Windows Server 2016 – Managing and Supporting Active Directory Certificate Services (ADCS) – Advanced

Overview

The Windows Server 2016 Managing and Supporting Active Directory Certificate Services (ADCS) Workshop series provides participants with the knowledge and skills to understand, plan, build, manage, monitor, and support a Windows based Public Key Infrastructure (PKI).

This 3-day Advanced Workshop PLUS consists of demonstrations and labs that provide hands-on experience focusing exclusively on the skills and objectives that align with migration, advanced ADCS role services, enrollment strategies and ADCS management processes.

The content of the workshop series has been designed in a way the modules can be delivered independently from each other, providing the possibility to select which modules are included in the workshop.

Key Features and Benefits

This workshop is valuable for organizations who wish to develop their understanding of Windows Server 2016 PKI management and support, aimed at improving the operational health of the PKI by implementing effective operations, support, and management best practices in addition to considerations to plan a migration to Windows Server 2016 PKI.

Technical Highlights

After completing this course, you will be able to:
• Understand and manage advanced ADCS role services
• Understand advanced enrollment strategies
• Understand the common support tasks required to manage and maintain a PKI
• Manage the most common tasks in managing Windows Server ADCS
• Learn how to upgrade and migrate a Certification Authority Infrastructure
This workshop runs for three full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

**Module 7: NDES - Advanced Enrollment Methods (Part 1)** - This module explains how network devices which cannot authenticate against Active Directory can enroll for a certificate by the usage of the Network Device Enrollment Protocol service and by implementing the Simple Certificate Enrollment Protocol (SCEP).

**Module 8: CES/CEP - Advanced Enrollment Methods (Part 2)** - This module explains how the optional role services Certificate Enrollment Policy Web Service and the Certificate Enrollment Web Service have changed the way certificates can be requested enrolled from a Windows Server® 2016 Certification Authority.

**Module 9: OCSP** - This module describes the Online Certificate Status Protocol (OCSP) implementation within the Active Directory Certificate Services in Windows Server® 2016. It will focuses on design principles and deployment strategies.

**Module 10: Upgrade and Migration** - This module explains in detail the proper planning and execution of a Certification Authority migration from Windows Server® 2012 R2 to Windows Server® 2016 in order to ensure stability and supportability of your Public Key Infrastructure.

**Module 11: Constraints, Virtual Smart Cards and Authentication Mechanism Assurance (AMA) for ADDS** – This module summarizes three of the advanced PKI-related concepts which together provide a comfortable and secure way of authentication, mainly used for high privileged accounts (aka Administrators).

**Hardware Requirements:**
Contact your TAM if the necessary hardware needs to be provided.

If you are attending an Open enrollment workshop, the hardware will be provided for you.