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

KILL EXAMS

COH-125 MCQs
COH-125 TestPrep
COH-125 Study Guide
COH-125 Practice Test
COH-125 Exam Questions

PASS

killexams.com

COHESITY

COH-125

Cohesity Certified Implementation Professional - SmartFiles

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/COH-125

Question: 712

Which parameter in the external NAS tiering job dictates the maximum amount of data transferred concurrently to avoid network congestion?

A. MaxConcurrentThreads
B. SyncInterval
C. DataTransferTimeout
D. BandwidthThrottleLimit

Answer: D

Explanation: BandwidthThrottleLimit specifies the maximum network throughput the tiering job uses, preventing network congestion during data migration.

Question: 713

For a retail chain consolidating 2.2PB e-commerce logs from Dell EMC PowerScale NAS to Cohesity View in a multi-site Helios-managed setup (version 7.0), identify use cases for external NAS tiering that support GDPR data residency and analytics integration? (Select All that Apply)

A. Tiering PII logs to geo-fenced Views, enforcing residency with 'iris_cli tier geo-policy --view retail_logs --region eu-west-1 --filter "contains_pii=true age>365d"'

B. Enabling integrated Insight app on tiered logs for pattern mining, querying 'SELECT patterns FROM tiered_logs WHERE anomaly_score > 0.8 GROUP BY category'
C. Archiving tiered data to EU Azure with retention formula: retain = base_365d + (log_volume_GB * 0.01 years/GB), using 'iris_cli tier archive --dest azure-eu --retention-calc custom'
D. Supporting dev/test environments by cloning tiered Views, 'iris_cli view clone --source retail_logs --name test_logs --qos low --size-limit 500TB'

Answer: A, B, C

Explanation: External NAS tiering excels in GDPR compliance by tiering PII-containing logs to region-specific Views via 'iris_cli tier geo-policy --view retail_logs --region eu-west-1 --filter "contains_pii=true age>365d"', ensuring data stays within EU boundaries for 2.2PB multi-site consolidation. It integrates with Insight for advanced analytics on tiered data, running queries like 'SELECT patterns FROM tiered_logs WHERE anomaly_score > 0.8 GROUP BY category' to detect fraud patterns without rehydration overhead. Additionally, it automates archival to compliant storage like EU Azure, applying custom retention 'iris_cli tier archive --dest azure-eu --retention-calc custom' with formula retain = 365 days + (volume_GB * 0.01 years/GB) for proportional long-term holds, optimizing costs in Helios environments.

Question: 714

Which feature of Cohesity Marketplace applications enables incremental scanning and indexing of new or changed files on SmartFiles?

A. Scan only files larger than a specified size
B. Full re-index on every scan without checkpoints
C. Manual scan trigger required for all incremental scans
D. Checkpointing based on file change time metadata

Answer: D

Explanation: Checkpointing allows Marketplace apps to maintain state on scanned files based on metadata, enabling them to scan only changed or new files incrementally. Without this, scans would be full or manual, which is inefficient.

Question: 715

For a hospital EMR system, SmartFiles View "EMRView" limits SMB to clinical nets

10.1.50.0/23 via cohesity_cli view clinical-allowlist add EMRView --subnet 10.1.50.0/23. Granular HIPAA ACLs read-only for "Nurses" on "/PatientCharts". Auth bypass via old clients. Which features identify fixes? (Select All that Apply)

A. Enforce SMB2+ minimum version in global settings for secure auth
B. Configure Kerberos realm trusts for cross-domain nurse access
C. Use View-level quotas to limit chart exposure per user
D. Implement AI anomaly detection for auth failures

Answer: A, B

Explanation: Enforcing SMB2+ minimum prevents legacy bypasses, securing mounts to 10.1.50.0/23 with granular read-only for "Nurses". Configuring Kerberos realm trusts enables secure cross-domain auth for EMR access. Quotas control size not auth, and AI detects but not prevents protocol weaknesses.

Question: 716

When enabling audit logs on a Cohesity View, the customer wants to reduce storage impact. What built-in feature helps control audit log storage consumption?

