Report: Advanced Auditing & Monitoring in Active Directory

1. Introduction

In any enterprise-level IT infrastructure, **Active Directory (AD)** serves as the backbone of identity and access management. It controls user authentication, permissions, and access to critical resources. However, its central role also makes it a prime target for both internal and external threats. Unauthorized changes to Active Directory objects — such as the addition of users to privileged groups, modifications to directory structures, or unauthorized access to sensitive files — can lead to privilege escalation, data breaches, and regulatory non-compliance.

To mitigate these risks, organizations must implement **advanced auditing and monitoring** techniques. These practices provide visibility into who is accessing or modifying sensitive data and systems, when they are doing it, and what exactly is being changed. By proactively auditing key objects and monitoring system logs, administrators can quickly detect and respond to suspicious or unauthorized activity, reducing the window of opportunity for attackers.

This task involves setting up **System Access Control Lists (SACLs)** on critical AD objects, configuring **custom audit policies** for file access, and monitoring **specific security event IDs** that indicate changes in group membership or object modifications. Such practices are not only essential for security monitoring but are also often required to meet compliance standards such as **ISO 27001**, **HIPAA**, **GDPR**, or **PCI-DSS**.

2. Objective

The objective of this task is to implement a robust auditing and monitoring framework within an Active Directory environment to enhance visibility, detect unauthorized actions, and maintain security compliance. This involves configuring System Access Control Lists (SACLs) on critical Active Directory objects, such as the Domain Admins group, to ensure that any access or modification attempts are logged in the Security Event Logs. In addition, the task focuses on monitoring specific security event IDs, including Event ID 4732, which indicates when a user is added to a privileged group, and Event ID 5136, which logs directory object modifications. Furthermore, a custom audit policy will be configured to monitor access to sensitive files and folders, enabling the detection of unauthorized read, write, or delete actions. Collectively, these measures aim to provide comprehensive audit trails, support incident response and forensic analysis, and help fulfill regulatory and organizational security requirements.

Key goals include:

- **Enhance Visibility into Critical AD Object Changes**
  Ensure that all access and modification attempts to sensitive AD objects—especially high-privilege groups like *Domain Admins*—are captured through configured SACLs and logged for review.

- **Detect Privilege Escalation Attempts in Real Time**
  Monitor specific security event IDs (e.g., **4732**, **5136**) to identify unauthorized changes to group memberships or directory objects, helping detect potential privilege abuse or insider threats.

- **Track Access to Sensitive Files and Directories**
  Implement custom file system auditing policies to monitor and log access to high-value data repositories, enabling early detection of unauthorized file access or data exfiltration attempts.

- **Establish a Comprehensive Audit Trail for Forensics and Compliance**
  Maintain detailed security logs that support incident investigations and help meet compliance standards such as **ISO 27001**, **HIPAA**, or **GDPR**.

- **Strengthen Security Monitoring and Incident Response Capabilities**
  Integrate auditing data with SIEM tools or manual review processes to enable timely alerts, reduce response time to anomalies, and support a proactive cybersecurity posture.

3. Methodology

This methodology is divided into three structured **phases**, corresponding to each task. Each phase contains detailed explanations of the steps involved, providing a clear understanding of their purpose and how they fit into the overall auditing and monitoring strategy.

3.1 Configure SACLs on Critical AD Objects

The first phase focuses on enabling **System Access Control Lists (SACLs)** for critical Active Directory (AD) objects. SACLs define the auditing settings for each AD object, specifying which actions should be logged when users or administrators interact with these objects. For sensitive objects like the **Domain Admins group**, any changes (such as adding or removing users, modifying permissions, etc.) need to be captured to ensure accountability and to detect unauthorized activities. By configuring SACLs, you enable a robust monitoring mechanism that can detect attempts to modify high-value groups or objects in Active Directory.

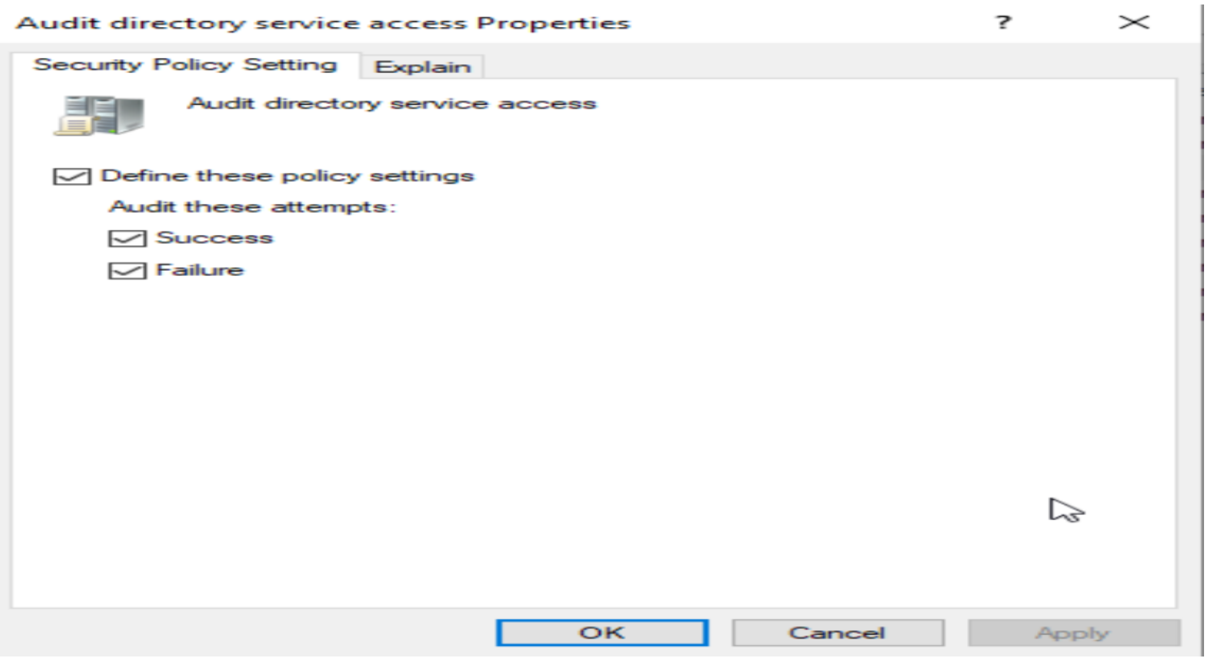
- **Enable Directory Service Auditing via GPO**

