Cohesity.COH350.v2026-11-23.q46

Exam Code:	COH350
Exam Name:	Cohesity Certified Security Specialist
Certification Provider:	Cohesity
Free Question Number:	46
Version:	v2026-11-23
# of views:	133
# of Questions views:	460
https://www.freeqas.com/qa/Cohesity/COH350/Cohesity.COH350.v2026-11-23.q46.html	

NEW QUESTION: 1
Which Cohesity data isolation method helps protect backup data from ransomware by separating backup storage from production systems?
A. Deduplication
B. Logical air gap
C. Snapshot scheduling
D. Storage tiering
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
Which network protocol is recommended to securely transmit data between Cohesity components?
A. FTP
B. Telnet
C. HTTP
D. TLS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
During incident recovery, which Cohesity capability helps identify anomalous backup activity that may indicate compromised data?
A. Deduplication
B. Storage tiering
C. Anomaly Detection
D. Snapshot scheduling
Answer: C (LEAVE A REPLY)

NEW QUESTION: 4
Which Cohesity security measure ensures that data transmitted between clusters during replication remains protected?
A. Deduplication scheduling
B. Encrypted replication using TLS
C. Storage tiering
D. Snapshot pruning
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Which strategy ensures long-term protection of critical data while maintaining compliance with industry regulations?
A. Allowing unrestricted administrative privileges
B. Removing backup retention policies
C. Disabling encryption to improve performance
D. Implementing immutable storage and retention policies
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
Which best practice ensures effective recovery after a ransomware attack in a Cohesity environment?
A. Remove retention policies for faster restoration
B. Validate backups in a Clean Room before restoration
C. Restore data directly without validation
D. Disable monitoring tools during recovery
Answer: B (LEAVE A REPLY)

NEW QUESTION: 7
Which best practice improves preparedness for responding to cyber incidents in a Cohesity environment?
A. Allow unrestricted administrative privileges
B. Conduct regular disaster recovery and security response testing
C. Store all backups on production systems
D. Disable monitoring and alerting features
Answer: B (LEAVE A REPLY)

NEW QUESTION: 8
Which Cohesity capability enables secure data management by isolating backup environments from external threats and unauthorized access?
A. Logical air gap with immutable backups
B. Deduplication policies

C. Storage tiering
D. Snapshot compression
Answer: (SHOW ANSWER)

NEW QUESTION: 9
Which best practice enhances the security of sensitive data stored within a Cohesity cluster?
A. Disabling encryption services
B. Implementing strong access controls and encryption policies
C. Allowing unrestricted administrative access
D. Removing retention policies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
Which Cohesity feature helps organizations validate their ability to recover data securely after a cyberattack?
A. Replication
B. Clean Room Recovery
C. Snapshot scheduling
D. CloudArchive
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
Which Cohesity capability helps administrators maintain compliance by recording system activity and user actions over time?
A. Snapshot Replication
B. CloudArchive
C. Storage Lifecycle Policies
D. Audit Logging
Answer: (SHOW ANSWER)

NEW QUESTION: 12
Which best practice ensures secure handling of sensitive backup data throughout its lifecycle?
A. Removing audit logs after backup completion
B. Allowing unrestricted administrative privileges
C. Disabling encryption for faster performance
D. Implementing encryption, access controls, and retention policies
Answer: (SHOW ANSWER)

NEW QUESTION: 13

Which encryption capability protects data stored within a Cohesity cluster?
A. Deduplication encryption
B. Data-at-rest encryption
C. Snapshot encryption
D. Tiering encryption
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
An organization wants to ensure that backup data remains isolated from external threats while still being accessible for recovery.
Which approach should be implemented?
A. Disable encryption
B. Store backups on production systems
C. Allow unrestricted administrative access
D. Use immutable storage and air-gapped backups
Answer: D (LEAVE A REPLY)

NEW QUESTION: 15
Which Cohesity capability ensures compliance with regulatory requirements by enforcing data immutability and retention controls?
A. Storage tiering
B. WORM storage
C. Deduplication
D. Snapshot replication
Answer: B (LEAVE A REPLY)

NEW QUESTION: 16
An administrator wants to block unauthorized protocols from accessing the Cohesity cluster.
Which approach should be used?
A. Disable all security policies
B. Remove firewall rules entirely
C. Configure protocol access control policies
D. Enable all ports for redundancy
Answer: C (LEAVE A REPLY)

