

## Windows Server® 2008 Group Policy Management: Hands-On - 4 Days

*Course 963 Overview*

- You Will Learn How To**
- Centrally manage workstations and servers with Group Policy Objects (GPOs)
  - Lock down user desktops and control computer configurations
  - Leverage techniques to target GPOs to specific clients
  - Create highly reliable and robust software deployment strategies
  - Enhance security with improved GPO features
  - Troubleshoot failures and optimise GPO performance
- Course Benefits** Maintaining highly reliable and secure Windows environments in a cost-effective manner is a challenge for many organisations. Group Policies provide the ability to centrally manage your workstation and server configurations while streamlining administrative tasks and reducing IT costs. This course provides the knowledge and skills you need to create and manage effective Group Policies.
- Who Should Attend** IT professionals who want to manage and administer Group Policies in a Windows Server 2008 Active Directory environment. A working knowledge of Windows Server 2003 AD or Course 960, "Windows Server 2008 Comprehensive Introduction", is assumed.
- Hands-On Training** Extensive hands-on exercises provide practical experience managing a Windows Server 2008 and Windows 7 environment through Group Policies. Exercises include:
- Establishing a central store and utilising starter GPOs
  - Applying computer and user configuration settings
  - Generating reports for diagnostic purposes
  - Writing WQL queries
  - Implementing robust software delivery mechanisms
  - Configuring core security settings
  - Converting role-based XML data into policy settings
  - Identifying and resolving failures
  - Utilising preferences to manipulate objects
  - Deploying printers through GPOs

# Windows Server® 2008 Group Policy Management: Hands-On - 4 Days

## Course 963 Outline

### Harnessing the Power of Group Policies

#### Introducing Group Policy Objects (GPOs)

- Advantages of centralised administration
- Investigating new features and functionality
- Contrasting user and computer-based settings

#### Controlling computer configurations

- Assigning software packages
- Enforcing workstation security
- Standardising computer settings

#### Managing user environments

- Deploying software packages
- Customising user configurations
- Locking down user desktops with administrative templates

### The Building Blocks of Group Policies

#### Leveraging administrative templates

- Analysing ADMX/ADML file structure
- Implementing predesigned templates and starter GPOs
- Adding custom templates to extend functionality

#### Storing and containerising GPOs

- Leveraging the central store
- Maintaining availability through replication

#### Refreshing user and computer configurations

- Regulating refresh intervals
- Working with policy object versions
- Invoking a policy refresh manually

### Controlling the Deployment of GPOs

#### Exploiting Scopes of Management (SOM)

- Local
- Sites
- Domains
- Organisational Units
- Combining settings through inheritance
- Resolving conflicts between GPO settings
- Generating a Resultant Set of Policies (RSOP) report

#### Limiting GPO application to specific entities

- Disabling GPOs for diagnostics
- Exploiting security filters
- Enforcing settings with No Override
- Merging or replacing user settings with loopback processing

### Writing effective WMI filters

- Enumerating Win32 management classes
- Creating WMI Query Language (WQL) queries
- Designing regular expressions for improved filtering

### Deploying Software Packages with GPOs

#### Constructing a strategic deployment plan

- Interpreting package file structure
- Obtaining and creating package files

#### Modifying software deployment options

- Assigning and publishing software
- Upgrading managed applications
- Customising installations with transform files

#### Ensuring the reliability of GPO-deployed software

- Providing self-healing applications with the Windows Installer Service (WIS)
- Leveraging DFS to enhance performance and reliability

### Centralising Security Management

#### Exposing security settings

- Bitlocker
- Network Access Protection
- Security Center
- Controlling group membership with Restricted Groups

#### Centrally managing security mechanisms

- Securing network communications
- Reducing operating system vulnerabilities

#### Leveraging the Security Configuration Wizard

- Transforming a role-based analysis into a GPO
- Importing settings into the Active Directory

### Tuning and Troubleshooting GPOs

#### Optimising GPO performance

- Expediting Group Policy application
- Detecting and handling slow links

#### Troubleshooting failures and unexpected results

- Isolating failures with Event Logs
- Predicting results through GPO modelling

#### Performing backup and recovery

- Contingency planning through backups

- Recovering Group Policy Objects after failures

### Extending GPO Administration

#### Automating GPO management

- Driving Management Console objects with PowerShell
- Exploiting ADSI with scripting technologies

#### Leveraging advanced tools

- Augmenting the management toolset
- Translating legacy ADM files