Windows Server - Kerberos and Authentication Troubleshooting

Course code: GOC172

This four-days instructor led course teaches principal details and how to implement, monitor and troubleshoot Windows authentication methods such as Kerberos, LM, NTLM, PKINIT, Schannel, Basic or simple bind. The training covers the security technologies in Windows 2000 and going through XP, 2003, Vista, 2008, 2008 R2 and 7 to the Windows 2019 and Windows 10. Practical exercises are based on virtual environment which consists of multi-forest and multi-domain Active Directory environment. Students will implement and troubleshoot authentication, Kerberos delegation and protocol transition on application technologies such as SharePoint, IIS, Terminal Services and Remote Desktop Services, SQL Server, Reporting Services, TMG or UAG, and with core technologies such as failover clustering or NLB. The course is taught by trainers who are certified on Microsoft Certified Master Directory Services (MCM: Directory).

At course completion students will be able

Understand the internal operation of various authentication methods availabe in Windows networks, such as Kerberos, NTLM and its older versions, PKINIT, Schannel and Basic and Simple Bind

Implement and troubleshoot complex authentication scenarios such as those requiring Kerberos delegation in environments based on Windows 2012 and application such as SharePoint, Exchange, UAG, System Center or SQL Server

Work in complex and secure environments comprising several Active Directory forests and domains with multiple trust relationships

Prerequisities

Knowledge in extent of the courses which are listed in the bellow sections **Previous Courses** and **Related Courses**

Good understanding of Active Directory and Group Policy

Good understanding of TCP/IP and DNS technologies

Course outline

Windows authentication and security subsystems, LSASS

Passwords, hashes, secret storage and protection with DPAPI, password caches, smart card logon

Principles of computer accounts, principals such as SYSTEM, Network Service, Local Service, NT SERVICE, IISAppPool and managed service accounts

LM, NTLM and NTLMv2 authentication internals and troubleshooting

Kerberos protocol operation and comparison with NTLM

Implementing AES for Kerberos

Service Principal Name (SPN) and its use with DNS aliases and service accounts

Time synchronization, role of Active Directory DCs and PDC, Kerberos reliance on time skew

Privilege Attribute Certificate (PAC), group membership and its limits and PAC validation

Kerberos Unconstrained Delegation, Constrained Delegation and Protocol Transition

Requirements and troubleshooting of Kerberos delegation

Implementing and troubleshooting delegation in complex environments with application such as SharePoint, Exchange, SQL Server, Reporting Services, UAG or System Center

Smart card and certificate (Schannel) logon

Certificate requirements and NTAuth CAs

GOPAS®

Monitoring and auditing

Complex Kerberos and NTLM authentication scenarios in multiforest multidomain environments

Traffic and user experience optimization

Preparation for Microsoft certification

Most Microsoft certification exams do not require students to attend an official MOC course in order to pass the exam.

This applies to all certifications except for MCM

Official Microsoft MOC courses as well as our own GOC courses are good ways of preparation for Microsoft certifications

such as MCP, MTA, MCSA, MCSE or MCM

This does not mean that official MOC courses would serve as the only necessary praparation. The primary goal of an

MOC course is to provide for sufficient theoretical knowledge and practical experience to effectively work with the

related product

MOC courses usually cover most of the topics required by their respective certification exams, but often do not give

every topic the same amount of time and emphassis as may be required to completelly pass the exam