  In this step, you enable the **Audit directory service access** policy through **Group Policy Management Console (GPMC)**. This policy ensures that any interaction with AD objects — including modifications, deletions, or access attempts — will be logged in the Security event logs. By enabling both **Success** and **Failure** auditing, you ensure that both successful and failed access attempts to critical AD objects are captured. This step lays the groundwork for later auditing and is crucial for monitoring high-privilege objects like the Domain Admins group, where unauthorized access or modification could lead to severe security risks.

  Go to:

  Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy

(Enable Audit directory service access.)



Audit directory service access

☑ Define these policy settings

Audit these attempts:

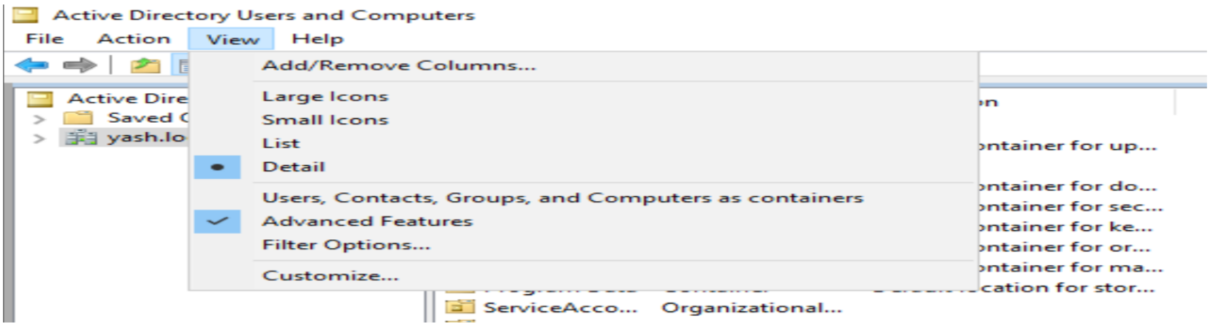
☑ Success

☑ Failure

- **Enable Advanced Features in ADUC**

  After enabling directory service auditing via GPO, the next step is to configure the **Active Directory Users and Computers (ADUC)** tool to expose additional advanced features. By default, some sensitive security settings in ADUC are hidden. Enabling **Advanced Features** ensures that these hidden properties, including the **Auditing** tab, become visible for critical objects like the Domain Admins group. This step is important as it gives you the necessary interface to configure the **SACLs** and specify which access attempts should be audited for this specific AD object.

  View > Advanced Features to enable hidden object properties and security settings.

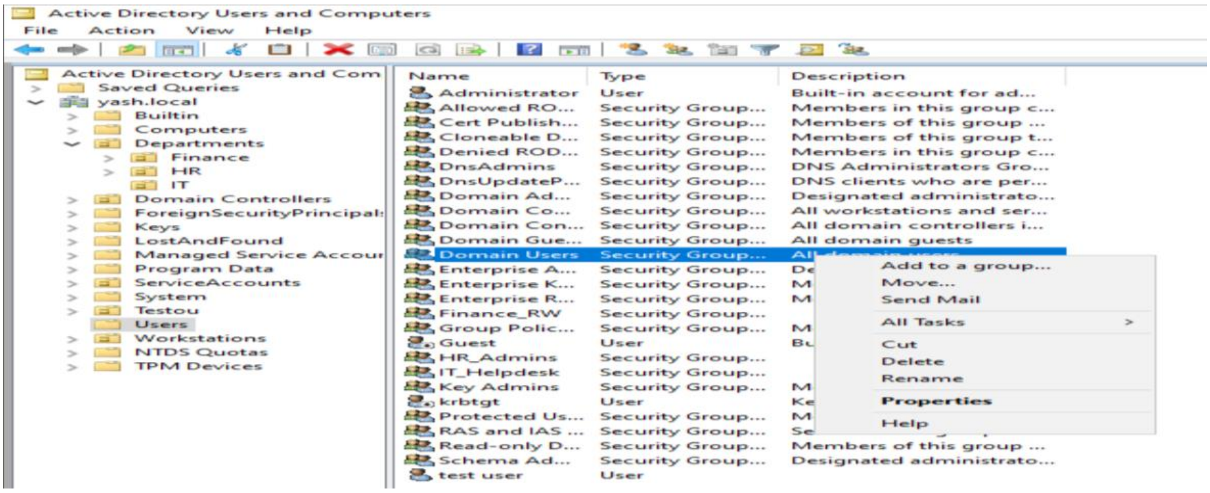


- **Set SACL on the Domain Admins Group**

  The final step of this phase involves configuring **SACLs** on the **Domain Admins** group itself. The **Auditing** tab in the Domain Admins group properties allows you to specify which actions should be monitored, such as adding/removing users, modifying permissions, or making changes to group properties. By selecting a principal, you can define what kind of activities should trigger logging, including actions like modifying group membership or changing security settings. Once configured, this SACL will capture any interaction with the Domain Admins group and log it as **Event ID 4662**, providing visibility into changes to this critical AD object.

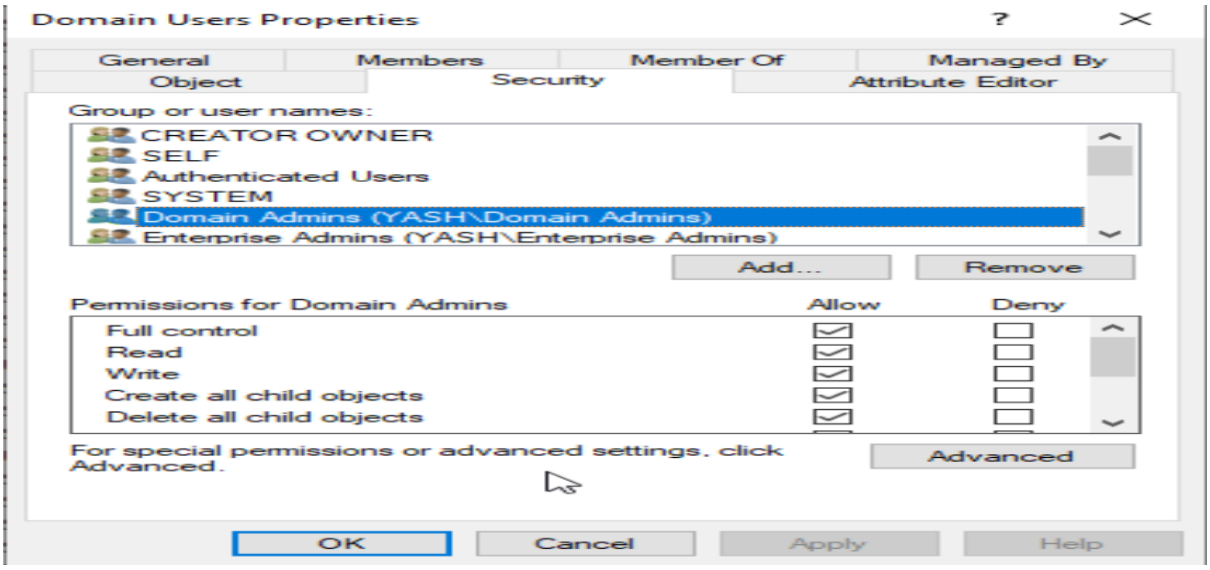
  Right-click > **Properties** > **Security** tab > Click **Advanced**.

  Go to the **Auditing** tab > Click **Add**.



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	De
Enterprise K...	Security Group...	M
Enterprise R...	Security Group...	M
Finance_RW	Security Group...	
Group Polic...	Security Group...	M
Guest	User	Bu
HR_Admins	Security Group...	
IT_Helpdesk	Security Group...	
Key Admins	Security Group...	M
krbtgt	User	Ke
Protected Us...	Security Group...	M
RAS and IAS ...	Security Group...	Se
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
test user	User	

  (Selected the Domain Admins)



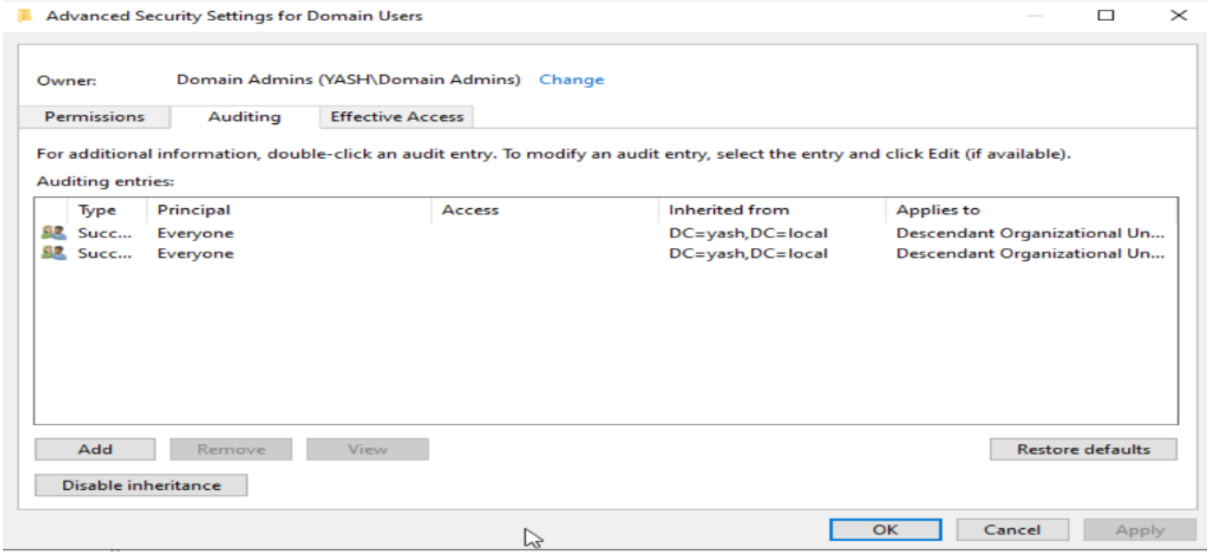
Group or user names:

CREATOR OWNER
SELF
Authenticated Users
SYSTEM
Domain Admins (YASH\Domain Admins)
Enterprise Admins (YASH\Enterprise Admins)

Permissions for Domain Admins	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.

