



NETAPP LEARNING SERVICES

# ONTAP Security and Compliance Solutions Administration

Delivery: Instructor-led-training (ILT)

Duration: 2 days

## Course Description

In this course, you learn how to administer NetApp® ONTAP® 9 data management software-integrated security and compliance features. You learn how to create a secure IT environment according to Zero Trust principals such as “least privilege access” and “encrypt everything.” You also administer, configure, and manage the integrated data security and compliance features in ONTAP 9, which include data retention with SnapLock software and data integrity with autonomous ransomware protection.

## Audience

Customers, partners, and employees

## Job Role

Systems administrator, cloud architect, operator, data protection specialist, enterprise architect

## Prerequisites

- *ONTAP Cluster Administration*

## Objectives

This course focuses on enabling you to do the following:

- Secure an ONTAP based storage system according to Zero Trust principles
- Apply least privilege access control to ONTAP administrators and users
- Secure data in flight
- Secure data at rest
- Enforce compliance with data privacy and retention regulations
- Secure access to data by NAS protocols
- Protect data from corruption by ransomware or malware

## Course Content

This course includes the following modules, lessons, and exercises:

<b>Module 1: Security concepts</b>	<ul style="list-style-type: none"><li>• Security threats</li><li>• Security standards and regulations</li><li>• Security defenses</li><li>• Zero Trust</li></ul>	Using the Active IQ Unified Manager security dashboard
<b>Module 2: NetApp ONTAP management security</b>	<ul style="list-style-type: none"><li>• ONTAP authentication</li><li>• Role-based access control</li><li>• Multifactor authentication</li></ul>	<ul style="list-style-type: none"><li>• Applying least privilege access control</li><li>• Configuring MAV</li></ul>
<b>Module 3: NetApp ONTAP network security</b>	<ul style="list-style-type: none"><li>• NAS network security</li><li>• Securing data in flight</li><li>• LIFs</li><li>• SAN security</li><li>• iSCSI security</li><li>• NVMe security</li></ul>	<ul style="list-style-type: none"><li>• Segregating network traffic</li><li>• Securing data in flight</li></ul>
<b>Module 4: NetApp ONTAP storage security</b>	<ul style="list-style-type: none"><li>• Encrypting data at rest</li><li>• NSE</li><li>• NVE</li><li>• Key management</li></ul>	<ul style="list-style-type: none"><li>• Encrypting a volume</li><li>• Deleting data securely</li></ul>
<b>Module 5: NetApp ONTAP data retention</b>	<ul style="list-style-type: none"><li>• SnapLock compliance software</li><li>• Managing SnapLock volumes</li><li>• Protecting SnapLock volumes</li><li>• Advanced SnapLock features</li></ul>	<ul style="list-style-type: none"><li>• Configuring SnapLock compliance software for file retention</li><li>• Using the privileged delete feature</li></ul>
<b>Module 6: NetApp ONTAP NAS security</b>	<ul style="list-style-type: none"><li>• NFS user authentication</li><li>• NFS user authorization</li><li>• NFS permissions</li></ul>	<ul style="list-style-type: none"><li>• Managing access to NAS shares</li><li>• Configuring Storage-Level Access Guard</li></ul>

	<ul style="list-style-type: none"> <li>• Securing in-flight SMB data</li> <li>• SMB user authentication</li> <li>• SMB user authorization</li> <li>• Active Directory features</li> <li>• Storage-Level Access Guard</li> <li>• User name-mapping</li> <li>• Auditing and logging</li> </ul>	
<p><b>Module 7: Protecting NAS data integrity</b></p>	<ul style="list-style-type: none"> <li>• NAS data integrity</li> <li>• Malware and antivirus protection</li> <li>• FPolicy</li> <li>• ONTAP anti-ransomware</li> <li>• Cloud Secure</li> </ul>	<ul style="list-style-type: none"> <li>• Blocking the storage of unwanted data</li> <li>• Creating frequent recovery points</li> <li>• Enabling anti-ransomware protection</li> <li>• Recovering from a ransomware attack</li> </ul>

Course ID: STRSW-ILT-OCSA  
7 February 2023