A. LDAP policies to restrict audit logging
B. On-demand antivirus scans to prevent unnecessary log entries
C. SMB throttling on the Cohesity View to reduce event generation
D. Audit log retention policy configured in days or size limits

Answer: D

Explanation: Audit log retention policies allow configuring maximum days of retention or total log size limits, helping control storage impact on audit logs. Antivirus scans, SMB throttling, or LDAP settings do not directly control audit log storage.

Question: 717

Which setting in the View domain allows you to adjust how long audit logs are stored locally before forwarding?

A. Audit log cache retention period
B. Local audit log flush interval

C. Audit log disk quota limit
D. Audit log rotation time

Answer: A

Explanation: The audit log cache retention period defines how long logs are kept locally before they are forwarded or purged, allowing administrators to control local disk usage while ensuring logs are kept long enough for transmission.

Question: 718

A telecom's View "CallRecordView" for CALEA 2025 auditing uses cohesity_cli audit calEA CallRecordView --events access,delete --retention 2y --spotlight-integrate, searching deletes from subpoena requests with ML on patterns. Flags 300 off-net accesses. Which capabilities? (Select All that Apply)

A. Event-specific logging for access/delete with 2-year retention, searchable for CALEA subpoenas
B. ML pattern detection flagging 300 off-net accesses for law enforcement alerts
C. Spotlight integration with DataGovern for record classification in audits
D. Session auditing for VoIP duration at 10ms granularity, without file events

Answer: A, B, C

Explanation: Auditing logs access/delete events with 2-year retention for CALEA-compliant subpoena responses via searches. ML detects patterns like 300 off-net accesses for timely alerts. DataGovern via Spotlight classifies records against audits for enhanced forensics. Session auditing tracks calls but not file-level CALEA needs.

Question: 719

You are searching through billions of files in a SmartFiles environment using Marketplace applications. Which feature prevents duplicated search results based on file content?

A. Search result caching on the client side
B. Content hashing and deduplication indexing
C. Timestamp-based file filtering in search queries
D. Permission-based file filtering on the cluster

Answer: B

Explanation: Content hashing and deduplication at the index level prevent duplicate entries of identical file content in search results, ensuring clean and unique results even if multiple copies exist. Client caching or timestamp filtering do not handle duplicates inherently.

Question: 720

During DR planning, a customer requests the ability to fail back data to the primary cluster after failover and recovery on the secondary cluster. Which Cohesity feature supports this bi-directional failover/failback workflow?

A. Active-active cluster federation with snapshot synchronization
B. Immutable archive snapshots stored on cloud
C. Non-disruptive cluster upgrade workflows
D. Periodic full backups using external backup software

Answer: A

Explanation: Active-active cluster federation with snapshot synchronization allows clusters to replicate data bi-directionally, supporting failover to a secondary cluster and failback to the primary cluster seamlessly without data loss or complex restore procedures.

Question: 721

In enterprise banking, view parameters cover global IP allowlists (network), RBAC roles (auth), and key rotation (crypto). Which are the three types for transaction views? (Select All that Apply)

A. Global IP allowlists for network isolation
B. RBAC roles for authentication enforcement
C. Key rotation policies for encryption management
D. Replication SLAs for availability security

Answer: A, B, C

Explanation: Network type via global IP allowlists secures connections. Authentication

type uses RBAC for role-based access. Encryption type includes key rotation for ongoing protection. Replication ensures availability, not core security parameters.

Question: 722

A customer wants to encrypt data at rest on Cohesity Views. What setting must be enabled or configured to ensure the View's data is encrypted when written?

A. Enable SMB signing on the View
B. Activate encryption at the storage domain level
C. Configure NFS export encryption options
D. Use client-side encryption before writing

Answer: B

Explanation: Encryption at rest for Cohesity Views is controlled via the storage domain settings. The storage domain must have encryption enabled to ensure all data written to Views within that domain is encrypted natively. SMB signing and NFS export settings govern data transmission security, while client-side encryption is outside the scope of View-managed encryption.