(Security settings for Domain Users)



Advanced Security Settings for Domain Users

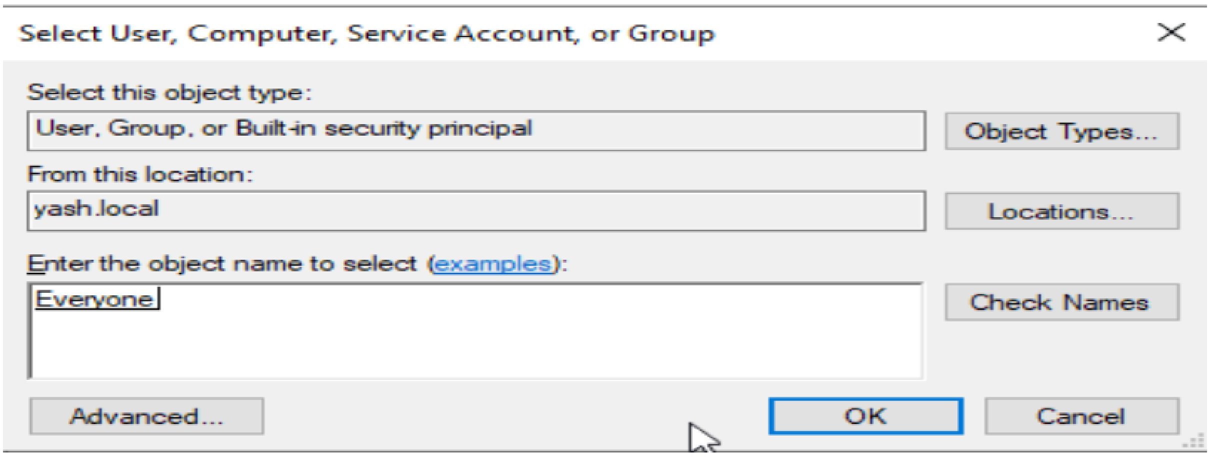
Owner: Domain Admins (YASH\Domain Admins) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone		DC=yash,DC=local	Descendant Organizational Un...
Succ...	Everyone		DC=yash,DC=local	Descendant Organizational Un...

(Select principal name)



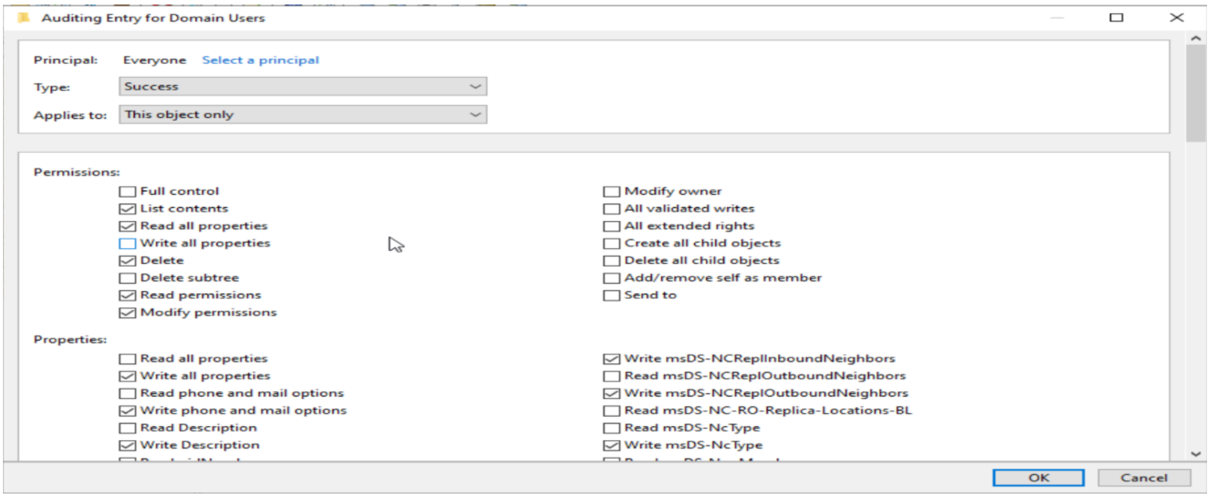
Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
yash.local

Enter the object name to select (examples):
Everyone

(Gave type:Success)



Auditing Entry for Domain Users

Principal: Everyone Select a principal

Type: Success

Applies to: This object only

Permissions:

□ Full control
☑ List contents
☑ Read all properties
□ Write all properties
☑ Delete
□ Delete subtree
☑ Read permissions
☑ Modify permissions

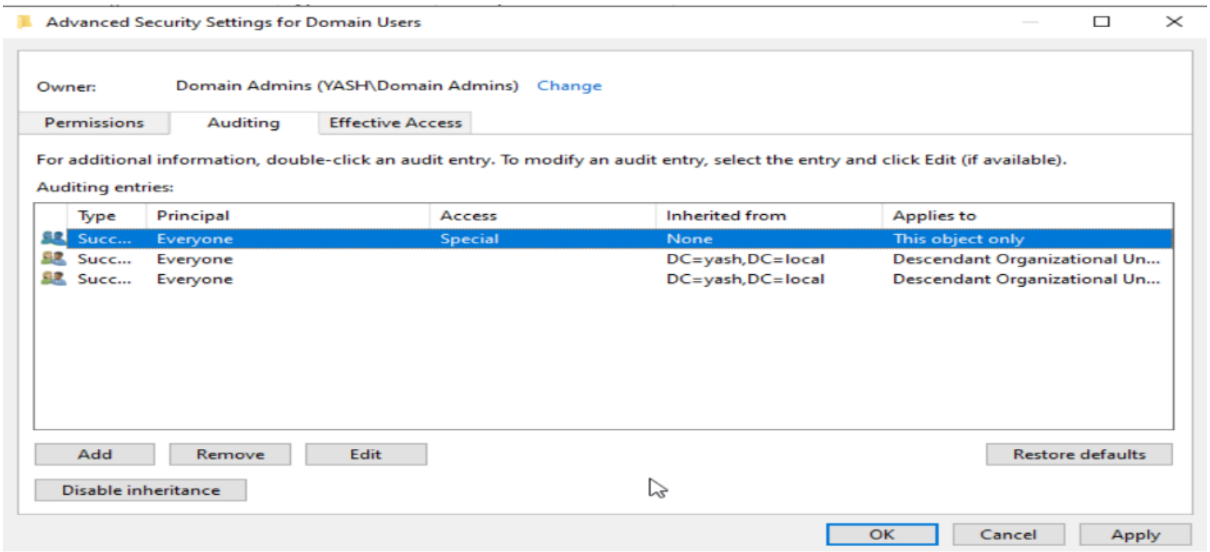
□ Modify owner
□ All validated writes
□ All extended rights
□ Create all child objects
□ Delete all child objects
□ Add/remove self as member
□ Send to

