Course : Windows 2022, securing your infrastructure

Practical course - 4d - 28h00 - Ref. WSF
Price : 2260 € E.T.

★★★★★ **5 / 5**

Secure your Windows Server 2022 infrastructure with this comprehensive technical training course! Master advanced protection technologies, from Credential Guard to PKI certificates. Learn how to lock down your identities, encrypt your data and secure your network access.

Teaching objectives

At the end of the training, the participant will be able to:

- Master the new security features of Windows Server 2022 (Credential Guard, Device Guard, VBS)
- Secure Active Directory infrastructure and manage user identities
- Set up and administer a certificate management infrastructure (PKI)
- Data protection through encryption (EFS, BitLocker) and file system management
- Configure access control and rights delegation mechanisms
- Secure network access with technologies such as VPN, IPSec and RADIUS
- Implement DNS protection mechanisms and secure domain controllers

Intended audience
System administrators and engineers.

Prerequisites
Good knowledge of TCP/IP, Windows Server 2019/2022 administration and Active Directory.

Course schedule

1 Windows Server 2022 architecture

- Security features and best practices for Windows 2022.
- What's new in AD domain services, Credential Guard, Device Guard.
- Secured-core server, Hardware root of trust.
- Virtualization-based security (VBS).
- Windows Admin Center to manage Windows Server 2022.
- Dynamic access control for user accounts.
- Set up a security audit using specific tools.

Hands-on work
Basic settings and auditing to secure a Windows 2022 server.

2 Certification authority and PKI architecture

- Presentation and roles of CAs (Certification Authorities).
- Installation and implementation of the Certificate Server (PKI) role.
- Creation and administration of specific certificate templates.
- Manage certificates from WAC and MMC consoles.
- Collection certificates and online answering role.

Hands-on work
Basic certificate server administration. Securing Web access with HTTPS.

3 AD federation services

- Benefits and implementation of the ADFS role.
- Certificate management and creation of trust relationships.
- Install WAP server. Import appropriate certificates.

Hands-on work
Setting up AD federation services, securing AD. WAP installation and configuration.

4 Manage identities

- Assign rights to users.
- Setting up user delegation via the active directory
- Install and configure Windows LAPS and associated GPOs

Hands-on work
Set up a user rights management policy. Use Windows LAPS. Set up user delegation.

5 Securing the DA

- Securing the AD: basic principles.
- What's new in AD-CS certificate services.
- RODC (Read Only Domain Controller): implementation scenarios and benefits.
- DNS SEC implementation. DNS zone protection.
- Roles and interests of ADAC (active directory administration center).
- PSO for password granularity: interest and implementation.

Hands-on work
Securing the AD. Password granularity. Installing and configuring a RODC.

(6) Data protection

- NTFS and ReFS file system security.
- Implementation of EFS and management of collection certificates.
- BitLocker: disk encryption and encryption key storage.
- Centralization of keys in AD via group policies.

Hands-on work

Set up encryption. Data recovery with agent and associated certificates.

(7) NPS, VPN and IP Sec

- VPN: Tunneling principle.
- Secure domain access with IPSec.
- NPS servers. RADIUS infrastructure components (802.1x)

Hands-on work

IPSec implementation. Advanced firewall settings. Setting up a RADIUS server. Limit network access for non DHCP-compliant machines.

Dates and locations

REMOTE CLASS
2026 : 24 Mar., 9 June, 22 Sep., 24 Nov.

PARIS LA DÉFENSE
2026 : 24 Mar., 2 June, 15 Sep., 17 Nov.