smaller block sizes and disabled caching reduce efficiency and throughput.

Question: 519

In a financial trading firm upgrading to quantum-resistant encryption amid rising quantum threats, the Cohesity platform manages sources from mainframe z/OS for transaction objects and Equinix Metal for edge trading objects; which two platform characteristics enhance quantum-resilient protection and automated failover for trading continuity? (Select Two)

A. Integrating post-quantum cryptography in the platform's multilayered security to encrypt z/OS and Equinix objects, with ML-based early threat detection for automated failover orchestration
B. Deploying the API-first design with partner ecosystem integrations to extend quantum-resistant policies to edge sources, supporting granular RBAC for transaction object isolation
C. Utilizing the unified management pane via Helios for global visibility into mainframe and edge objects, enabling immutable snapshot-based recovery with zero trust enforcement
D. Configuring enterprise-class performance scaling with sliding-window deduplication to handle high-velocity trading objects, integrated with MFA for quantum threat mitigation

Answer: A, C

Explanation: Cohesity's multilayered security architecture incorporates post-quantum cryptography options to safeguard transaction objects on mainframe z/OS and edge trading data on Equinix Metal against emerging quantum threats, while machine learning (ML)-based early threat detection automates failover processes to maintain trading continuity without manual intervention, aligning with the platform's cyber-resilience focus. This ensures forward-compatible protection in high-stakes financial environments. Additionally, the Helios unified management pane offers global visibility and control over disparate sources, enforcing zero trust principles through immutable snapshots that support rapid, verifiable recovery; these characteristics, as highlighted in Cohesity's 2025 GigaOm Radar leadership for unstructured data management, streamline operations in quantum-vulnerable upgrades.

Question: 520

During a compliance audit, a manufacturing firm discovers that Protection Group backups for Oracle VMs lack consistency due to active RMAN sessions conflicting with Cohesity snapshots. Which targeted configurations would enforce consistent protection? (Select Multiple Answers)

A. Integrate Oracle RMAN scripts into the Protection Group's pre-job phase to quiesce sessions and coordinate with Cohesity's SBT library for seamless backups.
B. Configure the group to use out-of-band incremental backups triggered post-log chain validation, ensuring no conflicts disrupt full consistency.
C. Enable multi-stream RMAN channels limited to 4 per database in the policy, balancing parallelism with snapshot stability to avoid partial captures.
D. Set up database-specific SLAs in the Protection Group to monitor and alert on RMAN conflicts, auto-pausing jobs for manual resolution.

Answer: A, B, C

Explanation: RMAN integration via pre-job scripts synchronizes quiescing, allowing Cohesity to capture clean states without interference. Out-of-band incrementals post-validation prevent chain disruptions, maintaining recovery consistency. Multi-stream limits control resource usage, avoiding overload that leads to incomplete snapshots; SLAs monitor but do not actively configure for prevention.

Question: 521

You are tasked with restoring a Linux VM's root filesystem from a recovery point without shutting down the VM or interrupting network services. Which replication or recovery feature should be leveraged?
A. Export backup to tape for delayed restore
B. Full system cold restore requiring shutdown
C. Manual file copy after VM shutdown
D. Instant Mass Restore with live streaming and block-level synchronization

Answer: D

Explanation: Instant Mass Restore supports streaming recovery and block-level synchronization to restore VM files live without downtime, essential for fast, non-disruptive recovery.

Question: 522

In a healthcare provider's Cohesity deployment, where HIPAA-compliant backups of patient databases must achieve sub-2-hour RPOs, the performance dashboard shows anomalous ingest rates following a recent cluster expansion. Which measurements should the administrator cross-reference to confirm if the anomalies are due to uneven load distribution across new nodes or misconfigured QoS policies? (Select Multiple Answers)

A. Data ingest velocity per protection group
B. Node-specific IOPS and latency variances
C. Overall cluster uptime percentage
D. Archival job queue depths

Answer: A, B

Explanation: Post-expansion anomalies in healthcare backups require examining data ingest velocity per protection group to quantify slowdowns in database captures, highlighting if load balancing is ineffective for RPO compliance. Node-specific IOPS and latency variances then reveal disparities among new nodes, guiding QoS reconfiguration or firmware alignment to equalize performance, ensuring HIPAA-mandated rapid recovery without data exposure risks.

