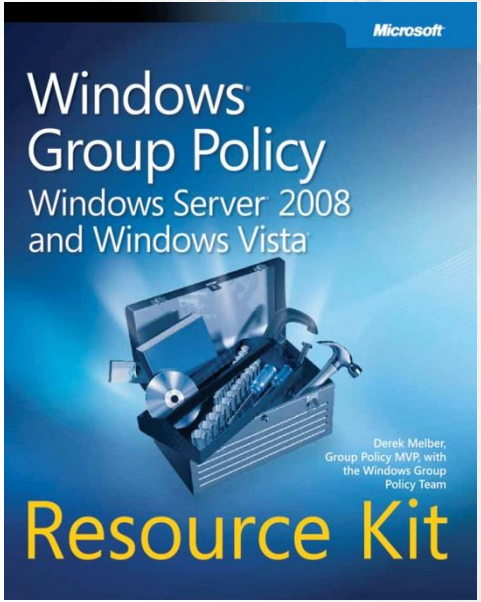
ManageEngine
Powering IT ahead

Next-Gen Monitoring of Active Directory

Click to edit style

About Your Speaker

- Derek Melber, MCSE & MVP (Group Policy and AD)
  - derek@manageengine.com
- Online Resources
  - ManageEngine Active Directory Blog
  - Group Policy Resource Kit – MSPress
- World Tour Seminars
  - Milan: November 17, 2015
  - Rome: November 18, 2015
  - Tokyo: December 8, 2015



Agenda

- What is Change Monitoring of Active Directory?
- Auditing to Track Active Directory Changes
- Advanced Auditing to Track Active Directory Changes
- Security Log in Event Viewer
- ADAudit Plus Reporting and Alerting

What is Change Monitoring of Active Directory?

- Tracking all changes that occur to objects in Active Directory
  - Users
  - Groups
  - Computers
  - Group Policy
  - Password Policy
  - Etc.

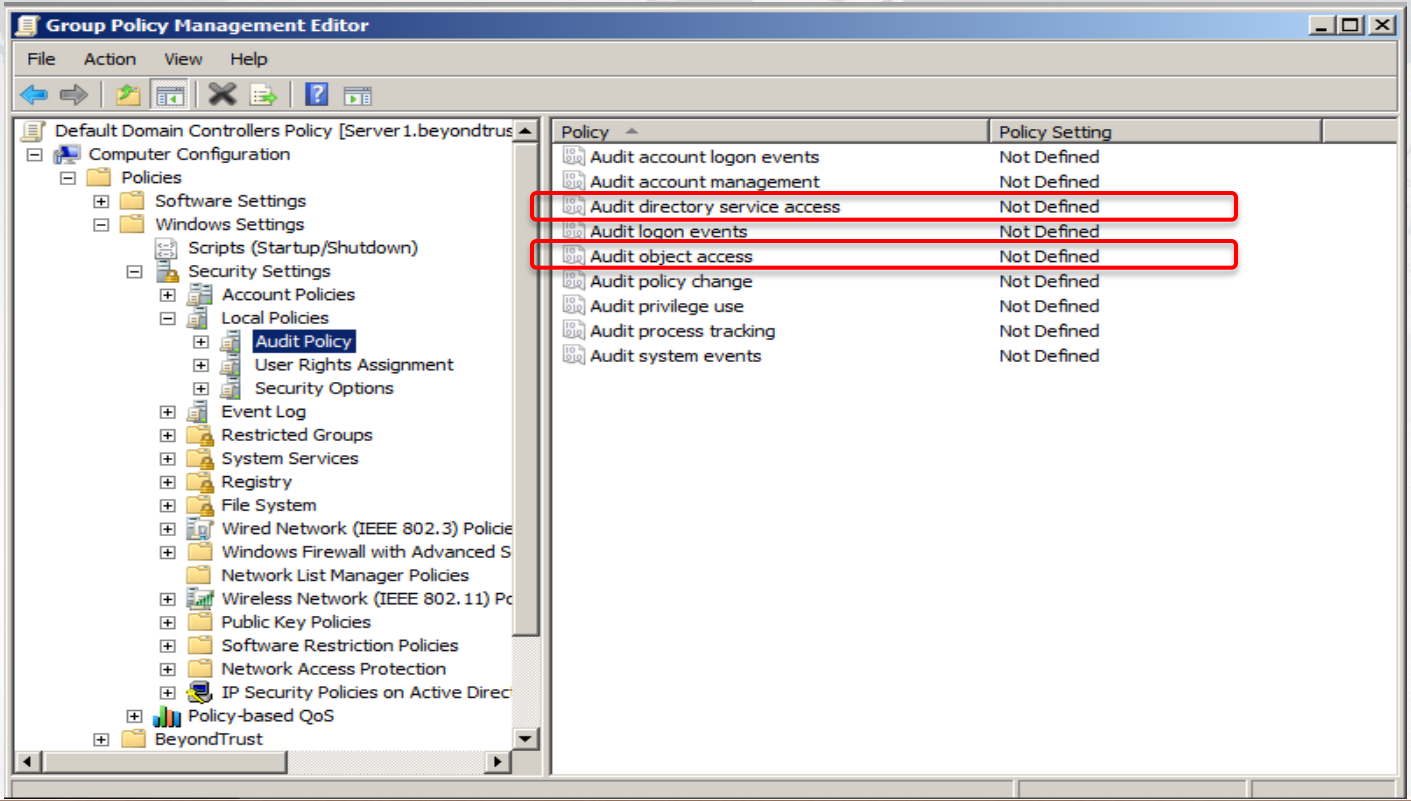
What is Change Monitoring of Active Directory?

