+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 10/27/2026

Sign Up

Cohesity Training

2 days (14 hours)

Overview

Cohesity DataProtect is a data protection solution that enables you to back up and restore physical, virtual, application, and NAS environments. With Protection Groups, retention policies, and restore mechanisms, Cohesity allows you to centralize backup operations and strengthen the resilience of your infrastructure.

Our Cohesity training will help you master essential backup and restore operations so you can effectively manage a data protection infrastructure on a daily basis.

You'll learn to understand the architecture, register sources using agents or APIs, and configure policies tailored to business requirements. You'll set up protection for servers, virtual machines, applications, and NAS shares.

By the end of the training, you'll be able to search for restore points, recover files and volumes, and perform instant restores on compatible platforms. You'll also know how to adjust groups and manage their execution.

This training also covers dashboards, alerts, reports, and logs for diagnosing incidents. The DataLock and extended retention features round out the workshops to enhance security and ensure the reliability of your operational practices.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Describe the architecture and components of Cohesity DataProtect for physical, virtual, application, and NAS environments

- Register and configure protection sources using agents and APIs based on the platforms
- Create and optimize Protection Groups and Protection Policies according to backup, retention, and compliance requirements
- Perform backups and restores of files, volumes, and virtual machines on supported platforms
- Monitor operations, diagnose failures, and manage the execution of protection and restoration
- Configure DataLock and extended retention mechanisms according to security requirements

Target Audience

- Backup administrator
- System administrator
- Virtualization administrator
- Infrastructure engineer
- IT Operations Technician

Prerequisites

- Experience administering Windows Server and Linux
- Knowledge of a virtualization environment such as VMware vSphere or Microsoft Hyper-V
- Proficiency in backup and retention principles, as well as data loss objectives and recovery time objectives
- Knowledge of networks, access rights, and SMB and NFS shares

Technical Prerequisites

- Workstation with a quad-core processor and at least 8 GB of RAM to access the remote lab
- Google Chrome or Mozilla Firefox browser in a supported version compatible with the lab console
- Stable internet connection allowing secure access to the console and tools of the remote lab
- A personal account with the necessary permissions to perform exercises in a Cohesity environment DataProtect environment isolated from production
- Remote lab set up with Windows Server and Linux servers, compatible hypervisors, an application, and test NAS shares

Cohesity Training Agenda

[Day 1 - Morning]

Architecture and Source Preparation

- Cohesity DataProtect architecture: cluster, nodes, distributed storage, management console, and protection components
- Coverage of physical, virtual, application, and NAS environments: data flows and component responsibilities
- Source preparation: compatibility, network connectivity, name resolution, service accounts, and minimum permissions
- Installation and configuration of the Cohesity Agent for Windows and Linux physical servers and the relevant applications
- Registering VMware, Hyper-V, Nutanix AHV, and RHV hypervisors via their management interfaces; distinguishing between generic NAS access and API integrations
- Hands-on workshop: explore the cluster, register a physical server with an agent, a via its management interface, and a NAS share, then verify object discovery.

[Day 1 - Afternoon]

Backup Policies and Execution

- Creating and modifying Protection Groups: selecting objects, inclusion and exclusion rules, organization by criticality
- Configuring Protection Policies: scheduling, retention, data loss objectives, backup windows, and capacity management
- Implementing DataLock and extended retention: lock duration, dedicated permissions, compliance requirements, and consequences of changes
- Executing backups of Windows and Linux servers, VMware and Hyper-V machines, Nutanix AHV and RHV, applications, and NAS sources, according to their specific consistency and compatibility requirements
- Managing jobs with Run Now: selecting objects, pausing upcoming jobs, resuming, canceling, and retrying based on available actions
- Hands-on workshop: Create groups and a policy, configure extended retention and DataLock on test data, then launch and monitor on-demand backups.

[Day 2 - Morning]

Searching for and Restoring Data

- Using search and filters to locate protected objects, jobs, and restore points
- Selecting the restore point, destination, and recovery options: permissions, overwrite, and dependency checking
- File and volume recovery for physical Windows and Linux servers based on supported features
- Restoration of VMware, Hyper-V, Nutanix AHV, and RHV machines, with instant restore when the platform and version allow it
- Recovery of applications and NAS data: consistency, permissions, and functional validation after restoration
- Hands-on workshop: search for a restore point, recover a file and a compatible volume , start a virtual machine using instant restore, and verify restored application or NAS data.

[Day 2 - Afternoon]

Monitoring and Day-to-Day Operations

- Reading dashboards: protection coverage, task statuses, capacity, durations, and compliance with backup objectives
- Using alerts, reports, and logs to identify incidents and document their resolution
- Troubleshooting failures: agents, authentication, connectivity, snapshots, NAS access, and restore destination resources
- Task lifecycle management: distinguishing between pausing and resuming protection, canceling a execution and retrying based on the task type's capabilities, then using Resubmit to resubmit a failed restore
- Operator best practices: daily review of failures, adjustment of groups and policies, monitoring locked retention sets, and regularly validating restores
- Hands-on workshop: diagnosing a simulated failure using alerts and logs, correcting the cause, restarting a backup, resubmitting a restore, and generating an operational summary.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams on new, advanced IT technology or to acquire specific industry knowledge or modern methods.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg