Windows Server 2012 / Windows 8 Audit Fundamentals

Jacksonville ISACA Chapter
May 17, 2013

Speaker Introduction: Timothy P. McAliley

13+ years in IT
Currently work for Microsoft
• Premier Field Engineer – SQL Server, Washington, DC.
Previously Worked for:
• Symantec
• Football Fanatics (Jacksonville, FL) (High Volume e-Commerce)
• ASM Research, Inc. (Fairfax, VA) (Defense Contractor)
CISM, CISA, CISSP, MCT, MCITP, MCTS, PMP, ITIL V3

Microsoft
Structure of this Presentation

- Part 2 – New Audit Features in Windows Server 2012 and Windows 8
- 50 minutes each, break in between
- Focused on Demonstrations/Walk-Throughs

Objective and Scope of this Presentation

- Cover security fundamentals – high level
- Dig into new security and audit features
- Nothing specifically covering virtualization, although this is applicable to both physical and virtual infrastructure
- Nothing specifically covering Cloud technologies, although this is applicable to Infrastructure as a Service (IaaS)
Framing the Discussion

• Why Are We Auditing?
  • Compliance Framework
  • Best Practices
  • Reduce Risk Surface
  • Change Monitoring and Tracking

Framing the Discussion

• What Are We Auditing?
  • Changes to user account and resource permissions.
  • Failed attempts by users to log on.
  • Failed attempts to access resources.
  • Changes to system files.
  • Lots more!
Framing the Discussion

• Challenges
  • Control Audit Volume
  • Analyze Audit Events
  • Centrally Manage Audit Policy
  • Audit Removable Storage Devices

Part 1 - Agenda

• Windows Server 2012 and Windows 8 Security Model Fundamentals
• Demo/Walk-through of Local Security Model and Local Security Audit Policy
• Active Directory Overview
• Group Policy Objects (GPOs) Overview
• Domain Security Policy and Group Policy Objects
• Demo/Walk-through of Active Directory /GPO Administrative Tools
Windows Server 2012 and Windows 8 Security Model Fundamentals

• Demo/Walk-through of Local Security Model and Local Security Audit Policy
Windows Server 2012 and Windows 8 Security Model Fundamentals

• Active Directory Overview
  • What Are AD DS Domains?
  • What Are OUs?
  • What Is an AD DS Forest?
  • What Is the AD DS Schema?
  • What Is a Domain Controller?
  • What Is the Global Catalog?
  • What Are Operations Masters?

Overview of AD DS

AD DS is composed of both physical and logical components

<table>
<thead>
<tr>
<th>Physical components</th>
<th>Logical components</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data store</td>
<td>• Partitions</td>
</tr>
<tr>
<td>• Domain controllers</td>
<td>• Schema</td>
</tr>
<tr>
<td>• Global catalog server</td>
<td>• Domains</td>
</tr>
<tr>
<td>• RODC</td>
<td>• Domain trees</td>
</tr>
<tr>
<td></td>
<td>• Forests</td>
</tr>
<tr>
<td></td>
<td>• Sites</td>
</tr>
<tr>
<td></td>
<td>• OUs</td>
</tr>
</tbody>
</table>
What Are AD DS Domains?

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database which is continually synchronized
  - The domain is the context within which user, group, and computer accounts are created
  - The domain is a replication boundary
  - An administrative center for configuring and managing objects
  - Any domain controller can authenticate any logon in the domain

What Are OUs?

Organizational Units

- Containers that can be used to group objects within a domain
- Create OUs to:
  - Delegate administrative permissions
  - Apply Group Policy
What Is an ADDS Forest?

Tree Root Domain

- fabrikam.com
- adatum.com
- atl.adatum.com

Forest Root Domain

What Is the ADDS Schema?

The Active Directory schema acts as a blueprint for AD DS by defining the attributes and object classes such as:

- Attributes
  - objectSID
  - sAMAccountName
  - location
  - manager
  - department

- Classes
  - User
  - Group
  - Computer
  - Site
What Is a Domain Controller?

Domain Controllers

- Servers that host the Active Directory database (NTDS.DIT) and SYSVOL
- Kerberos authentication service and KDC services perform authentication
- Best practices:
  - Availability: At least two domain controllers in a domain
  - Security: Read-Only Domain Controller (RODC) and BitLocker

What Is the Global Catalog?

Global catalog:
- Hosts a partial attribute set for other domains in the forest
- Supports queries for objects throughout the forest
What Are Operations Masters?
In any multimaster replication topology, some operations must be single master

Many terms are used for single master operations in AD DS, including the following:
- Operations master (or operations master roles)
- Single master roles
- FSMOs

Roles
- Forest:
  - Domain naming master
  - Schema master
- Domain:
  - RID master
  - Infrastructure master
  - PDC Emulator master

Windows Server 2012 and Windows 8 Security Model Fundamentals
- Group Policy Objects (GPOs) Overview
- Group Policy Processing
Group Policy Objects (GPOs) Overview

- Components of Group Policy
- What Are Multiple Local GPOs?
- Storage of Domain GPOs

Components of Group Policy

A Group Policy setting defines a specific configuration change to apply to a user or a computer.

A GPO is a collection of Group Policy settings that can be applied to a user, computer, or both, to enact changes.
What Are Multiple Local GPOs?

**Multiple Local Group Policies:**
- Have a single computer configuration that applies to the computer for all users who log on
- Have layers of user settings that can apply only to individual users, not to groups

**There are three layers of user configurations:**
- Administrator
- Non-Administrator
- User-specific

---

**Storage of Domain GPOs**

**Group Policy Components**

**GPO**
- Contains Group Policy settings
- Stores content in two locations

**Group Policy Container**
- Stored in AD DS
- Provides version information

**Template**
- Stored in shared SYSVOL folder on PDC Emulator Single Operations Master
- Provides Group Policy settings
Group Policy Processing

• GPO Links
• Applying GPOs
• Group Policy Processing Order
• What Are the Default GPOs?