- Tracking all details regarding changes to objects in Active Directory
  - Who made the change
  - Which object was changed
  - When the change was made
  - What the new setting is
  - What the old setting was

Auditing to Track Active Directory Changes

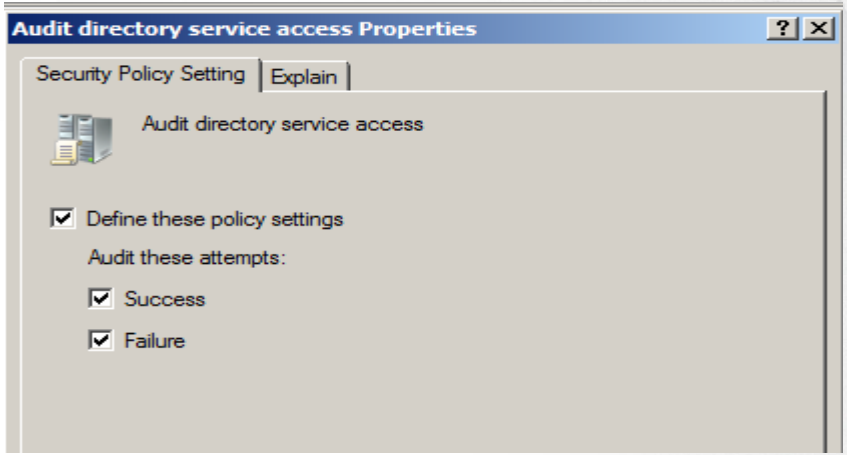
- Each domain controller must have auditing enabled
  - Enabled Auditing of AD through Group Policy
  - Configure the Default Domain Controllers policy OR create new GPO and link to Domain Controllers OU
  - Auditing is located at:
    Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy

Auditing to Track Active Directory Changes



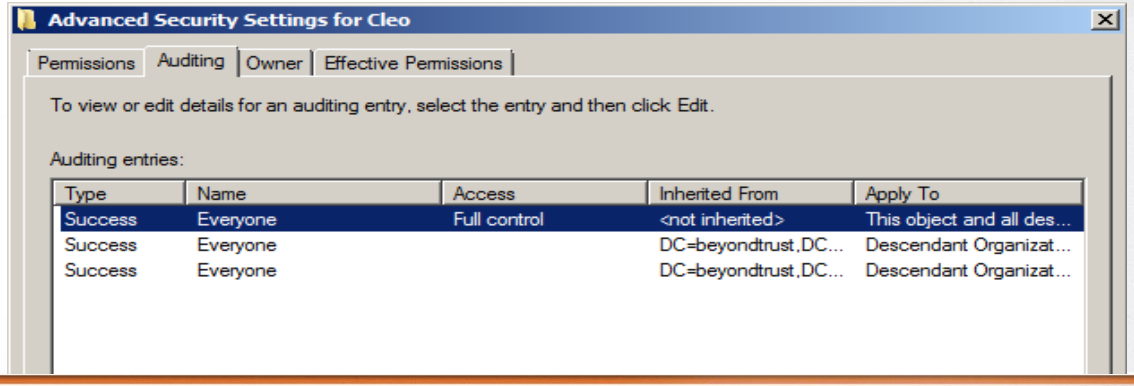
Auditing to Track Active Directory Changes

- Success – Tracks successful changes to AD
- Failure – Tracks denials to change AD



Auditing to Track Active Directory Changes

- Secret!
  - Enable Auditing directory service access
  - Configure Auditing tab after clicking Security tab of object Properties
  - Must select “each property” you want to track!



