COHESITY

Cohesity Security Specialist Exam Preparation Guide

Introduction

The Cohesity Security Specialist certification exam focuses on ensuring individuals are able to successfully use and deploy Cohesity AI-powered data security and management solutions for robust threat protection. The successful exam candidate should be able to identify potential security risks and how to mitigate those risks by deploying both industry-standard knowledge as well as implementing Cohesity best practices and Cohesity security hardening guidelines. A Cohesity Certified Security Specialist digital badge will be provided upon successful completion of this exam.

Target Audience

The Cohesity Security Specialist certification exam is designed for technical roles, such as:

- Professional Services Engineer
- Security Administrator
- Data Protection Administrator
- Data Architect
- Sales Engineer (SEs)
- Storage Administrators
- Network Administrators

Products Covered

Products, solution areas and capabilities covered in this exam include:

- Cohesity Data Cloud
- Cohesity DataProtect
- Cohesity CloudArchive
- Cohesity Replication
- Cohesity SmartFiles
- Cohesity Threat Defense Architecture
- Cohesity Cloud Services

Recommended Training, Knowledge, and Hands-On Experience

- The Cohesity Platform Foundations course or equivalent knowledge
- The Data Protection Operations course, the Data Protection Implementation course or equivalent knowledge
- The Cohesity Cyber Resilience Foundation course or equivalent knowledge
- The Cohesity Data Security Administration course or equivalent knowledge
- Familiarity with the Cohesity UI
- It is recommended that the candidate have at least six months of hands-on experience with the Cohesity platform and Cohesity DataProtect in a platform or security operator, administrator-level role, security position, or professional services position

Recommended Study Materials

- Cohesity User Guide
- Cohesity Support Portal and Knowledgebase articles
- Cohesity Product Documentation – e.g., Data Cloud, DataProtect, SmartFiles, Hardware Guides, Technical Guides, etc.

Exam Domains/Topics

Section 1 – Network Security (15%)

- Demonstrate knowledge of how to control network protocol access
- Describe Cohesity best practices to secure inflight backup data

Section 2 – System Hardening (22%)

- Describe Write Once, Read Many (WORM) storage technology
- Describe Cohesity encryption capabilities
- Demonstrate knowledge of how to reduce the attack surface
- Demonstrate knowledge of how to secure underlying system access

Section 3 – Security Assessment (13%)

- Describe compliance, legal holds and data retention capabilities
- Describe how Cohesity features can protect against attacks
- Describe Zero Trust platform design
- Describe scenarios where third-party solutions are relevant to a secure Cohesity design
- Assess Clean Room Requirements

Section 4 – User and Access Management (17%)

- Describe the options available for multi-factor authentication
- Describe how to configure single sign-on (SSO)
- Describe how to configure or manage role-based access control (RBAC)
- Demonstrate knowledge of Active Directory user authentication best practices
- Demonstrate knowledge of how to configure multi-tenancy security
- Demonstrate knowledge of how Quorum groups can restrict privileged actions

Section 5 – Periodic Monitoring, Alerting and Auditing (10%)

- Describe Cohesity audit logging capabilities
- Describe the benefits of using remote syslog servers
- Demonstrate knowledge of how to implement monitoring for ransomware or data breaches
- Describe alert notifications on a Cohesity cluster

Section 6 – Incident Response and Remediation (13%)

- Demonstrate knowledge of how to recover from an incident
- Demonstrate knowledge of using a Clean Room to respond to a cyber event

Section 7 – Secure Data Management (10%)

- Demonstrate knowledge of data isolation methods

Recommended Preparation

In addition to the recommended training, reference study materials, and hands-on experience, this document includes a practice test to help candidates prepare for the Cohesity Security Specialist Certification Exam.

Exam Details

Cohesity exams are delivered and proctored through a third-party testing center, with both onsite and remote testing options available. Onsite testing is available in specific locations.

Register for the exam

| Certification Track	Cohesity Solutions Professional
Credential	Cohesity Certified Security Specialist
Exam Number and Title	COH350 – Cohesity Certified Security Specialist
Prerequisite Exams or Certifications	None
Exam Duration	90 minutes
Fee	$200 (USD)
Expiration	2 year
Retake Policy	The exam can be attempted once every 14 days
Language	English
Age requirement	None
Passing Score	60%
Number of Questions	60

Cohesity Certified Security Specialist – Practice Exam Questions and Answers

Below are practice questions similar to those found on the certification exam. Please note that these practice exam questions are provided to give candidates a general idea of the type, look, and feel of the questions on the proctored certification exam. Answers to the questions can be found at the bottom of the document.

