Windows Server 2012 – Managing and Supporting Active Directory Certificate Services (ADCS)

Workshop*PLUS*

Target Audience

To ensure the high-quality knowledge transfer expected by the attendees of this four day workshop, the class size is limited to a maximum of 16 students who meet the following criteria:

- *Minimum of 2-3 years' experience with Active Directory administration*
- *Job titles such as:*
  - *System Administrators*
  - *Security Architect/Engineer*
  - *Active Directory Architect/Engineer*

Detailed instruction combined with high quality practice labs prepares students to successfully master the management and support of a Windows Server 2012 ADCS.

Overview

The Windows Server 2012 Managing and Supporting Active Directory Certificate Services (ADCS) Workshop provides participants with the knowledge and skills to understand, manage, monitor, and support a Windows based PKI infrastructure. This 4 day Workshop*PLUS* consists of demonstrations and labs that provide hands-on experience focused exclusively on the skills and objectives that align with managing, monitoring and supporting a Windows Server Public Key Infrastructure (PKI), in addition to the new features in Windows 2012 PKI.

All workshop have been designed so the offering can be delivered independently, allowing the option to select which modules are delivered instead of the full workshop.

Key Features and Benefits

Organizations who wish to develop their understanding of Windows Server 2012 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 2012 PKI.

Technical Highlights

After completing this course, you will be able to:

- Understand basics of Public Key Infrastructure (PKI)
- Understand operational and support considerations for PKI
- Understand the common support tasks required to manage and maintain a PKI
- Understand certificates and Active Directory Certificate Services
- Describe how certificates are used with common Microsoft applications
- Manage the most common tasks in managing a Windows ADCS

Syllabus

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.

This workshop runs for **four** full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Introduction to PKI - This module introduces the components of a PKI and discusses the different design topologies available to deploy a certification authority and PKI hierarchy including Offline, and Online Certification Authorities.

Module 2: Revocation and Chain Building - This module describes how a trust chain against a Public Key Infrastructure (PKI) is established and as well a certificate revocation information works so individuals, computers and applications attempt to verify the validity of certificates.

Module 3: Deploy a 2 Tier PKI Hierarchy - This module covers in details the design and key configuration settings on how to deploy a Two Tier PKI Hierarchy installation and configuration.

Module 4: Upgrade and Migration - This module explains in detail the proper planning and execution of a Certification Authority migration from Windows Server 2008 R2 to Windows Server 2012 in order to ensure stability and supportability of your Public Key Infrastructure.

Module 5: New Features in ADCS 2012 - Active Directory Certificate Services (ADCS) in Windows Server® 2012 provides multiple new features and capabilities over previous versions. This Module describes new deployment, manageability, and capabilities added to ADCS in Windows Server 2012.

Module 6: Certificate Templates and Enrollment Methods - This module explains and demo the correct use of certificate templates in Active Directory Certificate Services and as well what enrollment methods are available so administrators can understand how to successfully enroll for a certificate against a Windows Server 2012.

Module 7: Advanced Enrollment Methods (NDES, CES/CEP) - This module explains how the optional services Certificate Enrollment Policy Web Service and the Certificate Enrollment Web Service changed the way a certificate is enrolled against an Active Directory Certificate Service and as well how network devices that cannot authenticate against Active Directory can enroll for a certificate by the usage of the Network Device Enrollment Protocol service.

Module 8: Cross Forest Auto-Enrollment - This module describes how organizations holding more than one Active Directory forest can take profit from a single Active Directory Certificate Service running on Windows Server 2012 allowing objects across more than one forest to enroll against.

Module 9: Disaster Recovery and Business Continuity - This module will cover the business continuity plans and disaster procedures any company should have in place to quickly recover from a failure affecting the Active Directory Certificate Services in Windows Server 2012.

Module 10: Certificate Operations and Maintenance - This module describes how to properly maintain an healthy Active Directory Certificate Services, explaining in detail what maintenance tasks and operations any administrator should have present while administering the certificate services in Windows Server 2012.

Microsoft