Question: 523

A security audit mandates encrypted replication traffic. How does Cohesity enforce encryption on replication connections?

A. VLAN segmentation substitutes replication encryption requirement
B. Replication traffic is encrypted by default and requires no additional setting
C. TLS encryption must be enabled on replication protocol settings within the cluster
D. WAN acceleration features automatically perform encryption on traffic

Answer: C

Explanation: TLS encryption for replication is configurable within the cluster's replication settings to ensure traffic confidentiality. Encryption is not automatic in all cases and VLAN or WAN acceleration does not substitute for encryption.

Question: 524

A utility company archives grid sensor data in Cohesity DataProtect to hybrid tape-cloud for 20-year retention, but faces retrieval delays for incident investigations. Which concepts accelerate forensic archival access? (Select Multiple Answers)

A. Indexed archival stubs for metadata-fast retrieval
B. Parallel chunk rehydration from multi-targets
C. Event-driven warm-up triggers for incident data
D. Dedup-verified partial restores for sensor streams

Answer: B, C

Explanation: Parallel chunk rehydration from multi-targets pulls data concurrently from tape and cloud, slashing investigation times for grid incidents. Event-driven warm-up triggers automatically transition relevant sensor archives to hot tiers upon alert detection, enabling rapid forensic analysis.

Question: 525

Given that a protection policy is configured with application consistent backups and VSS freeze time setting of 30 seconds, what impact can you expect on production applications?
A. Continuous application performance degradation during job
B. Transient pause in I/O operations up to 30 seconds
C. Application crashes during the backup process
D. No impact; backups are non-intrusive

Answer: B

Explanation: VSS freeze temporarily pauses I/O to applications to create a consistent snapshot, which can last up to the freeze time setting, here 30 seconds. This transient pause is a known impact and must be considered for sensitive applications. Continuous degradation or crashes are not expected if VSS is functioning correctly. Backups are intrusive to a minor degree during quiescence.

Question: 526

A global e-commerce company uses Cohesity DataProtect to protect thousands of EC2 instances across AWS regions, with Protection Groups enforcing strict RPO of 4 hours. During a cyber incident simulation in Q3 2025, the team identifies anomalous task behaviors in the Helios dashboard. Which task state status types would Cohesity DataProtect report for Protection Group tasks affected by the simulated ransomware-induced bandwidth throttling? (Select Multiple Answers)

A. Completed
B. Expired
C. Success
D. Warning

Answer: A, D

Explanation: Cohesity DataProtect task states include Completed, which signifies a run that finished but may have encountered non-critical issues like partial data skips due to throttling, ensuring the majority of objects are captured. Warning appears when the run meets basic criteria but flags deviations, such as delayed increments from bandwidth limits impacting RPO adherence. Expired relates to snapshot lifecycle, not task execution, and Success implies no anomalies, which wouldn't apply in a throttled simulation.

Question: 527

A source system backup needs to be crash consistent but also must reduce backup window impact. Which Cohesity Agent setting will assist most?

A. Enable Continuous Data Protection (CDP) on the agent
B. Configure application consistent scripts with minimal timeout
C. Schedule backups during system off-hours only
D. Use snapshot-based crash consistent backup without scripts or application hooks

Answer: D

Explanation: Snapshot-based crash consistent backups minimize application impact by not performing quiescence; avoiding scripts reduces overhead. Application consistent with scripts increases impact, scheduling off-hours impacts timing not backup runtime, and CDP is not crash consistent backup.

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.*