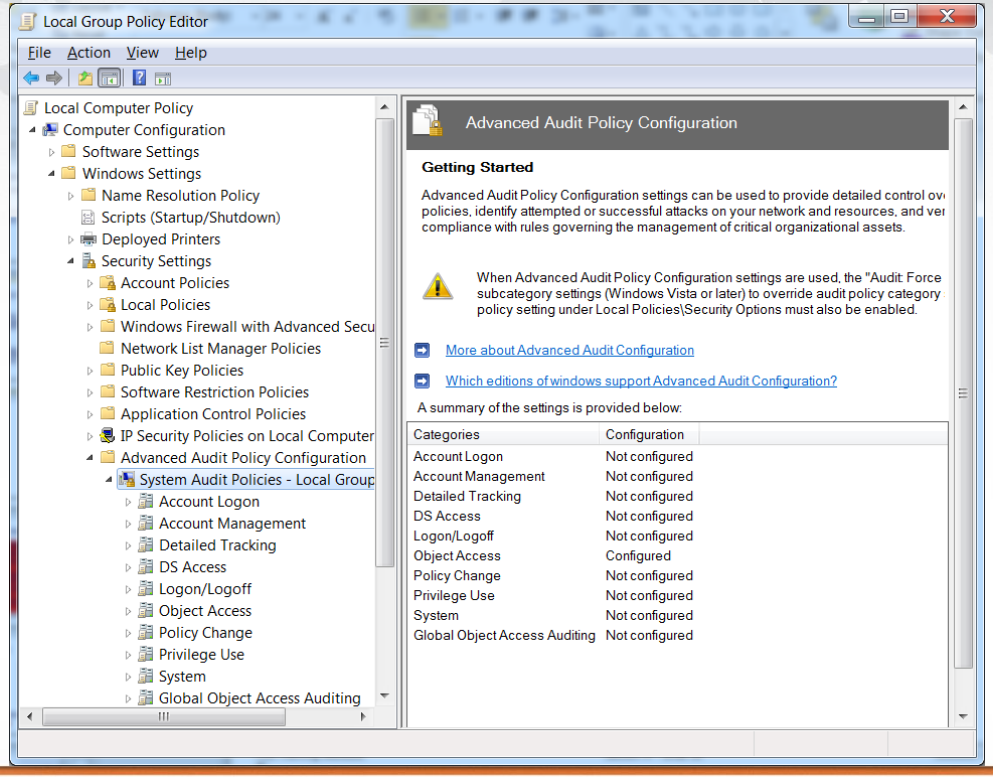
Auditing to Track Active Directory Changes

- Audited events are stored in Event Viewer
  - Tracked changes are stored in Security Log on DC where event occurred
  - Each DC has a unique Security Log
  - In order to view all events, must view each DC or consolidate logs
- Some events generated by Auditing Directory Service Access
- Some events generated by Auditing Object Access

Advanced Auditing to Track AD Changes

- Expanded auditing for auditors and security professionals
- Provides details for most compliance mandates
- Still reports audited events to Security Log

