Publication date : 05/30/2024

Course : Windows 2019, securing your infrastructure

Practical course - 4d - 28h00 - Ref. WCH
Price : 2650 CHF E.T.

★★★★★ 5 / 5

Acquire the knowledge you need to secure your Windows Server 2019 environment and implement the integrated security tools. You'll learn how to secure the OS, Active Directory, create a PKI architecture, and protect your data and network access.

Teaching objectives

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

- Master the basic settings for securing Windows Server 2019
- Managing certificates
- Be able to secure AD
- Protecting your data
- Protect network access

Intended audience

System administrators and engineers.

Prerequisites

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

Course schedule

1 Windows Server 2019 architecture

- Windows Server 2019 security features.
- What's new in AD domain services. Credential Guard, Device Guard.
- Windows Admin Center (WAC). System Insights.
- AD's role in security, cloud orientation.
- Login and authentication: NTLM and Kerberos.
- Dynamic access control for user accounts.
- Windows 2019 Server advanced firewall.

Hands-on work

Basic settings to secure a Windows 2019 server.

PARTICIPANTS

System administrators and engineers.

PREREQUISITES

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

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more.
Participants also complete a placement test before and after the course to measure the skills they've developed.

2 Certification authority and PKI architecture

- Certificate and private key management. 2-level PKI architecture.
- The certificate server role.
- Manage certificates from the MMC.
- The online answering role.

Hands-on work

Basic certificate server administration. Securing Web access with HTTPS.

3 AD federation services

- Install the ADFS role.
- Install WAP server. Import certificates.
- Building trusting relationships.

Hands-on work

Setting up AD federation services, Securing AD. WAP installation and configuration.

4 Manage identities

- Assign rights to users.
- Set up user delegation.
- Install and configure LAPS. Update AD schema.

Hands-on work

Set up a user rights management policy. Use 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): benefits and implementation.
- ACL (access control list) protection.

Hands-on work

Securing the AD. Password granularity. Installing and configuring a RODC.

6 Data protection

- NTFS and ReFS security.
- Setting up EFS.
- BitLocker: disk encryption and encryption key storage.
- Install Microsoft BitLocker Administration and Monitoring.
- Configure MBAM client via AD group policies.

Hands-on work

Setting up EFS. Retrieving data with an agent. Install MBAM.

TEACHING AIDS AND TECHNICAL RESOURCES

• The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
• At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
• A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

7 NPS, VPN and IP Sec

- VPN: tunneling principle.
- Secure domain access with IPSec.
- NPS servers. RADIUS infrastructure components.

Hands-on work
IPSec implementation. Advanced firewall configuration. RADIUS server setup. Limit network access for non-DHCP-compliant machines.

Dates and locations

REMOTE CLASS
2026 : 10 Mar., 16 June, 29 Sep., 1 Dec.