Question: 723

In SEC 17a-4(f) compliant trading, View "TradeView" SMB allowlists broker nets 172.17.0.0/20 using cohesity_cli view sec-allowlist add TradeView --subnet 172.17.0.0/20. Granular for "Brokers" modify on "/Orders". WORM non-compliant. Which features secure client trades? (Select All that Apply)

A. Enable File DataLock Compliance with Cohasset-certified WORM
B. Configure S3-compatible access with bucket-level encryption
C. Use AD granular for broker modify enforcement
D. Rotate keys quarterly for trade encryption

Answer: A, C

Explanation: Enabling File DataLock Compliance provides Cohasset-certified WORM for immutable trades within 172.17.0.0/20, satisfying SEC 17a-4(f). Using AD granular NTFS for "Brokers" modify ensures role control. S3 adds but not WORM primary, and quarterly rotations secure but secondary to compliance mode.

Question: 724

An administrator wants to export audit logs in CSV format for external analysis. Which method is supported for extracting bulk audit log data from a Cohesity View?

A. Use the Cohesity Web UI to export logs via the Audit Logs section in Views
B. Extract logs via Cohesity API using a bulk download endpoint
C. Email logs generated by antivirus scans automatically
D. Access the logs via direct SMB share and copy audit files

Answer: B

Explanation: Bulk audit log data extraction is best handled via the Cohesity API bulk download endpoints designed to provide logs in a consumable format for external tools. The Web UI may have limited export capabilities but bulk downloads via API are preferred. SMB shares and antivirus email do not deliver audit log exports.

Question: 725

View "HRDB" domain "HRSD" no quota default. 9TB -> 6TB log 1.5:1. Behaviors? (Select All that Apply)

A. Domain 87% alert no block; GET /domains/HRSD?used=6e12 thresh=0.87
B. Logical inf default, throttle >90% domain rate=(1-used/total)*1.5 IOPS
C. iris_cli domain q status --HRSD false, manual --view quota 12TB log
D. Alert global --q_pct=92 default 88, log /logs/hr_capacity.yaml

Answer: A, C

Explanation: Domain alert 87%, no block; status false till manual quota. Throttle 90%, alert 88%.

Question: 726

Default View quotas in a domain with 5TB capacity show 4.8TB used logically. If post-process dedupe frees 1TB unique data nightly at 11 PM UTC, what behavior occurs at 5TB limit during peak writes? (Select All that Apply)

A. Writes block at exact 5TB logical, with ENOSPC error until dedupe cycle completes
B. Schedule post-process via cron-like policy in domain settings: "0 23 * * * cohesity

dedupe run"
C. Alert emails at 90% (4.5TB) if threshold enabled, but soft enforcement allows overcommit until hard limit
D. Logical quota ignores reductions until manual 'view quota refresh' CLI, defaulting to domain total

Answer: A, C

Explanation: Defaults enforce hard logical quota at domain capacity (5TB), blocking writes with ENOSPC until space frees via dedupe. Alerts at 90% notify without halting; post-process is automated nightly without cron spec, and reductions auto-reflect without CLI—manual refresh is for overrides only.

Question: 727

During configuration of an SMB share allowlist, which setting must be enabled for the IP allowlisting to effectively deny all other non-allowed connections?

A. Check "Deny all other clients" in the allowlist panel
B. Disable SMB protocol version negotiation
C. Enable "Allow guest access" globally
D. Add all network subnets manually to the allowlist

Answer: A

Explanation: The "Deny all other clients" checkbox enforces that only explicitly allowed IPs can connect, denying all others by default. Disabling negotiation or enabling guest conflicts with security policies, and manually adding all subnets dilutes intent of allowlisting.

Question: 728

A file stored on a WORM-enabled Cohesity View share cannot be deleted after 90 days retention period. What is the likely cause?