Properties:

□ Read all properties
☑ Write all properties
□ Read phone and mail options
☑ Write phone and mail options
□ Read Description
☑ Write Description

☑ Write msDS-NCReplInboundNeighbors
□ Read msDS-NCReplOutboundNeighbors
☑ Write msDS-NCReplOutboundNeighbors
□ Read msDS-NC-RO-Replica-Locations-BL
□ Read msDS-NcType
☑ Write msDS-NcType

(Modification made to the Domain Admins group.)



Owner: Domain Admins (YASH\Domain Admins) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone	Special	None	This object only
Succ...	Everyone		DC=yash,DC=local	Descendant Organizational Un...
Succ...	Everyone		DC=yash,DC=local	Descendant Organizational Un...

3.2 Monitor Event Logs for Unauthorized AD Changes

This phase focuses on actively monitoring changes within Active Directory, particularly privileged group membership and directory object modifications. You've already enabled two specific advanced auditing subcategories—Audit Security Group Management and Audit Directory Service Changes—under the Default Domain Policy. These settings are crucial, as they trigger the generation of detailed logs (Event IDs 4732 and 5136) for actions like adding a user to a group or modifying AD objects. This phase now involves validating the policy, simulating realistic changes, and analyzing the resulting security logs to ensure everything is functioning as expected.

- **Enable Fine-Grained Audit Policies via GPMC**

  Begin by opening the Group Policy Management Console (GPMC) and editing the Default Domain Policy.

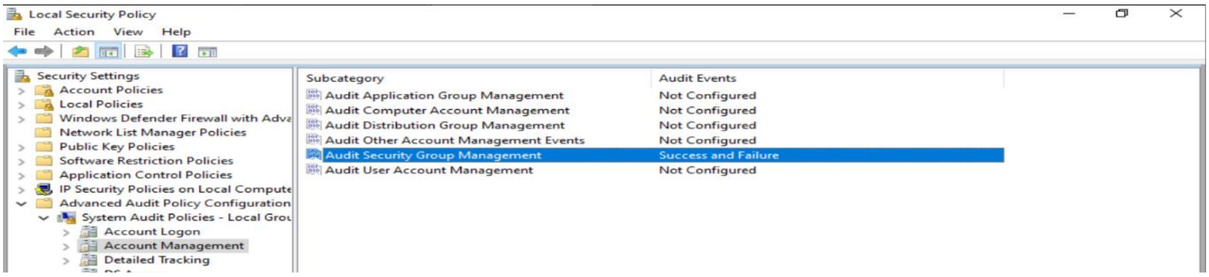
  Navigate to:

  Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies

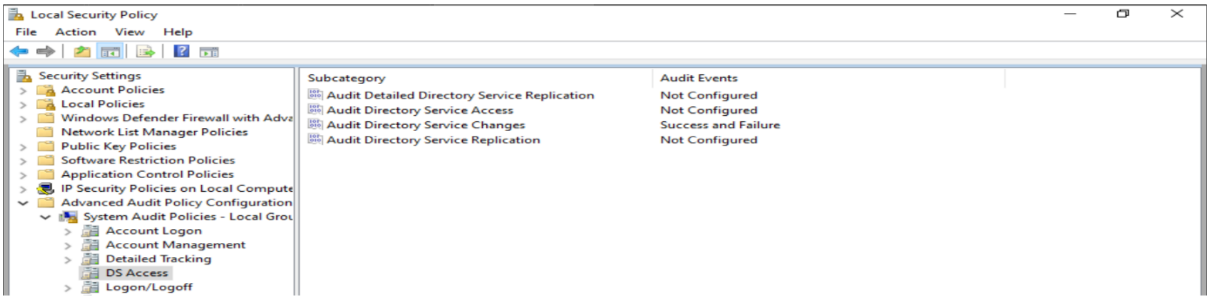
Under this, enable:

Audit Security Group Management → Success and Failure

Audit Directory Service Changes → Success and Failure


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon
Account Management
Detailed Tracking

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Not Configured
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Success and Failure
Audit User Account Management	Not Configured


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
System Audit Policies - Local Grou
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff

Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Not Configured

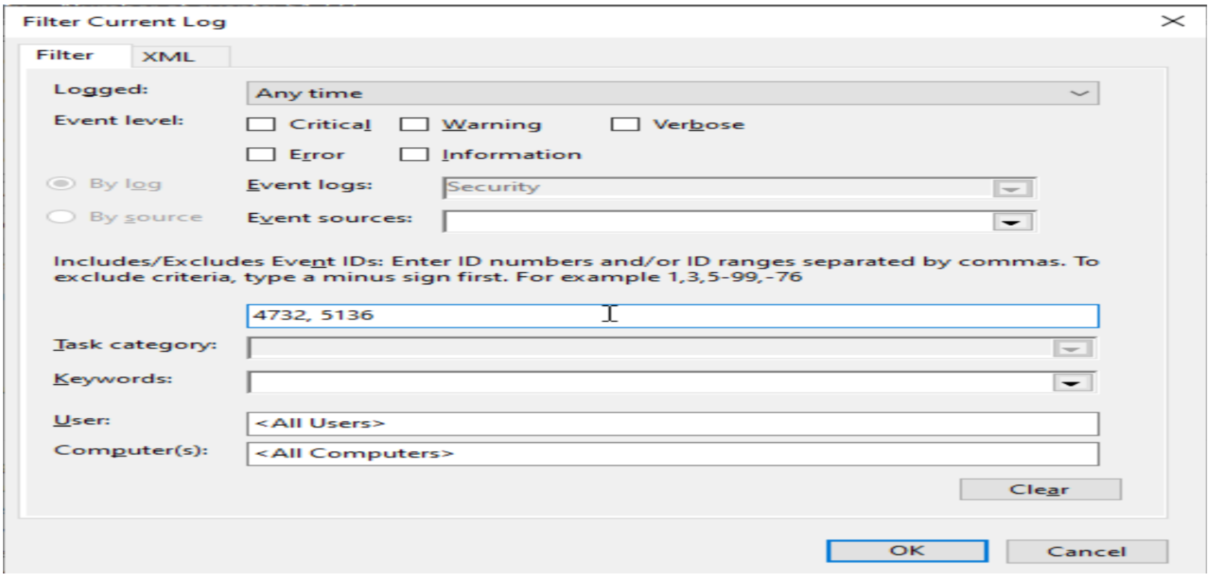
- **View Security Logs for Events**

  Once you have performed some test actions, it's time to check the logs to see if the changes were captured. Open **Event Viewer** and navigate to the **Security Logs**. Use the filter to search for specific event IDs such as **4732** and **5136**, which represent key actions related to group membership changes and directory object modifications. Reviewing these logs allows you to identify unauthorized or suspicious activities that might indicate privilege escalation, insider threats, or external attacks on your AD infrastructure.

  Now open **Event Viewer** on the domain controller and navigate to: Windows Logs > Security

  Use the “Filter Current Log” option to search for **Event ID 4732** and **5136**.

(Filter the logs.)



Logged: Any time

Event level: □ Critical □ Warning □ Verbose □ Error □ Information

● By log Event logs: Security

○ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4732, 5136

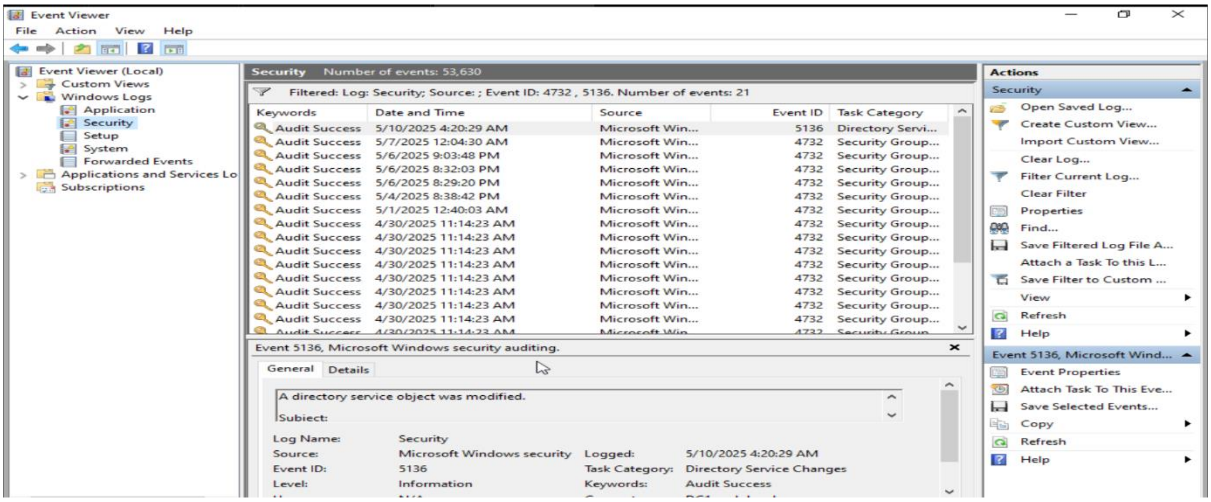
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

(Logs of event id-4732, 5136.)



Security Number of events: 53,630

Filtered: Log: Security; Source: ; Event ID: 4732 , 5136. Number of events: 21

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/10/2025 4:20:29 AM	Microsoft Win...	5136	Directory Servi...
Audit Success	5/7/2025 12:04:30 AM	Microsoft Win...	4732	Security Group...
Audit Success	5/6/2025 9:03:48 PM	Microsoft Win...	4732	Security Group...
Audit Success	5/6/2025 8:32:03 PM	Microsoft Win...	4732	Security Group...
Audit Success	5/6/2025 8:29:20 PM	Microsoft Win...	4732	Security Group...
Audit Success	5/4/2025 8:38:42 PM	Microsoft Win...	4732	Security Group...
Audit Success	5/1/2025 12:40:03 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...
Audit Success	4/30/2025 11:14:23 AM	Microsoft Win...	4732	Security Group...

Event 5136, Microsoft Windows security auditing.

A directory service object was modified.

Subject:

Log Name: Security
Source: Microsoft Windows security Logged: 5/10/2025 4:20:29 AM
Event ID: 5136 Task Category: Directory Service Changes
Level: Information Keywords: Audit Success

