

ST120 ONTAP Security and Compliance Solutions Administration

Kurzbeschreibung:

Teilnehmer lernen, die in NetApp ONTAP 9 integrierten Security- und Compliance-Features zu administrieren, konfigurieren und managen. Behandelt werden Zero Trust-Prinzipien wie Least Privilege Access und Encrypt Everything sowie SnapLock für Datenaufbewahrung und Autonomous Ransomware Protection für Datenintegrität. Ziel ist der Aufbau und Betrieb einer sicheren IT-Umgebung mit ONTAP 9.

Zielgruppe:

Das NetApp Training **ST120 ONTAP Security and Compliance Solutions Administration** ist ideal geeignet für:

- Systemadministratoren
- Cloud Architekten
- Operatoren
- Datenschutzspezialisten
- Unternehmensarchitekten

Voraussetzungen:

Um dem Lerntempo und den Kursinhalten des Workshops **ST120 ONTAP Security and Compliance Solutions Administration** gut folgen zu können, empfehlen wir vorab den Besuch der NetApp Trainings:

- ST200c ONTAP 9.x Admin Basics
- ST221c ONTAP 9.x Data Protection & High Availability
- ST217c ONTAP 9.x - NAS Advanced inkl. Troubleshooting

Sonstiges:

Dauer: 2 Tage

Preis: 1980 Euro plus Mwst.

Ziele:

Der NetApp Kurse **ST120 ONTAP Security and Ransomware Protection Administration** befähigt Sie zu:

- Sichern eines ONTAP-basierten Speichersystems nach den Prinzipien von Zero Trust
- Anwendung der Least Privilege Access Control für ONTAP-Administratoren und -Benutzer
- Sicherung von Daten während der Übertragung
- Schutz von Daten während der Speicherung
- Durchsetzung der Einhaltung von Datenschutz- und Datenaufbewahrungsrichtlinien
- Sicherer Zugriff auf Daten durch NAS-Protokolle
- Schutz der Daten vor Beschädigung durch Ransomware oder Malware

Hierbei handelt es sich um einen offiziellen NetApp Kurs mit englischen Unterlagen.



Inhalte/Agenda:

- **◆ Security-Konzepte**
 - ◆ Security-Bedrohungen
 - ◆ Security-Standards und Compliance-Vorschriften
 - ◆ Security-Abwehrmaßnahmen
 - ◆ Zero Trust
 - ◆ Verwendung des Active IQ Unified Manager Security Dashboards
- **◆ ~~ONTAP~~ Management Security**
 - ◆ ONTAP-Authentifizierung
 - ◆ Rollenbasierte Zugriffskontrolle (RBAC)
 - ◆ Multi-Faktor-Authentifizierung (MFA)
 - ◆ Anwendung von Least-Privilege-Zugriffskontrolle
 - ◆ Konfiguration der Multi-Admin-Verifizierung
- **◆ ~~ONTAP~~ Network Security**
 - ◆ NAS Network Security
 - ◆ Absicherung von In-Flight-Daten
 - ◆ Logische Netzwerk-Interfaces
 - ◆ SAN Network Security
 - ◆ iSCSI Security
 - ◆ NVMe Security
 - ◆ Segregierung von Netzwerk-Traffic
- **◆ ~~ONTAP~~ Storage Security**
 - ◆ Verschlüsselung von Data-at-Rest
 - ◆ NetApp Storage Encryption (NSE)
 - ◆ NetApp Volume Encryption (NVE)
 - ◆ Key Management
 - ◆ Verschlüsselung eines Volumes
 - ◆ Sicheres Löschen von Daten
- **◆ ~~ONTAP~~ Data Retention**
 - ◆ SnapLock Compliance Software
 - ◆ Management von SnapLock Volumes
 - ◆ Schutz von SnapLock Volumes
 - ◆ Erweiterte SnapLock Features
 - ◆ Konfiguration der SnapLock Compliance Software für File Retention
 - ◆ Verwendung des Privileged Delete Features
- **◆ ~~ONTAP~~ NAS Security**
 - ◆ Absicherung von In-Flight NFS-Daten
 - ◆ NFS User Authentication
 - ◆ NFS User Authorization
 - ◆ Absicherung von In-Flight SMB-Daten
 - ◆ SMB User Authentication
 - ◆ SMB User Authorization
 - ◆ Active Directory Features
 - ◆ Storage-Level Access Guard
 - ◆ Auditing und Logging
 - ◆ Management des Zugriffs auf NAS Shares
 - ◆ Konfiguration des Service Level Access Guards
- **◆ ~~Schutz~~ der NAS Data Integrity**
 - ◆ NAS Data Integrity
 - ◆ File Access Policy
 - ◆ ONTAP Anti-Ransomware
 - ◆ Cloud Insights Cloud Secure
 - ◆ Blockierung der Speicherung unerwünschter Daten
 - ◆ Erstellung häufiger Recovery Points
 - ◆ Aktivierung des Anti-Ransomware-Schutzes
 - ◆ Recovery von einem Ransomware-Angriff