Valid COH350 Dumps shared by PrepPdf.com for Helping Passing COH350 Exam! PrepPdf.com now offer the **newest COH350 exam dumps**, the PrepPdf.com COH350 exam **questions have been updated** and **answers have been corrected** get the

newest PrepPdf.com COH350 dumps with Test Engine here: https://www.preppdf.com/Cohesity/COH350-prepaway-exam-dumps.html (**133** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

NEW QUESTION: 17
You are enabling encryption at the Cohesity cluster level at the time of the cluster installation. In this scenario, which statement is true about data at rest encryption if the cluster has multiple multitenancy organizations?
A. All Views will have the same encryption keys.
B. Each View will have its encryption keys.
C. All Storage Domains will have the same encryption keys.
D. Each created Storage Domain will have its encryption keys.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 18
Which feature ensures that backup data remains secure and protected against unauthorized modification or deletion?
A. Storage tiering
B. Deduplication
C. WORM storage
D. Snapshot compression
Answer: C (LEAVE A REPLY)

NEW QUESTION: 19
During a security audit, which Cohesity capability demonstrates compliance with data governance and retention requirements?
A. WORM storage with retention policies
B. Storage tiering
C. Snapshot replication
D. Deduplication
Answer: (SHOW ANSWER)

NEW QUESTION: 20
Which best practice enhances secure data management within a Cohesity environment?
A. Remove retention policies to free storage space
B. Disable audit logging
C. Implement encryption, access controls, and data isolation strategies
D. Allow unrestricted user access to all data
Answer: (SHOW ANSWER)

NEW QUESTION: 21

An organization wants to analyze Cohesity logs using a centralized SIEM platform.
Which configuration should be implemented?
A. Disable audit logging
B. Forward logs to a remote syslog server
C. Enable storage tiering
D. Use local-only log storage
Answer: B (LEAVE A REPLY)

NEW QUESTION: 22
What is the primary objective of conducting regular cyber recovery drills in a Cohesity environment?
A. Reduce encryption overhead
B. Improve storage performance
C. Increase backup compression efficiency
D. Ensure preparedness and validate recovery procedures
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Which feature provides secure separation between production workloads and backup data repositories in a Cohesity deployment?
A. Logical air gap
B. Snapshot scheduling
C. Compression
D. Storage tiering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 24
An organization must retain critical data for regulatory compliance while ensuring it cannot be modified or deleted.
Which Cohesity capability supports this requirement?
A. Snapshot pruning
B. Storage tiering
C. Deduplication
D. Legal Hold
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
Which Cohesity feature ensures that stored data remains confidential even if physical drives are compromised?
A. Data compression
B. Data-at-rest encryption

C. Storage tiering
D. Snapshot replication
Answer: (SHOW ANSWER)

NEW QUESTION: 26
An administrator wants to restrict access to specific datasets for different departments.
Which Cohesity feature should be used?
A. Snapshot Replication
B. Role-Based Access Control (RBAC)
C. CloudArchive
D. Storage Tiering
Answer: B (LEAVE A REPLY)

NEW QUESTION: 27
Which Cohesity data protection strategy combines immutability and isolation to safeguard backup data against ransomware attacks?
A. Immutable storage with logical air gap
B. Deduplication scheduling
C. Snapshot compression
D. Storage tiering
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
An administrator wants to prevent unauthorized access to the Cohesity operating environment.
Which practice should be implemented?
A. Allow anonymous login for troubleshooting
B. Enable unrestricted root access
C. Disable logging services
D. Use secure authentication and restrict administrative privileges
Answer: (SHOW ANSWER)

NEW QUESTION: 29
Which best practice enhances data protection and compliance within a Cohesity deployment?
A. Implement encryption, access controls, and retention policies
B. Allow unrestricted administrative access
C. Remove audit logging capabilities
D. Disable encryption to improve performance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
Which authentication method provides the strongest protection against credential theft?
A. Shared administrator accounts
B. Anonymous access
C. Multi-Factor Authentication (MFA)
D. Local authentication with simple passwords
Answer: C (LEAVE A REPLY)

NEW QUESTION: 31
Which security practice ensures accountability and traceability of administrative actions within a Cohesity cluster?
A. Disabling logging services
B. Assigning unique user accounts and roles
C. Sharing administrative credentials
D. Enabling anonymous login
Answer: B (LEAVE A REPLY)

Valid COH350 Dumps shared by PrepPdf.com for Helping Passing COH350 Exam! PrepPdf.com now offer the **newest COH350 exam dumps**, the PrepPdf.com COH350 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com COH350 dumps with Test Engine here: https://www.preppdf.com/Cohesity/COH350-prepaway-exam-dumps.html (**133** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 32
Which Cohesity feature enables organizations to securely store data in isolated environments for long-term protection against cyber threats?
A. Logical air gap with immutable backups
B. Storage tiering
C. Deduplication policies
D. Snapshot compression
Answer: A (LEAVE A REPLY)

