

Cohesity Data Security Administration

The **Cohesity Data Security Administration** instructor-led course is an 8-hour session focused on the implementation and administration of Cohesity platform security solutions in on-premises, edge, cloud and hybrid environments while adhering to industry and Cohesity security hardening guidelines and best practices. Various hands-on security lab activities are provided as a part of the course.

Target Audience

Cohesity Administrators, Professional Services Engineers, Solution Engineers, Information Security Analysts, Cyber Security Engineers, Information Security Administrators

Prerequisites

(Strongly Recommended) Basic understanding of Information security or Cybersecurity concepts

(Strongly Recommended) Cohesity Platform Foundations and Data Protection Operations Courses or equivalent experience

Course Objectives

Introductions

- Class Introduction
- Course Overview

Data Resiliency

- Fault-tolerance
 - Platform and Data Fault Tolerance
- Immutability (for DataProtect and SmartFiles File & Object)
 - File system immutability
 - DataLock
 - Legal Hold
 - Geographical fault-tolerance
 - Data Isolation

Encryption

- Data at rest
 - Overview
 - Internal KMS (Key Management Server)
 - External KMS
- Data Inflight
 - Overview

- Backup
- Replication
- CloudArchive
- CloudTier
- Labs
 - Configure DataLock
 - Configure Legal Hold
 - Configure Data at rest and in-flight encryption

Zero Trust and Strong Authentication

- Platform management & data access control
 - Network access control
 - Management
 - Data
- User management & RBAC (Role-Based Access Control)
 - Local users
 - Active Directory integration
 - Secure Shell and Secure API Access
 - Multifactor authentication (MFA)
 - Single Sign-On (SSO)
 - Quorum Groups
 - IPMI and underlying OS security

- Support Channel security considerations
 - File & Object access control (external Views access control)
 - NFS access control
 - SMB access control
 - S3 access control
 - Labs
 - Configure network access control using firewall
 - Configure users and RBAC
 - Configure MFA for user access
 - Secure the Linux shell user
 - Configure File-based & Object storage access control
- Detection & Analytics**
- Continuous Monitoring
 - Auditing & Log Management
 - Cluster-level
 - File-level
 - Syslog
 - SNMP
- Helios Security Center
 - Posture Advisor
 - AntiRansomware Dashboard
 - Overview
 - Configuration settings
 - Security Apps & Integrations
 - Overview and examples
 - Introduction to Cohesity Threat Detection and Data Classification
 - Labs
 - Configure auditing
 - Configure an external syslog server
 - Configure SNMP server
 - Security Incident Response and Recovery
 - Overview of Cyber Recovery
 - Cohesity Best Practices

Learn more information contact academy@cohesity.com

© 2025 Cohesity, Inc. All rights reserved.

Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated. This material (a) is intended to provide you information about Cohesity and our business and products; (b) was believed to be true and accurate at the time it was written, but is subject to change without notice; and (c) is provided on an "AS IS" basis. Cohesity disclaims all express or implied conditions, representations, warranties of any kind.

COHESITY

cohesity.com

1-855-926-4374

2625 Augustine Drive, Santa Clara, CA 95054

1000045-004-EN 9-2025