

Cohesity COH350

Cohesity Certified Security Specialist

For More Information – Visit link below:

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

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

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

Latest Version: 6.2

Question: 1

A customer deploys a Cohesity cluster in a data center with separate production, backup, and management networks. The security team requires that cluster administration be possible only from the management network. Which design best satisfies this requirement?

- A. Allow administrative access from any subnet that contains protected workloads.
- B. Route backup traffic and administrator sessions through the same unrestricted VLAN.
- C. Permit all internal RFC1918 networks and rely on user authentication only.
- D. Restrict management access using network segmentation and firewall rules.

Answer: D

Question: 2

Which two controls help reduce unnecessary network exposure for a Cohesity deployment? Choose two.

- A. Publish administrative interfaces to all internal user networks for easier support.
- B. Use encrypted communication channels where supported.
- C. Allow all backup clients to reach all Cohesity service ports by default.
- D. Permit only the required ports and protocols between approved systems.

Answer: B, D

Question: 3

A security audit identifies that backup data and administrative traffic traverse shared network infrastructure. The customer wants to reduce the risk of interception and unauthorized access. What should the administrator prioritize?

- A. Enforce supported encryption and restrict traffic paths between required endpoints.
- B. Increase backup job concurrency so network sessions complete faster.
- C. Extend snapshot retention to reduce the number of network connections.
- D. Disable indexing because indexed backups require additional metadata.

Answer: A

Question: 4

A network security architect is reviewing Cohesity access paths before production go-live. Which two findings indicate a stronger network security posture? Choose two.

- A. Administrative access is limited to approved management networks.
- B. Backup sources can reach the cluster UI without additional controls.
- C. Firewall rules allow only documented Cohesity traffic flows.
- D. All tenants and administrators share one unrestricted service network.

Answer: A, C

Question: 5

A protected application server is compromised. The security team wants to reduce the chance that this server can be used to attack Cohesity administrative services. Which design choice best addresses this risk?

- A. Increase the number of restore points for the affected application.
- B. Use the same service account for application backups and cluster administration.
- C. Separate administrative access paths from workload backup traffic paths.
- D. Allow application administrators to access the cluster UI during incidents.

Answer: C

Question: 6

A compliance requirement states that protected backup copies must not be modified or deleted before the required retention period expires. Which Cohesity capability is most relevant?

- A. Backup job retry policy
- B. WORM or immutable retention
- C. Protection group priority
- D. File indexing configuration

Answer: B

Question: 7

Which two practices are most aligned with Cohesity system hardening? Choose two.

- A. Disable services and protocols that are not required.
- B. Keep all local administrative accounts enabled for convenience.
- C. Disable external logging to reduce operational noise.
- D. Enforce strong authentication for privileged operations.

Answer: A, D

Question: 8

A customer is concerned that one compromised administrator account could approve a destructive action against protected data.

- a. Which control best reduces this risk?
- A. Longer retention for all protection groups
- B. More frequent backup indexing
- C. Larger backup windows
- D. Quorum approval for sensitive operations

Answer: D

Question: 9

During a Cohesity hardening review, which three findings should be treated as security risks? Choose three.

- A. Privileged accounts do not require MFA.
- B. Sensitive operations can be completed by a single administrator.
- C. Security logs are forwarded to a monitored SIEM.
- D. Unused services remain enabled on the cluster.

Answer: A, B, D

Question: 10

A legal team requires that certain protected data remain undeletable for a defined period, even by administrators. Which configuration area should be reviewed first?

- A. Retention lock or immutable retention policy
- B. Backup job naming convention
- C. Storage efficiency reporting
- D. Dashboard customization

Answer: A

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>