

Cohesity COH350

Cohesity Certified Security Specialist



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ **Up to Date products, reliable and verified.**
- ✓ **Questions and Answers in PDF Format.**

Latest Version: 6.0

Question: 1

Which authentication mechanism allows users to access the Cohesity platform using their corporate credentials without needing separate login information?

Response:

- A. Multi-Factor Authentication (MFA)
- B. Single Sign-On (SSO)
- C. Local Authentication
- D. Token-Based Access

Answer: B

Question: 2

An organization wants to implement a comprehensive data security strategy using Cohesity solutions. Which combination of features provides the strongest protection?

- A. Deduplication and compression
- B. Encryption, RBAC, and immutable storage
- C. Snapshot scheduling and tiering
- D. Storage expansion and replication

Answer: B

Question: 3

An administrator wants to block unauthorized protocols from accessing the Cohesity cluster. Which approach should be used?

- A. Disable all security policies
- B. Configure protocol access control policies
- C. Enable all ports for redundancy
- D. Remove firewall rules entirely

Answer: B

Question: 4

Which step should be performed first when responding to a suspected cybersecurity incident in a Cohesity environment?

- A. Delete all backup data immediately
- B. Identify and contain the affected systems
- C. Disable all monitoring tools
- D. Restore data without verification

Answer: B

Question: 5

Which authentication method enables centralized identity management and simplifies user access to the Cohesity platform?

- A. Local authentication
- B. Single Sign-On (SSO)
- C. Snapshot replication
- D. Deduplication

Answer: B

Question: 6

You want to protect more workloads using Cohesity. You need to protect your production SMB NAS share but want to ensure that all transferred data is encrypted first. In this scenario, what is the configuration option in the UI that should be enabled?

- A. Encryption should be enabled when registering the Source.
- B. Encryption should be enabled at the Protection Group level.
- C. Encryption should be enabled at the Policy level.
- D. Encryption should be enabled at the Storage Domain level.

Answer: B

Question: 7

An organization must ensure that sensitive backup data remains protected during both storage and transmission. Which Cohesity security measures should be implemented?

- A. Deduplication and compression
- B. Encryption in transit and at rest
- C. Snapshot scheduling and replication
- D. Storage tiering and pruning

Answer: B

Question: 8

Which Cohesity security feature protects backup data from ransomware attacks by ensuring immutability?

- A. Replication
- B. WORM storage with retention policies
- C. Deduplication
- D. Compression

Answer: B

Question: 9

After detecting a ransomware attack, which Cohesity capability allows administrators to restore clean data in an isolated environment?

- A. Snapshot Replication
- B. Clean Room Recovery
- C. Storage Tiering
- D. Deduplication

Answer: B

Question: 10

Which best practice improves preparedness for responding to cyber incidents in a Cohesity environment?

- A. Disable monitoring and alerting features
- B. Conduct regular disaster recovery and security response testing
- C. Allow unrestricted administrative privileges

D. Store all backups on production systems

Answer: B

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/coh350>