The list of exam domains/topics and the recommended study materials offer much more detailed information regarding exam content. Performance on these practice questions does not guarantee similar results or passing marks on the actual certification exam(s).

Cohesity Certified Security Specialist – Practice Exam Questions

Question 1:
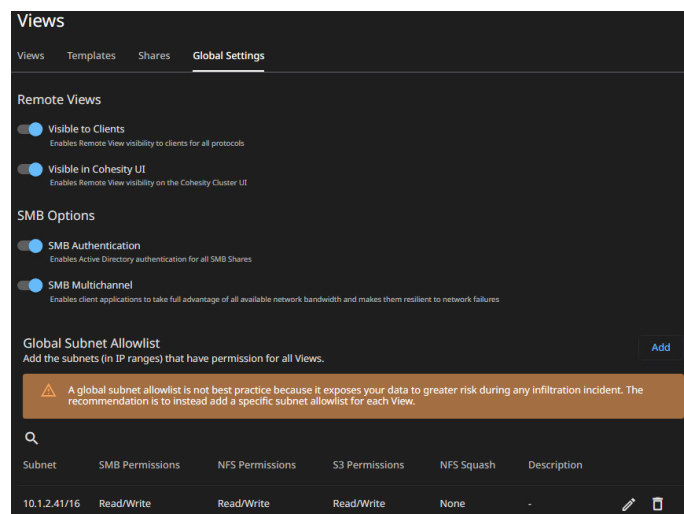
Referring to the exhibit, which statement is correct?

A. Any sessions initiated from 10.1.2.4 can view, modify, and delete a file.

B. Any sessions initiated from 10.2.2.4 can view, modify, and delete a file.

C. Any sessions initiated from 10.2.1.4 can only view and modify a file.

D. Any sessions initiated from 10.1.3.4 can only view a file.

Question 2:

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.

Question 3:

You are asked to enable DataLock on a Protection Policy but you are unable to toggle on the settings.

Which statement is correct in this scenario?

- A. Your user account is not assigned the admin role.
- B. Your user account is not assigned the data security role.
- C. FIPS 140-2 encryption was not enabled.
- D. The Protection Policy is not being used by a Protection Group.

Question 4:

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. Each View will have its encryption keys.
- B. All Views will have the same encryption keys.
- C. Each created Storage Domain will have its encryption keys.
- D. All Storage Domains will have the same encryption keys.

Question 5:

You are working with your team to reduce the attack surface to strengthen your organization's security posture.

In this scenario, what are two best practices that should be implemented according to the Cohesity security hardening guidelines? (Choose two.)

- A. Create roles to enforce the least user privileges.
- B. Create multiple users as needed.
- C. Use the admin user to perform all tasks.
- D. Keep the support channel on at all times.

Question 6:

You want to prevent Cohesity cluster credentials from being compromised by a man-in-the-middle attack.

In this scenario, which method would satisfy this requirement?

- A. Ensure that the cluster or storage domain is encrypted.
- B. Enable SMB encryption.
- C. Add a Network Information Services provider.
- D. Replace the default SSL certificate.

Question 7:

You created a custom role for a new Microsoft SQL DBA. You want to ensure that this user only has access to all backup and recovery operations of the Microsoft SQL servers that are registered within Cohesity.

In this scenario, how would you accomplish this task?

- A. The custom role must have Admin Privileges.
- B. The custom role must have Data Security Privileges.
- C. The user account has restricted access to select Microsoft SQL sources.
- D. The user account has restricted access to select internal Microsoft SQL backup Views.

Question 8:

As part of your responsibilities during a recovery scenario, you need to determine how to re-create your existing Protection Groups and policies.

Which two methods would you use to document this information for re-creation at a later date? (Choose two.)

A. Use the custom reporting database.

B. Use the REST API.

C. Use the built-in Cohesity reports.

D. Share Product Usage Statistics.

Question 9:

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. Open a case with support.

B. Enable audit logging.

C. Change passwords.

D. Perform an instant mass restore of critical workloads.

Question 10:

You need to ensure that the data you are archiving to an External Target cannot be modified by any cluster user.

Which Policy setting must be configured to accomplish this task?

A. CloudSpin

B. DataLock

C. Extended Retention

D. Full Backup

Cohesity Security Specialist – Practice Exam Answers

Sample Question 1	A
Sample Question 2	B
Sample Question 3	B
Sample Question 4	C
Sample Question 5	A, B
Sample Question 6	D
Sample Question 7	C
Sample Question 8	A, B
Sample Question 9	A, C
Sample Question 10	B

Learn more information contact academy@cohesity.com

COHESITY