Advanced Auditing to Track AD Changes



Advanced Auditing to Track AD Changes

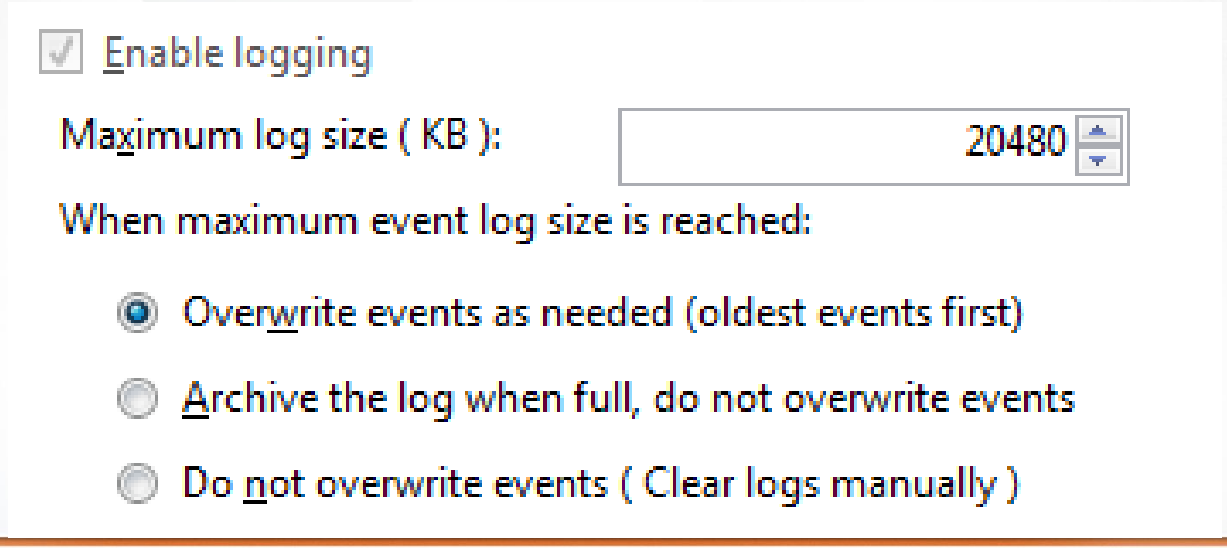
DS Access–Directory Service Changes	Reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed.
DS Access–Directory Service Replication	Reports when replication between two domain controllers begins and ends.
DS Access–Detailed Directory Service Replication	Reports detailed information about the information replicating between domain controllers. These events can be very high in volume.
DS Access–Directory Service Access	Reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server.

Advanced Auditing to Track AD Changes

- Local GPO on Windows 2008 R2 and 7
  - Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System
- AD GPO in GPMC (2008 R2 and 7)
  - Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System

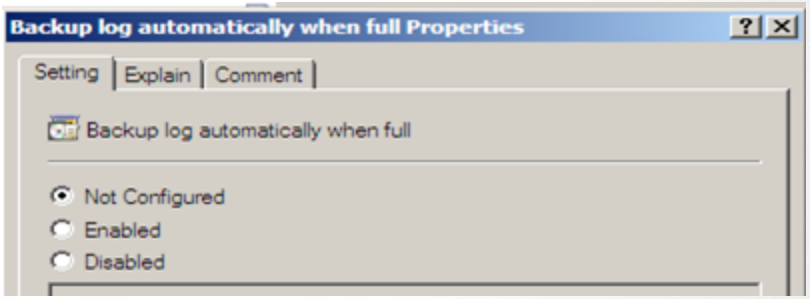
Security Log in Event Viewer

- Maximum Log size: 4GB
- Microsoft Recommended: 300MB



Security Log in Event Viewer

- Backing up Security Log
  - Automatically back up logs
  - Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security
  - Also configure Log file path



Security Log in Event Viewer

- Create **Custom View** of “many logs” or “many sources” into “one log”
- 2008 Domain Controllers
  - Administrative Events
  - Server Roles
    - Active Directory Domain Services
    - DHCP Server
    - DNS Server
    - File Server
    - Network Policy and Access Services
    - Web Server

Security Log in Event Viewer

- Custom View Options
  - Filter by log
  - Logged (Date/Time ranges)
  - Event level (type of log)
  - View options
    - By log(s)
    - By source(s)
  - Task category
  - Keywords

Issues with Event Viewer

- Security Logs size too small
- Interface does not provide for reporting
- Events are hard to decrypt and not easy to analyze
- Events are logged on DC where event occurs… multiple logs
- Alerting is not detailed enough

ADAudit Plus Reporting

- Reporting
  - Over 125 default reports
  - Over 10 default report areas
    - Users
    - Groups
    - Passwords
    - Logons
    - …more

ADAudit Plus Custom Reporting

- Custom Reporting
  - Track service account activity
  - Track Administrator activity
  - Track administrative activity
  - Track modifications to Group Policy

ADAudit Plus Alerting

- Alerting
  - Allows for an email to be sent immediately when a key change is made
    - Track service account activity
    - Track Administrator activity
    - Track administrative activity
    - Track modifications to Group Policy

Summary

- What is Change Monitoring of Active Directory?
- Auditing to Track Active Directory Changes
- Advanced Auditing to Track Active Directory Changes
- Security Log in Event Viewer
- ADAudit Plus Reporting and Alerting

Our gift to you… the link to download the tools!

http://www.manageengine.com/products/active-directory-audit/

Thank you!

ManageEngine
Powering IT ahead

Questions?