



ManageEngine

IT Management, Simplified

Real-time IT management solutions for the new speed of business

Security Hardening: Securing File/Folder Permissions and Delegations

Derek Melber, MVP

derek@manageengine.com



About Your Speaker



Derek Melber, MCSE & MVP (Active Directory and GP)

derek@manageengine.com

- **www.manageengine.com resources**
 - ManageEngine “Active Directory” Blog
 - Security Hardening Website
- **Other useful resources**
 - Twitter: @derekmelber
 - www.windowsecurity.com
 - www.derekmelber.com
 - Group Policy Resource Kit – MSPress



Agenda

- Group Policy Delegations
- Active Directory Delegations
- File and Folder Permissions



Group Policy Delegations



Default Group Policy Delegation

- Organize and manage Group Policy Objects in GPMC
- Used to delegate administration
 - Creating GPOs
 - Linking GPOs
 - Managing GPOs
 - Reading GPOs

Where Group Policy Delegation is Performed

- Creating GPOs
 - Delegated at Group Policy Objects node
- Linking GPOs
 - Delegated at Domain, OU, and site nodes
- Managing GPOs
 - Delegated at each GPO

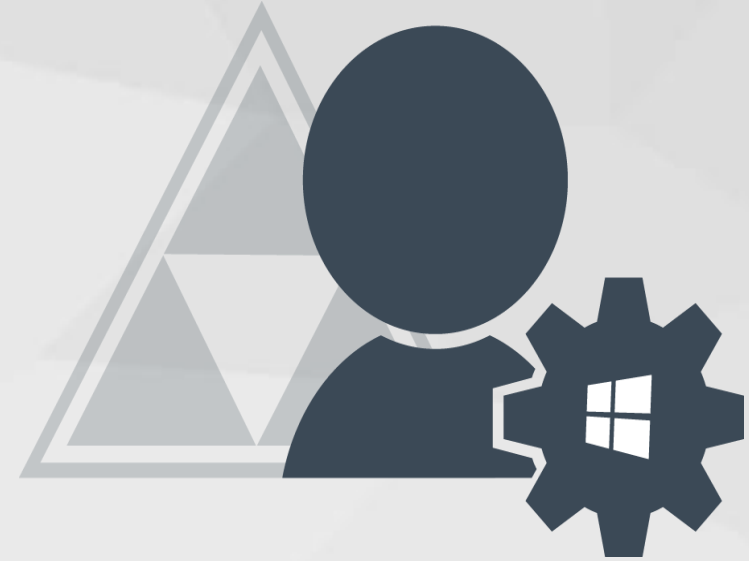
Reporting on Group Policy Delegation

- Screen captures
 - Creating GPOs
 - Group Policy Objects node – Delegation tab
 - Linking GPOs
 - Domain, OU, and site nodes – Delegation tab
 - Managing GPOs
 - GPO – Delegation tab
- GPMC Scripts
- PowerShell Scripts for GPMC

Monitoring and Alerting on Group Policy Delegation

- Monitoring Tools
 - ADAP
- Alerting Tools
 - ADAP

Active Directory Delegations



Establishing AD Delegations

- Active Directory Users and Computers
 - Delegate Control Wizard
 - Establish at domain or OU level
- Typical Delegations
 - Resetting User Password
 - Changing Group Membership
 - Adding Computer to OU

Reporting AD Delegations

- Manually using Security tab on Domain/OU
- PowerShell (Does not provide details for permissions)
- DSACLS command

Securely Configuring AD Delegations

- Remove any delegations that are incorrect
 - Groups
 - All user accounts
- Use product that can “proxy” access to delegated tasks
 - Users can not bypass the product with ADUC
 - Need product to audit behavior of delegated users

Monitoring and Alerting on AD Delegations

- ADMP
 - AD Delegation
 - Provides Audit Reporting
- ADAP
 - Reporting
 - OU Management – Extended Attribute Changes – Permission Changes
 - Alerting
 - Alert for above report

File and Folder Permissions



Default File and Folder Permissions

- Default permissions might not be secure for environment
- Ideally, all file and folder permissions should be configured at creation time

Reporting on File and Folder Permissions

- ICACLS – Windows Vista/2008 and greater
- XCACLS – Windows XP/2003 and before
- ADMP
 - Security Reports - AD Objects Accessible by Accounts

Securing File and Folder Permissions

- Configuring File and Folder Permissions
 - NTFS permissions should be established
 - Share permissions can be left at Everyone – Full Control
 - No user accounts should be on the ACL

Monitoring and Alerting File and Folder Permissions

- ADAP
 - Monitoring File and Folder Permissions
 - File Audit – File Audit Reports – Folder Permission Changes
 - File, User, Server, Share
 - Server Audit – File Integrity Reports
 - Alerting File and Folder Permissions
 - Alerts for above reports

Summary



Summary

- Group Policy Delegations
- Active Directory Delegations
- File and Folder Permissions

Thank you!

Questions?

Derek Melber
derek@manageengine.com