

## MOC 20744 Securing Windows Server 2016

### Übersicht:

Dieser Fünf-Tage-Lehrer-geführte Kurs vermittelt IT-Fachleuten, wie sie die Sicherheit der IT-Infrastruktur, die sie verwalten, verbessern können. Dieser Kurs beginnt mit der Betonung der Bedeutung der Annahme, dass Netzwerkverletzungen bereits aufgetreten sind, und dann lehrt Sie, wie man administrative Anmeldeinformationen und Rechte zu schützen, um sicherzustellen, dass Administratoren können nur die Aufgaben, die sie benötigen, wenn sie müssen.

In diesem Kurs erfahren Sie außerdem, wie Sie Malware-Bedrohungen abschrecken, Sicherheitsfragen durch die Verwendung von Auditing und die Advanced Threat Analysis-Funktion in Windows Server 2016 identifizieren, Ihre Virtualisierungsplattform sichern und neue Bereitstellungsoptionen wie Nano Server und Container nutzen können, um die Sicherheit zu erhöhen. Der Kurs erklärt auch, wie Sie den Zugriff auf Dateien durch Verschlüsselung und dynamische Zugriffskontrolle schützen können und wie Sie die Sicherheit Ihres Netzwerks verbessern können.

### Zielgruppe:

Dieser Kurs richtet sich an IT-Profis, die Windows Server 2016 Netzwerke sicher verwalten müssen. Diese Profis arbeiten normalerweise mit Netzwerken, die als Windows Server-Domänen-basierte Umgebungen konfiguriert sind, mit verwaltetem Zugriff auf die Internet- und Cloud-Services.

Studierende, die Zertifizierung in der 70-744 Securing Windows Server-Prüfung suchen, werden auch von diesem Kurs profitieren.

### Kursziel:

Nach Abschluss dieses Kurses werden die Studierenden in der Lage sein:

- Secure Windows Server.
- Sichere Anwendungsentwicklung und eine Server-Workload-Infrastruktur.
- Sicherheits-Baselines verwalten.
- Konfigurieren und verwalten Sie gerade genug und just-in-time (JIT) Verwaltung.
- Datensicherheit verwalten
- Konfigurieren der Windows-Firewall und einer softwaredefinierten verteilten Firewall.
- Sicherer Netzwerkverkehr.
- Sichern Sie Ihre Virtualisierungsinfrastruktur.
- Verwalten von Malware und Bedrohungen.
- Konfigurieren der erweiterten Auditierung.
- Software-Updates verwalten
- Verwalten von Bedrohungen durch die Verwendung von Advanced Threat Analytics (ATA) und Microsoft Operations Management Suite (OMS)

**Kursübersicht:**

- Angriffe, Brucherkennung und Sysinternals-Werkzeuge
- Schutz von Anmeldeinformationen und privilegierten Zugriff
- Begrenzung der Administratorrechte mit Just Enough Administration
- Privilegierte Zugangsverwaltung und Verwaltungswälder
- Vermeidung von Malware und Bedrohungen
- Analysieren von Aktivitäten mit erweiterten Audit- und Log-Analytics
- Bereitstellen und Konfigurieren von Advanced Threat Analytics und Microsoft Operations Management Suite
- Sichere Virtualisierungsinfrastruktur
- Sichern der Anwendungsentwicklung und der Server-Workload-Infrastruktur
- Planung und Schutz von Daten
- Optimierung und Sicherung von Dateidiensten
- Sicherung des Netzwerkverkehrs mit Firewalls und Verschlüsselung
- Sicherung des Netzwerkverkehrs
- Windows Server aktualisieren

**Voraussetzungen:**

Die Studierenden sollten mindestens zwei Jahre Erfahrung im IT-Bereich haben und sollten:

- Abgeschlossene Kurse 740, 741 und 742 oder das Äquivalent haben.
- Ein solides, praktisches Verständnis von Netzwerkgrundlagen wie TCP / IP, User Datagram Protocol (UDP) und Domain Name System (DNS).
- Ein solides, praktisches Verständnis von Active Directory Domain Services (AD DS) Prinzipien.
- Ein solides, praktisches Verständnis von Microsoft Hyper-V Virtualisierungsgrundlagen.
- Ein Verständnis der Windows Server-Sicherheitsprinzipien.