
ManageEngine
IT Management, Simplified
Real-time IT management solutions for the new speed of business

Security Hardening:

Securing Privileged Accounts

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

- Privileged User Accounts
- Privileged Group Accounts
- User Rights
- Service Accounts

Privileged User Accounts

Default Privileged User Accounts

- Local
  - Administrator
- Active Directory
  - Administrator
- Every Windows “administrator” ends with -500 SID

Granting Privileges to User Accounts

- Group membership
- User Right Assignment
- Delegation
- ACL/Permissions
- Service ACLs

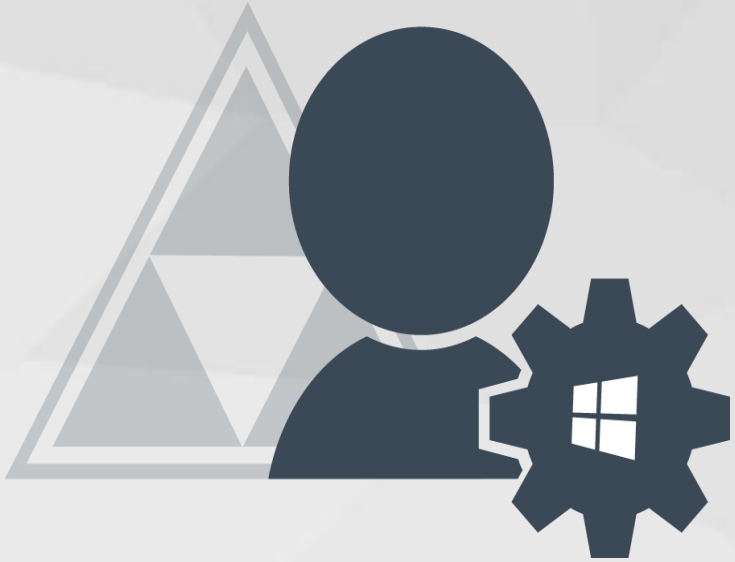
Reporting on Privileged Users

- Once list is obtained
  - ADManager Plus for “user properties”
  - Password required, password expires, more…

Monitoring and Alerting on Privileged Users

- Monitoring Tools
  - ADAudit Plus
  - Monitor logons (S/F), password changes, more…
- Alerting Tools
  - ADAudit Plus
  - Create alerts for reports related to privileged users

Privileged Group Accounts



Default Privileged Groups

- Local
  - Administrators
  - Backup Operators

Default Privileged Groups

- Domain
  - Domain Admins
  - Administrators
  - Cert Publishers
  - DHCP Administrators
  - DNSAdmins
  - Group Policy Creator Owners
  - Account Operators
  - Backup Operators

Default Privileged Groups

- Forest
  - Schema Admins
  - Enterprise Admins

Additional Privileged Groups

- Application and Service Groups
  - SQL
  - Exchange
  - Sharepoint
  - VMWare
  - Etc.

Additional Privileged Groups

- Custom groups
  - Usually created by IT for management
  - Groups are granted privileges through:
    - Group membership
    - User Rights Assignment
    - Delegation
    - ACL/Permissions
    - Service ACLs

Reporting on Privileged Groups

- Need tool that can enumerate/recursively nested groups
- Tools
  - Dumpsec (no iteration)
  - Powershell (recursive)
  - ADManager Plus (recursive)

Monitoring and Alerting on Privileged Groups

- Monitoring Tools
  - ADAudit Plus
  - Update default “Admin Group” report with all privileged groups
  - Create new reports for different types of privileged groups
- Alerting Tools
  - ADAudit Plus
  - Create alerts for reports related to privileged groups

User Rights

Default User Rights

- Default Domain Controllers Policy
  - Configures only domain controllers
- Servers and Workstations
  - No additional user right configurations beyond default install
  - Once joined to AD, no additional user right configurations

Reporting on User Rights

- Secpol.msc

Security Controls for User Rights

- Should not include user accounts
- Ideally Group Policy should configure for consistency

Monitoring and Alerting on User Rights

- Monitoring Tools
  - ADAudit Plus via GPO changes
  - ADAudit Plus via Server auditing
- Alerting
  - ADAudit Plus alerts for user rights reports

Service Accounts

Service Accounts

- Associated with Windows services
- Local or Domain user account
- Reasons for monitoring and control
  - Typically granted elevated privileges
  - Passwords are not changed often
  - Not known where used

Reporting on Service Accounts

- Services.msc
- ManageEngine Free Active Directory Tools

Security Configurations for Service Accounts

- Should not be “Administrator”
- Should not be any “human” account
- Configure with long and complex password
- User account settings
  - Don’t allow account to change password
  - Restrict which computers accounts can logon to

Monitoring and Alerting Service Accounts

- ADAudit Plus
  - Create custom report based on ME Free AD Tool
  - Create alert for “any” change to service accounts

Summary

Summary

- Privileged User Accounts
- Privileged Group Accounts
- User Rights
- Service Accounts

Thank you!

Questions?

Derek Melber
derek@manageengine.com