

SnapProtect Solution Administration (SPSA)

Modality: Virtual Classroom

Duration: 2 Days

SATV Value:

CLC:

NATU: 24 Units

SUBSCRIPTION: No

About this course:

This is a two-day course for learning about NetApp Element Software Administration. In this course, you will be learning with professional instructors who will deliver lectures and give you the opportunity for practical demonstration exercises to learn the administration methods. You will be taught the basic techniques for administering a NetApp Element software cluster in a SolidFire system. You will be learning extensively about the configuring and maintaining a cluster in the system. The Element software has a wide array of features which require adequate training for use. This course will provide you with the opportunity of learning and practicing with those features. You will use the Element CLI tool and web UI feature to manage the storage and network resources.

Learning outcomes:

The course enables you with the following learning outcomes:

- Recognizing and learning about the basic hardware features of an Element cluster
- Completing the steps for the task of configuration for a new Element cluster
- Practically demonstrating the basic aspects of system administration tasks from the Element UI.
- Recognizing the Element data replication features and method for the purpose of backup and recovery
- Overseeing the amount of health and performance level of an Element cluster
- Practically demonstrating the basic steps of system administration tasks by using Element API plug-in.

Audience:

Element Administration enables you to cater to the requirements of NetApp customers, partners, and employees. Hence, this course has an intermediate level for a concise learning of Element Administration.

Requirements:

You need to have a good know-how of Element Fundamentals (Web-based training [WBT])

Course Outline:

Module 1: Getting Started with the SnapProtect Solution

- Describe the SnapProtect solution
- Describe SnapProtect for Open Systems
- Use the Getting Started tab to configure the initial settings of the CommCell Browser
- Describe setup configurations that impact SnapProtect operations

Module 2: The NDMP Protocol and the SnapProtect Solution

- Describe the NDMP protocol
- Node-Scoped NDMP for Clustered Data ONTAP
- Describe Cluster Aware Backup (CAB) operations
- Configure the NDMP Services for Cluster Data ONTAP 8.2 and later
- Configure the NDMP protocol in Data ONTAP systems

Module 3: Protecting Data on NAS File Servers

- Add Data ONTAP clusters and storage virtual machines (SVMs) to a CommCell
- Create NAS subclients and storage policies
- Manage NAS backup and restore operations
- Create schedule policies for NAS data

Module 4: Protecting Microsoft SQL Server Databases

- Describe Microsoft SQL Server architecture
- Backup and restore SQL Server databases
- Schedule backup operations for SQL Server database and log files

Module 5: Protecting Microsoft Exchange Servers

- Describe Microsoft Exchange clients
- Administer SnapProtect backup operations for Exchange mailbox databases
- Restore Exchange mailbox databases
- Use snap mining to perform single-mailbox recovery

Module 6: Protecting Virtual Machines

- Describe the components that protect virtual machines in a SnapProtect solution
- Define guest machines or virtual machines as subclients
- Back up and restore guest machines or virtual machines

Module 7: SnapProtect Solution Management Tasks

- Describe best practices for administering the SnapProtect solution
- Change access passwords, IP addresses, and host names
- Upgrade SnapProtect service packs

New Features

- SnapProtect 10 SP8 New Features
 - Download manager for UNIX installations
 - Warning for NAS client restores
 - Cascade Topology support for SnapProtect for Open Systems (SPOS)
 - Cluster Aware Backup (CAB) extension for clustered data ONTAP
 - VMware view for ALL Versions feature
 - Virtual machines conversion (VMware to Microsoft Hyper-V)
 - Cloud support with AltaVault appliances
- SnapProtect Version 10 SP10
 - Single-file restore (SFR)
 - Root file system support for SnapProtect for Open Systems
- SnapProtect Version 10 SP11
 - Support for two-node MetroCluster configuration Support for MySQL on the UNIX operating system Support for Hyper-V on SMB 3.0 shares

Labs

Locate Vserver Associations

Locate resource pools

Manage disk space of resource pools

Delegate volume creation to SVMs

Tour the CommCell browser

Verify that the SnapProtect license file is valid

Setting up the Windows domain administrator and administrators' group

Use the getting started tab to create two disk libraries

Modify the CommServerDR storage policy

Add the OnCommand Unified Manager server to the CommCell

Review the NDMP configurations on cluster1 and cluster2

Add storage systems to the CommCell

Configure a NAS file server as a CommCell client machine

Use the detect tool to add the SVMs of a cluster as separate clients

Create a NAS subclient

Initiate backup operations

Restore individual files from the primary (snap) copy

Restore individual files from the mirror copy

Create and assign a NAS schedule policy

Set the database option to full recovery

Create a storage policy that is dedicated to a Microsoft SQL database

Create a subclient for a Microsoft SQL database

Initiate a local backup of the AdventureWorks database subclient

Resolve an SQL database backup issue

Initiate a mirror replication of the AdventureWorks database subclient

Configure iSCSI connection between SQL Server host and SVMs

Restore SQL databases

Challenge task

Configure required Exchange server settings

- Create an Exchange database subclient and storage policy
- Initiate local, mirror, and vault back up operations
- Restore Exchange databases from a SnapMirror copy
- Schedule backup operations
- Add the vCenter Server as a virtualization client
- Create a subclient with a dedicated storage policy
- Initiate a backup job
- Restore a virtual machine
- Create and run an auxiliary vault copy of the VMware datastore
- Create schedule policies to back up vCenter servers
- Change user credentials globally
- Gather log files with the send log files tool – not specifying a Job ID
- Initiate and schedule the Job Summary Report