COURSE TABLE OF CONTENTS

Cohesity Data Protection Operations

OEM: Cohesity • Code: COHESITY_DATA_PROTECTION_OPERATIONS

COURSE DESCRIPTION

The Cohesity Data Protection Operations course is a one-day technical class focused on teaching backup administrators how to best utilize Cohesity DataProtect to protect their data. The Data Protection Operations training course teaches common Cohesity DataProtect workflows. Students will be introduced to new data protection concepts realized with Cohesity's revolutionary platform. Lab access is included with this course and expires six months after being assigned. Students of this course will automatically be assigned a self-paced M365 Protection eCourse that includes workflows for Self-Managed and CCS (Cohesity Cloud Services) DataProtect as a Service.

AUDIENCE PROFILE

- New Cohesity Administrators and Operators
- Backup Administrators and Operators

PREREQUISITES

Prerequisite Skills

- Prior experience performing backup and recovery tasks
- Basic System Administration skills (Linux, Windows, Hypervisors)
- Basic understanding of Computer Networking

Training Prerequisites

- Cohesity Platform Foundations (required)
- Hands-on labs for registering, protecting and recovering various sources

COURSE OBJECTIVES

By the end of this course, participants will be able to:

- Describe key Cohesity DataProtect features and use cases
- Register, protect, and recover data from various data sources including physical and virtual servers, and NAS
- Understand the basics of protecting business apps including Microsoft Exchange and Active Directory
- Understand the basics of Cohesity DataProtect workflows troubleshooting

COURSE OUTLINE

Module 1: Introductions

- Class Introduction
- Course Overview

Module 2: Optimizing Cohesity DataProtect

- Foundations Overview

Protection Group Optimization

- API vs Agent-Based Protection
- Agent Deployment
- Application vs Crash Consistency
- Scheduling Options
- Performance Features

Module 3: Hypervisors/Virtual Machines

- VMware Protection Workflows
- Hyper-V Protection Overview

Module 4: Physical servers

Windows

- File-based Protection Workflows
- Block-based Protection Workflows

- Linux Protection Overview

Module 5: Protection Walkthrough Lab - Choose Any Source Type

- Windows (File-Based)
- Windows (Block-Based)
- Linux (File-Based)
- Linux (Block-Based)
- Hyper-V
- Active Directory
- Generic NAS

Module 6: NAS

- Generic NAS Protection Workflows
- NetApp Protection Workflows
- Isilon Protection Overview

Module 7: Business Application

- SQL and Oracle Protection Method Overview
- Exchange Protection Workflows
- Active Directory Protection Overview

Module 8: Reporting and monitoring

- Common monitoring tools and reports

Module 9: Protection Operations Lab

- Verify basic operational tasks utilizing a pre-built Cluster