Windows Server - Kerberos and Authentication Troubleshooting

Kód kurzu: GOC172

Posluchači se v tomto kurzu seznámí s principy, funkcí, bezpečností a řešením potíží ověřovacích metod používaných v systémech Windows. Kurz se detailně zabývá autentizačními protokoly jako jsou Kerberos, PKINIT, LM, NTLM, Schannel, Basic i LDAP simple bind a Windows Hello for Business (WHB). Veškerá témata jsou probírána na komplexním multi-forest a multi-domain Active Directory prostředí se vztahy důvěry i AAD/EntraID hybridu. Na kurzu se pracuje v prostředí od Windows 2000, přes XP, 2003, Vista, 2008, přes 7 a 2008 R2 až po Windows 2025 a Windows 11. Účastníci si procvičí nastavení Kerberos a Basic delegaci, constrained delegaci i protocol transition na technologiích jako je IIS, SharePoint, Reporting Services, SQL Server, TMG, nebo ADFS web application proxy, ale i Terminal Services a Remote Desktop Services, nebo Failover Cluster a NLB. Podstatným prvkem školení jsou praktická cvičení na řešení potíží souvisejících s ověřováním. Všichni lektoři kurzu jsou certifikování na nejvyšší možnou technologickou úroveň v této oblasti MCM:Directory a/nebo MCSM:Directory.

Pro koho je kurz určen

Jedná se o pokročilé školení pro zájemce o vnitřnosti a detaily chování ověřovacích protokolů Kerberos, PKINIT, NTLM a Schannel postavených nad Active Directory ve složitých prostředích s Windows Server 2012 R2 a staršími systémy.

Kurz obsahuje kompletní tématiku AD od verzí Windows 2000 až po Windows 2012 R2.

Účastníci si vyzkouší sami prakticky mnoho nestandardních a chybových situací a jejich vlastnoručního řešení a využití low-level nástrojů.

Kurz zahrnuje praktické ukázky konfigurace ověřování a řešení potíží v aplikacích jako je System Center, Exchange, SharePoint, SQL Server, Reporting Services, TMG a UAG.

Co vás na kurzu naučíme

Porozumět do nejmenšího detailu všem autentizačním metodám dostupným ve Windows Server 2012 a starších systémech

Efektivně řešit potíže s ověřováním v libovolně komplikovaném prostředí multi-forest multi-domain trustů a aplikací jako je SQL Server, Reporting Services, System Center, Exchange, SharePoint, UAG a další

Předpokládané vstupní znalosti

Znalosti v rozsahu kurzů uvedených v sekcích Předchozí kurzy a Související kurzy

Dobrá znalost Active Directory a Group Policy

Dobrá znalost technologií TCP/IP a DNS

Osnova kurzu

- Úvod do bezpečnostní a autentizační infrastruktury Windows a LSASS
- Ukládání hesel, heší, přihlašování čipovou kartou, cache a Single-Sign-On (SSO)
- Lokální vs. doménové účty, útoky na hesla a jejich šifrované komunikace přes síť
- Princip počítačových účtů, účty SYSTEM, Network Service, Local Service, NT SERVICE, IISAppPool
- Ověřovací protokoly Basic, Kerberos, LM, NTLM, NTLMv2, Schannel a EAP/TLS a PKINIT
- Optimalizace zabezpečení pro NTLM a Kerberos, implementace AES, omezení NTLM, likvidace RC4
- Kerberos SPN, použití a definice pro DNS aliasy a servisní účty, managed service accounts
- Synchronizace času a požadavky na jeho přesnost v Kerberos, NTLMv2 a SChannel
- Privilege Attribute Certificate (PAC), členství ve skupinách a jejich omezení, velikosti tiketů a access tokenu
- Fungování RODC (Read-Only DC) z pohledu uložených hash hesel a vydávání Kerberos ticketů

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved

- Kerberos unconstrained delegation, constrained delegation, protocol transition
- Podmínky pro Kerberos delegaci, řešení potíží delegace, S4U a S4U2Self
- Použití a nastavení Kerberos ověřování a delegace pro služby jako je Remote Desktop Services a Terminal Services (RDP), SQL Server, SharePoint, System Center, Exchange, UAG, ADFS ad Web Application Proxy
- Porovnání verzí operačních systémů a jejich podpory a schopností týkajících se ověřování
- Active Directory atributy uživatelských účtů týkající se ověřování
- Auditování a řešení potíží a bezpečnostních incidentů
- Příhlašování certifikáty na SSL/TLS služby - Schannel
- Přihlašování čipovou kartou (smart card) - PKINIT a Windows Hello for Business (WHB) s AAD/EntraID
- Windows Hello for Business (WHB) s Key Trust a za použití Cloud Trust s RODC účtem
- Zásady použití a vydávání čipových karet (smart card)
- Optimalizace ověřování v komplikovaných prostředí multiforest multidomain vztahů důvěry
- Závislost ověřování na parametrech síťových linek
- Technologie Kerberos Armoring, Compound Id a Claims
- Autentizační politiky a kombinace identity zařízení do Kerberos tiketů
- Dynamic Access Control (DAC)
- Detaily omezení při členství ve skupině Protected Users
- SID history, SID filtering a PIM/PAM trusty (red forest scénáře)

Příprava k certifikačním zkouškám

U certifikačních zkoušek Microsoft platí, že kromě certifikací MCM, není účast na oficiálním MOC kurzu nutnou podmínkou pro složení zkoušky.

Oficiální kurzy MOC společnosti Microsoft i naše vlastní kurzy GOC jsou vhodnou součástí přípravy na certifikační zkoušky Microsoft jako jsou MTA, MCP, MCSA, MCSE nebo MCM.

Primárním cílem kurzu ovšem není přímo příprava na certifikační zkoušky, ale zvládnutí teoretických principů a osvojení si praktických dovedností nutných k efektivní práci s daným produktem.

MOC kurzy obvykle pokrývají téměř všechny oblasti požadované u odpovídajících certifikačních zkoušek. Jejich probrání na kurzu ale nebývá dán vždy přesně stejný čas a důraz, jako vyžaduje certifikační zkouška.

Jako další přípravu k certifikačním zkouškám lze využít například knihy od MS Press (tzv. Self-paced Training Kit) i elektronický self-test software.

GOPAS Praha
Na Strži 2097/63
140 00 Praha 4 - Krč
Tel.: +420 226 201 390
info@gopas.cz

GOPAS Brno
Nové sady 996/25
602 00 Brno
Tel.: +420 530 513 590
info@gopas.cz

GOPAS Bratislava
Dr. Vladimíra Clementisa 10
Bratislava, 821 02
Tel.: +421 902 903 132
info@gopas.sk

Copyright © 2026 GOPAS, a.s.,
All rights reserved