3.3 Set Up Custom Audit Policy for Sensitive File Access

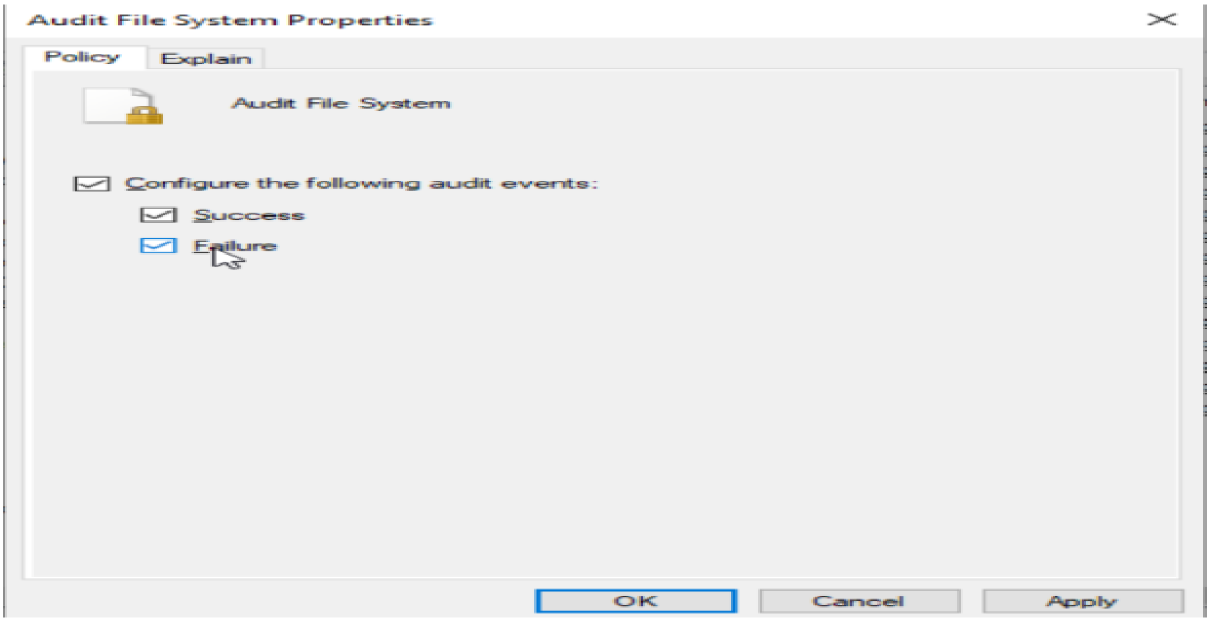
The goal of this phase is to monitor access to sensitive files or folders on a system, such as configuration files, logs, backups, or confidential data repositories. This is critical for detecting unauthorized access, insider threats, or even accidental modifications. The process involves two major components: first, enabling **Object Access auditing** through Group Policy (to instruct the system to generate logs for file system access), and second, applying **SACLs (audit rules)** on specific folders to track access attempts. Once in place, these settings will generate detailed logs (such as **Event ID 4663**) every time the folder is accessed, modified, or deleted.

- **Enable “Audit Object Access” in Group Policy**

  To begin, open the **Group Policy Management Console (GPMC)** and edit a policy applied to the relevant machine (e.g., Default Domain Policy or a custom GPO). Navigate to: Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy

  Locate the setting **Audit object access**, and **check both "Success" and "Failure"**. This enables the operating system to begin tracking and logging all attempts (successful or failed) to access objects like files, folders, and printers.

  (Check both the boxes.)



☑ Configure the following audit events:

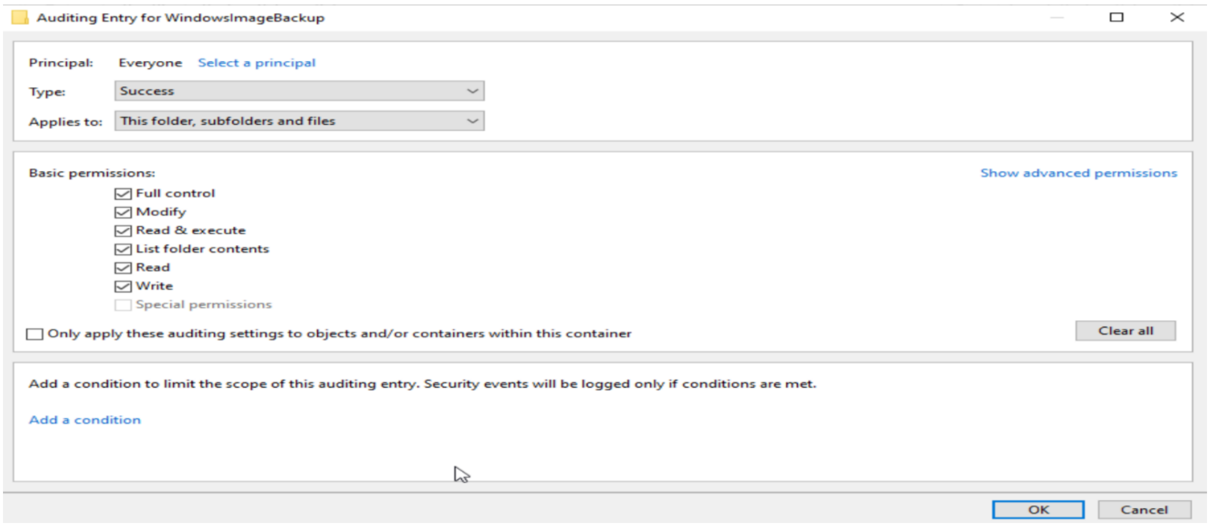
☑ Success

☑ Failure

- **Apply SACL (Auditing Entry) on Sensitive Folder**

  Next, select a specific folder you want to monitor. Right-click the folder, choose **Properties**, then go to the **Security** tab and click **Advanced**. From there, navigate to the **Auditing** tab and click **Add**. Select a principal and then specify the access types you want to audit. Also, choose whether to audit for success, failure, or both.

