

Opleiding : Windows 2022, beveiliging van uw infrastructuur

Praktijkcursus - 4d - 28u00 - Ref. WSF

Prijs : 2260 € V.B.

★★★★★ 5 / 5

Beveilig uw Windows Server 2022 infrastructuur met deze uitgebreide technische training! Beheers geavanceerde beveiligingstechnologieën, van Credential Guard tot PKI-certificaten. Leer hoe u uw identiteiten kunt vergrendelen, uw gegevens kunt versleutelen en uw netwerktoegang kunt beveiligen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ De nieuwe beveiligingsfuncties van Windows Server 2022 (Credential Guard, Device Guard, VBS) onder de knie krijgen.
- ✓ De Active Directory-infrastructuur beveiligen en gebruikersidentiteiten beheren
- ✓ Een infrastructuur voor certificaatbeheer (PKI) opzetten en beheren
- ✓ Gegevens beschermen met versleuteling (EFS, BitLocker) en bestandssysteembeheer
- ✓ Mechanismen voor toegangscontrole en delegatie van rechten configureren
- ✓ Netwerktoegang beveiligen met technologieën zoals VPN, IPSec en RADIUS
- ✓ DNS-beschermingsmechanismen implementeren en domeincontrollers beveiligen

Doelgroep

Systeembeheerders en ingenieurs.

Voorafgaande vereisten

Goede kennis van TCP/IP, Windows Server 2019/2022 administratie en Active Directory.

Opleidingsprogramma

DEELNEMERS

Systeembeheerders en ingenieurs.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP, Windows Server 2019/2022 administratie en Active Directory.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vak kennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 Architectuur van Windows Server 2022

- Beveiligingsfuncties en best practices voor Windows 2022.
- Nieuw in AD domeinservices, Credential Guard, Device Guard.
- Beveiligde kernserver, Hardware root of trust.
- Beveiliging op basis van virtualisatie (VBS).
- Windows Admin Center om Windows Server 2022 te beheren.
- Dynamische toegangscontrole voor gebruikersaccounts.
- Zet een beveiligingsaudit op met specifieke tools.

Praktisch werk

Basisconfiguratie en auditing om een Windows 2022-server te beveiligen.

2 Certificeringsautoriteit en PKI-architectuur

- Presentatie en rollen van CA's (certificeringsinstanties).
- Installatie en implementatie van de rol Certificaatserver (PKI).
- Creatie en beheer van specifieke certificaatmodellen.
- Certificaten beheren vanuit WAC- en MMC-consoles.
- Verzamelcertificaten en de online antwoordrol.

Praktisch werk

Basisbeheer van een certificaatserver. Webtoegang beveiligen met HTTPS.

3 AD-federatiediensten

- Voordelen en implementatie van de ADFS-rol.
- Beheer van certificaten en creëren van vertrouwensrelaties.
- De WAP-server installeren. Importeer geschikte certificaten.

Praktisch werk

AD federatiediensten opzetten, AD beveiligen. Installatie en configuratie van WAP.

4 Identiteiten beheren

- Rechten toewijzen aan gebruikers.
- Gebruikersdelegatie instellen via de actieve map
- Windows LAPS en bijbehorende GPO's installeren en configureren

Praktisch werk

Een beleid voor het beheer van gebruikersrechten implementeren. Windows LAPS gebruiken. Delegatie van gebruikers instellen.

5 De DA beveiligen

- Beveiliging van de DBA: basisprincipes.
- Nieuw in AD-CS-certificaatservices.
- RODC (Read Only Domain Controller): implementatiescenario's en voordelen.
- Implementatie van DNS SEC. DNS zone bescherming.
- Rollen en belangen van het ADAC (Active Directory Administration Center).
- PSO voor wachtwoordgranulariteit: interesse en implementatie.

Praktisch werk

De AD beveiligen. Wachtwoord granulariteit. Een RODC installeren en configureren.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

6 Gegevensbescherming

- NTFS en ReFS bestandssysteembeveiliging.
- Implementatie van EFS en beheer van herstelcertificaten.
- BitLocker: schijfcodering en opslag van de coderingssleutel.
- Centralisatie van sleutels in de AD via groepsbeleid.

Praktisch werk

Encryptie instellen. Gegevensherstel met behulp van de agent en bijbehorende certificaten.

7 NPS, VPN en IP Sec

- VPN: principe van tunneling.
- Domeintoegang beveiligen met IPSec.
- NPS-servers. Onderdelen van een RADIUS-infrastructuur (802.1x)

Praktisch werk

IPSec implementeren. Geavanceerde firewall configuratie. Het opzetten van een RADIUS server. Beperken van netwerktoegang voor niet-DHCP-compliant machines.

Data en plaats

KLAS OP AFSTAND

2026 : 24 maa., 9 juni, 22 sep., 24 nov.

PARIS LA DÉFENSE

2026 : 24 maa., 2 juni, 15 sep., 17 nov.