A. Retention period has not yet expired, so file deletion is blocked
B. File permissions disallow deletion
C. Allowlist IP denies deletion requests
D. SMB protocol does not support deletions on WORM shares

Answer: A

Explanation: In WORM mode, files cannot be deleted during the retention period. Until 90 days expire, the system prevents deletion irrespective of permissions or network configuration. Allowlists do not control file operations, and SMB supports deletions if permitted.

Question: 729

Logs missing on 400TB View post-migration; troubleshoot rotation and export. (Select All that Apply)

A. 'audit rotation-check --view migrated --size-max 2GB', set 'config audit.rotation 2GB'
B. 'export audit --view --to s3://backup --format parquet --date 2025-09-01+'
C. Restart 'audit-service restart --view migrated', status 'audit health'
D. 'log-grep "MIGRATION_GAP" /var/audit.log', fix 'sync-migration-logs'

Answer: A, B, C, D

Explanation: Check/fix rotation for 400TB. Export to S3 parquet. Restart service. Grep/fix gaps.

Question: 730

What is the default behavior of a Cohesity View SMB share regarding anonymous access when a new share is created?

A. Anonymous write access is enabled by default
B. Anonymous read-only access is enabled by default
C. Anonymous access is disabled by default, requiring authentication
D. Anonymous access is enabled only for local clients

Answer: C

Explanation: By default, Cohesity View SMB shares disable anonymous access, requiring users to authenticate before accessing data. This approach reduces risk of unauthorized access.

Question: 731

A customer requires running a custom Marketplace application that queries SmartFiles metadata using the Cohesity REST API. Which REST API permission scope should the API token include?

A. Write permissions on SmartFiles views
B. Read and list permissions on SmartFiles Views metadata and content
C. Backup and restore permissions on the cluster
D. Admin permissions on cluster configuration

Answer: B

Explanation: For querying metadata and content, API tokens need at least read and list permissions on SmartFiles Views metadata and content, enabling safe, controlled access. Write, backup/restore, or admin cluster permissions exceed requirements.

Question: 732

In a hospital, Cohesity View file auditing logs {"RequestType": "Delete", "Result": "NFS3_OK", "ClientIP": "10.1.2.3"} and integrates with SIEM via syslog. Which capabilities monitor patient record deletions? (Select All that Apply)

A. JSON logs capturing Delete requests and results
B. SIEM integration via syslog for real-time alerts
C. Subnet-specific audit permissions for read-only
D. No-timestamp logs for privacy compliance

Answer: A, B, C

Explanation: JSON-formatted logs detail deletions with IPs and results, enabling record monitoring. Syslog to SIEM provides real-time HIPAA alerts. Subnet permissions restrict audit view to read-only for security. Timestamps are included for audit integrity.

Question: 733

A customer reports that file services audit logs on their Cohesity View do not show any SMB write operations. What is the most likely cause?

A. Audit logging is enabled but not configured for the ‘write’ operation category
B. SMB protocol is disabled on the View
C. Antivirus scanning is interfering with audit log generation
D. The user accessing the files does not have audit privileges

Answer: A

Explanation: Cohesity file services audit logging can be selectively configured by operation categories (e.g., read, write, delete). If SMB write operations do not appear, it typically means that audit logging for the ‘write’ category was not enabled, even though the audit logging feature itself is active. Protocol availability or antivirus interference does not selectively block write operation logging. User audit privileges do not prevent logging but only affect visibility.

Question: 734

During troubleshooting of file services audit logs on a Cohesity View, which command provides a detailed log of SMB and NFS operations relevant to audit events?

A. viewaudit show --view --detailed
B. auditlogs get --view --file-services
C. smbstat --view --verbose
D. cohesity audit logs fetch --type file-services --view

Answer: A

Explanation: The command viewaudit show --view --detailed is used to retrieve detailed audit logs of file service access events for the specified Cohesity View. This includes SMB and NFS operation details critical for troubleshooting. Other commands are either not valid Cohesity CLI commands or don’t return audit logs specific to file services.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, 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.

Exam Questions:

Killexams.com provides 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 questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

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

Practice Test:

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

Guaranteed Success:

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

Updated Contents:

Killexams.com regularly updates its question bank of MCQs 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.