Windows Server 2012 Active Directory Domain Services

Workshop*PLUS*

Target Audience:

This course is an advanced course for Windows Server 2012 Active Directory Domain Services and is only targeted at senior IT staff who have deployed, administered, and managed an active directory forest infrastructure for at least one full year.

The basic concepts and know-how of the product will not be covered in this course, and it is expected that attendees will already possess that knowledge

Overview

The Windows Server 2012 Active Directory Domain Services workshop introduces new features that improve ease of management and deployment, as well as new features for managed service accounts, group policies and new access control capabilities leveraging Dynamic Access Control.

Key Features and Benefits

Students will upgrade a Windows 2008 R2 forest with a trust to a Windows 2012 forest. With extensive hands-on labs and presentations, this course introduces the student to new features related to Domain Services in Windows Server 2012.

Technical Highlights

After completing this course, you will be able to utilize:

- New Server Manager
- New Promotion/Demotion processes
- New Virtualization
- New/improved [Group] Managed Service Accounts
- New features for Kerberos
- New Dynamic Access Control
- Changes in Group Policy

Syllabus

Hardware Requirements:

- Windows Server 2012 or Windows 8 Pro with Hyper-V
- 16 gigabytes (GB) of RAM
- 250 GB hard disk space, 7200 RPM speed (120 GB min available)
- 16-megabyte (MB) video adapter (32 MB recommended)

This workshop runs for **4** full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Deployment and Administration
Upgrade existing 2008 R2 domain to 2012, Explore new features in Server Manager, Promotion/Demotion of 2012 DCs, PowerShell, Server monitoring, changes to RID management

Module 2: Virtualized Domain Controllers
Learn how to clone existing virtual domain controllers and learn about safe restore features for virtual domain controllers.

Module 3: Group Managed Service Accounts (GMSA)
Introduction to GMSA feature including setup and use. Improved over legacy Managed Service Account.

Module 4: Authorization
Refresh Kerberos knowledge. Introduce Kerberos armoring, token compression, changes to Kerberos implementation, disabling cross domain unconstrained Kerberos delegation.

Module 5: Dynamic Access Control
Introduction to setup and use of Windows authorization claims including claim creation, resource management, and new access control user interface using conditions.

Module 6: Group Policy Objects (GPOs)
Introduction to new features with GPOs with reporting, RSOP, and remote GPO refresh.

Microsoft