NEW QUESTION: 33
Which Cohesity capability ensures that sensitive data stored on the cluster remains protected from unauthorized access by encrypting it at the hardware level?
A. Data-at-rest encryption using self-encrypting drives (SEDs)
B. Storage tiering
C. Data deduplication

D. Snapshot replication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 34
Which feature ensures that backup data cannot be deleted prematurely, even by administrators?
A. Incremental backup policies
B. Snapshot replication
C. Storage tiering
D. WORM compliance mode
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
Which administrative practice strengthens the security posture of a Cohesity cluster by reducing potential vulnerabilities?
A. Enabling anonymous authentication
B. Disabling system updates
C. Disabling unnecessary services and protocols
D. Allowing all services to remain enabled
Answer: (SHOW ANSWER)

NEW QUESTION: 36
Which Cohesity feature supports rapid recovery of data and applications after a cyber incident?
A. Storage Tiering
B. Snapshot Replication and Disaster Recovery
C. Compression Algorithms
D. Deduplication Policies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
To enhance network segmentation, where should a Cohesity cluster typically be deployed?
A. Directly connected to the internet
B. In an unsecured guest VLAN
C. On a public network without restrictions
D. Within a secured internal network segment
Answer: (SHOW ANSWER)

NEW QUESTION: 38
Which action enhances the overall security posture of a Cohesity cluster by minimizing exposure to potential threats?

A. Allowing anonymous administrative access
B. Disabling unnecessary services and restricting system access
C. Enabling all services and protocols
D. Disabling encryption features
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
After detecting a ransomware attack, which Cohesity capability allows administrators to restore clean data in an isolated environment?
A. Storage Tiering
B. Snapshot Replication
C. Deduplication
D. Clean Room Recovery
Answer: D (LEAVE A REPLY)

NEW QUESTION: 40
Which configuration helps protect the Cohesity platform by limiting administrative actions to authorized personnel only?
A. Enabling unrestricted root access
B. Disabling audit logs
C. Allowing shared administrator accounts
D. Implementing Role-Based Access Control (RBAC)
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which Cohesity capability records system events and administrative actions for compliance and security investigations?
A. Audit Logging
B. CloudArchive
C. Storage Lifecycle Policies
D. Replication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 42
An organization is evaluating third-party security tools to enhance its Cohesity deployment. Which scenario justifies integrating such solutions?
A. Simplifying snapshot scheduling
B. Increasing storage performance
C. Enhancing threat detection and security analytics
D. Improving backup compression ratios
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
Which Cohesity feature ensures secure management of encryption keys used to protect backup data?
A. Storage tiering
B. Deduplication
C. Snapshot scheduling
D. Key Management Service (KMS) integration
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
You have determined that ransomware has been triggered in the environment, and administrative credentials may have been compromised.
Which two steps should be performed first to help ensure that the Cohesity cluster is protected in this situation?(Choose two.)
A. Enable audit logging.
B. Change passwords.
C. Open a case with support.
D. Perform an instant mass restore of critical workloads.
Answer: (SHOW ANSWER)

NEW QUESTION: 45
An organization wants to isolate tenant data and administrative controls within a shared Cohesity environment.
Which feature supports this requirement?
A. Snapshot scheduling
B. Deduplication
C. Multitenancy
D. Compression
Answer: C (LEAVE A REPLY)

NEW QUESTION: 46
Which step is essential for maintaining business continuity during a cybersecurity incident affecting production systems?
A. Disable backup operations permanently
B. Restore data from verified immutable backups
C. Disable monitoring and alerting features
D. Remove encryption from backup data
Answer: B (LEAVE A REPLY)

Valid COH350 Dumps shared by PrepPdf.com for Helping Passing COH350 Exam! PrepPdf.com now offer the **newest COH350 exam dumps**, the PrepPdf.com COH350 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com COH350 dumps with Test Engine here: https://www.preppdf.com/Cohesity/COH350-prepaway-exam-dumps.html (**133** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)

Valid COH350 Dumps shared by PrepPdf.com for Helping Passing COH350 Exam! PrepPdf.com now offer the **newest COH350 exam dumps**, the PrepPdf.com COH350 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com COH350 dumps with Test Engine here: https://www.preppdf.com/Cohesity/COH350-prepaway-exam-dumps.html (**133** Q&As Dumps, **40%OFF** **Special Discount:** **Exam-Tests**)