MS20744 - Securing Windows Server 2016

Microsoft - Windows Server 2016 - Sistemistica

Durata:	Lingue:	Certificazione:
5 Giorni	**Italiano**	**MCSE Core Infrastructure**

Descrizione del corso

This five-day, instructor-led course teaches IT professionals how they can enhance the security of the IT infrastructure that they administer. This course begins by emphasizing the importance of assuming that network breaches have occurred already, and then teaches you how to protect administrative credentials and rights to help ensure that administrators can perform only the tasks that they need to, when they need to. This course explains how you can use auditing and the Advanced Threat Analysis feature in Windows Server 2016 to identify security issues. You will also learn how to mitigate malware threats, secure your virtualization platform, and use deployment options such as Nano server and containers to enhance security. The course also explains how you can help protect access to files by using encryption and dynamic access control, and how you can enhance your network's security.

Programma

1. Securing application development and server-workload infrastructure
    - Using Security Compliance Manager
    - Introduction to Nano Server
    - Understanding containers
    - Protecting data with encryption
    - Planning and implementing encryption
    - Planning and implementing BitLocker
    - Limiting access to file and folders
    - Introduction to FSRM
    - Implementing classification management and file-management tasks

2. Understanding Dynamic Access Control (DAC)
    - Using firewalls to control network traffic flow
    - Understanding Windows Firewall
    - Software-defined distributed firewalls
3. Securing network traffic
    - Network-related security threats and connection-security rules
    - Configuring advanced DNS settings
    - Examining network traffic with Microsoft Message Analyzer
    - Securing SMB traffic, and analysing SMB traffic
    - Updating Windows Server
4. Overview of WSUS
5. Deploying updates by using WSUS