GPO Links

To deliver settings to an object, a GPO must be linked to a container

Disabling a link removes the settings from the container

Deleting a link does not delete the GPO

GPOs can be linked to:
• Sites
• Domains
• OUs

GPOs cannot be linked to:
• Users
• Groups
• Computers
• System containers
Applying GPOs

- When you apply GPOs, remember that:
  - Computer settings apply at startup
  - User settings apply at logon
  - Policies refresh at regular, configurable intervals
  - Security settings refresh at least every 16 hours
  - Policies refresh manually by using:
    - The `Gpupdate` command
    - The Windows PowerShell cmdlet `Invoke-Gpupdate`

- With the new Remote Policy Refresh feature in Windows Server 2012, you can remotely refresh policies
What Are the Default GPOs?

There are two default GPOs:

- **Default Domain Policy**
  - Used to define the account policies for the domain:
    - Password
    - Account lockout
    - Kerberos protocol

- **Default Domain Controllers Policy**
  - Used to define auditing policies
  - Defines user rights on domain controllers

Windows Server 2012 and Windows 8 Security Model Fundamentals

- Demo/Walk-through of Active Directory /GPO Administrative Tools
Windows Server 2012 and Windows 8 Security Model Fundamentals

~BREAK~

Part 2 - Agenda

- New Audit Features in Windows Server 2012 and Windows 8
- Dynamic Access Control
- Expression-based Security Audit Policies
- Enhanced Global Object Access Auditing
- Enhanced User Login Auditing
- Auditing New Types of Securable Objects
- Auditing Removable Storage Devices
New Audit Features in Windows Server 2012 and Windows 8

• New or Enhanced Functionality:
  • Dynamic Access Control
  • Expression-based Security Audit Policies
  • Enhanced Global Object Access Auditing
  • Enhanced User Login Auditing
  • Auditing New Types of Securable Objects
  • Auditing Removable Storage Devices
Dynamic Access Control

What Is Dynamic Access Control? You can use Dynamic Access Control to help to address four scenarios:

• Central access policy for access to files
• Auditing for compliance and analysis
• Protecting sensitive information
• Access denied remediation
Dynamic Access Control

Most common reasons for implementing Dynamic Access Control:
- Cannot achieve desired results with NTFS
- Reduce security group complexity
- Adhere to compliance regulations
- Protect sensitive information
- Upgrading to access control based on attributes

Dynamic Access Control

- Demo/Walk-through of Configuring Dynamic Access Control
Expression-based Security Audit Policies

- Windows Server 2012 introduces expression-based security audit policies. Dynamic Access Control in Windows Server 2012 enables you to create targeted audit policies by using expressions that are based on:
  - user
  - Computer
  - resource claims
Expression-based Security Audit Policies

• The following are examples of expression-based audit policies that administrators can apply in Windows Server 2012:

  • Audit everyone who does not have a high security clearance and yet tries to access documents with high business value.

  • Audit all vendors when they try to access documents that are related to projects that they are not working on.

• Narrowly defined policies such as these can help regulate the volume of audit events and limit them to only the most relevant data or users.

• Expression-based audit policies can be authored directly on a file or folder or applied centrally through Group Policy by using Global Object Access Auditing.

Expressi-on-based Security Audit Policies

• Demo/Walk-through of Configuring Expression-based Access Control
Enhanced Global Object Access Auditing

- Windows Server 2012 enables you to create expression-based audit policies by using Global Object Access Auditing.
- Merges the Global Object Access Auditing policies from multiple GPOs located on the client computers.
Enhanced Global Object Access Auditing

- Global Object Access Auditing policy settings allow administrators to define computer system access control lists (SACLs) per object type for either:
  - file system
  - registry
- The specified SACL is then automatically applied to every object of that type.

Enhanced Global Object Access Auditing

- Auditors will be able to prove that every resource in the system is protected by an audit policy by just viewing the contents of the Global Object Access Auditing policy settings.
- For example, a policy setting "track all changes made by group administrators" shows that this policy is in effect.
Enhanced User Login Auditing

- Windows Server 2012 and Windows 8 include user logon auditing.
- With the right audit policy in place, the Windows operating systems will generate an audit event (4624) each time a user logs on to a computer locally or remotely.
- In Windows Server 2012 and Windows 8, a new event (4626) contains information about the attributes of the file that was accessed.
- This additional information can be leveraged by audit log management tools to enable event filtering that is based on file attributes and user attributes.
Auditing New Types of Securable Objects

• In Windows Server 2012 and Windows 8, existing File Access events (4656, 4663) contain information about the attributes of the file that was accessed.
Auditing Removable Storage Devices

• In Windows Server 2012 and Windows 8, an audit event is generated each time a user attempts to access a removable storage device.
Auditing Removable Storage Devices

• Demo – Configure and Validate Auditing Removable Storage Devices

Resources for More Information
Resources for More Information

• What’s New In Security Auditing

• Dynamic Access Control

• Security Auditing Overview

Summary

• Windows Server 2012 and Windows 8 Security Model Fundamentals
• New Audit Features in Windows Server 2012 and Windows 8
• Other Issues and Considerations
• Resources for More Information
Q&A?

Email me at timothy.mcaliley@Microsoft.com

~Presentation is on the event site~

Follow Me on Twitter @Sysframeworks

LinkedIn: Timothy P. McAliley

Make Sure To Register For
IT Pro Camp, June 15, 2013

6 CPEs - free for full day attendance

www.itprocamp.com/jacksonville
Thank You!