(Gave type:Success)



Auditing Entry for WindowsImageBackup

Principal: Everyone Select a principal

Type: Success

Applies to: This folder, subfolders and files

Basic permissions:

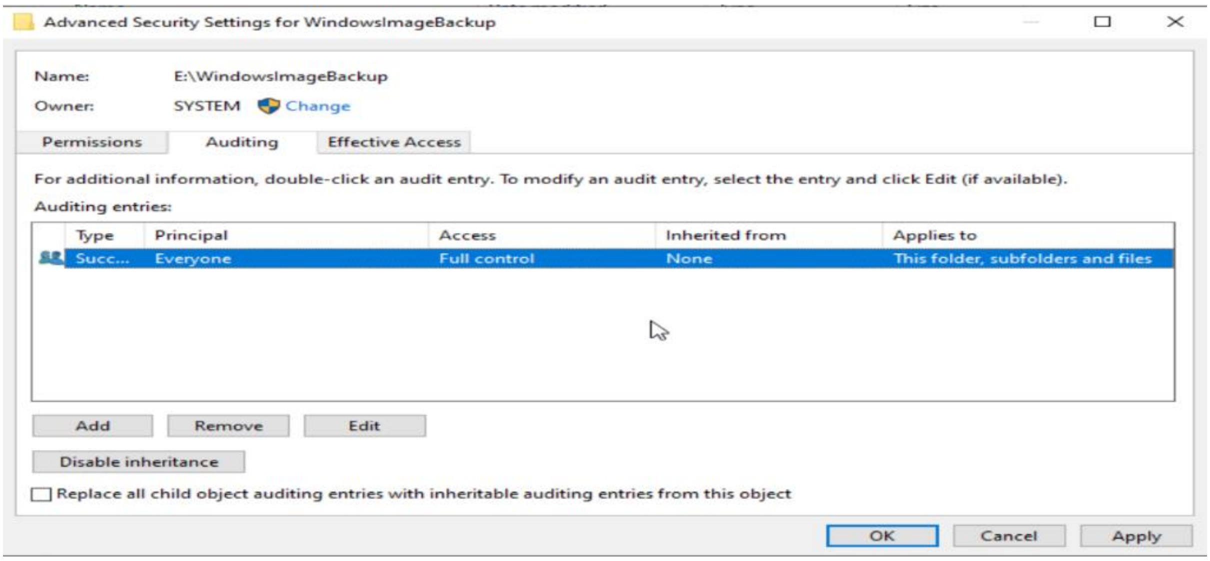
☑ Full control
☑ Modify
☑ Read & execute
☑ List folder contents
☑ Read
☑ Write
□ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Add a condition

(Modification made to Auditing tab.)



Advanced Security Settings for WindowsImageBackup

Name: E:\WindowsImageBackup

Owner: SYSTEM Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone	Full control	None	This folder, subfolders and files

□ Replace all child object auditing entries with inheritable auditing entries from this object

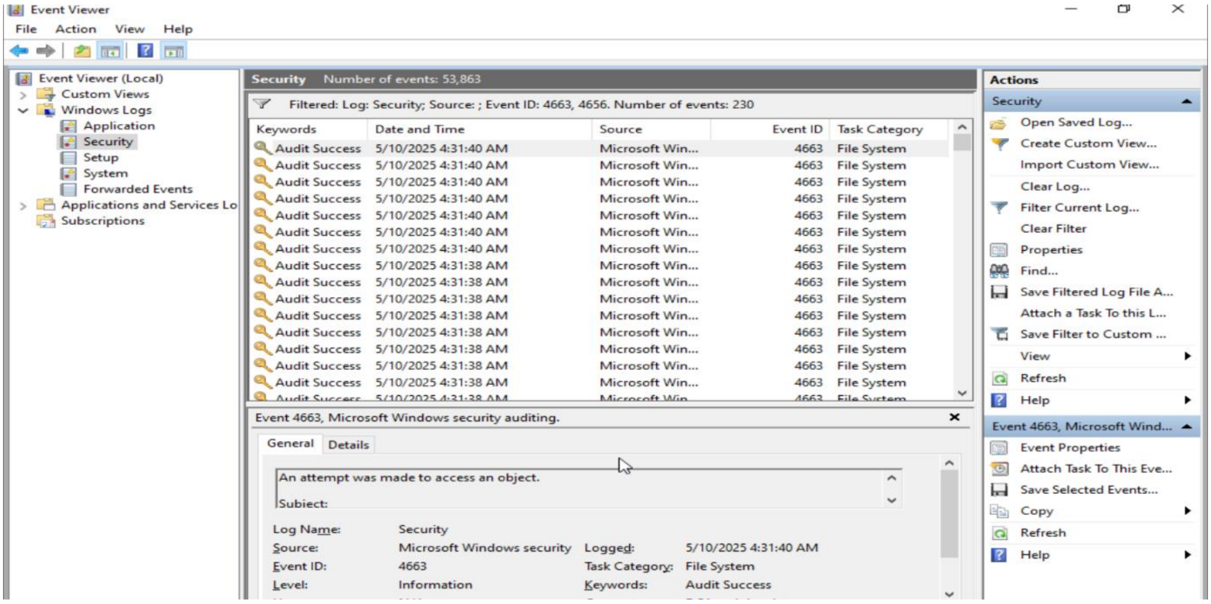
- **Simulate File Access to Generate Audit Events**

  After setting up the SACL, the next step is to validate the configuration by simulating an access attempt. Open, modify, or delete a file inside the monitored folder. These actions will now trigger auditing mechanisms and generate security log entries. This simulation serves as a controlled way to confirm that the auditing policies are not just configured—but actually functional.

- **Review Security Logs for File Access Events**

  After simulating access, check **Event Viewer** to ensure that the events are being logged correctly. Look for **Event ID 4663** (file access) and **Event ID 4656** (access request) under **Security Logs**. These events will show who accessed the file, what actions they performed, and whether the access was successful or failed. This step helps you verify that your auditing settings are working as intended and that any unauthorized access to sensitive files will be captured.

(Logs events of id-4663, 4656.)



Security Number of events: 53,863

Filtered: Log: Security; Source: ; Event ID: 4663, 4656. Number of events: 230

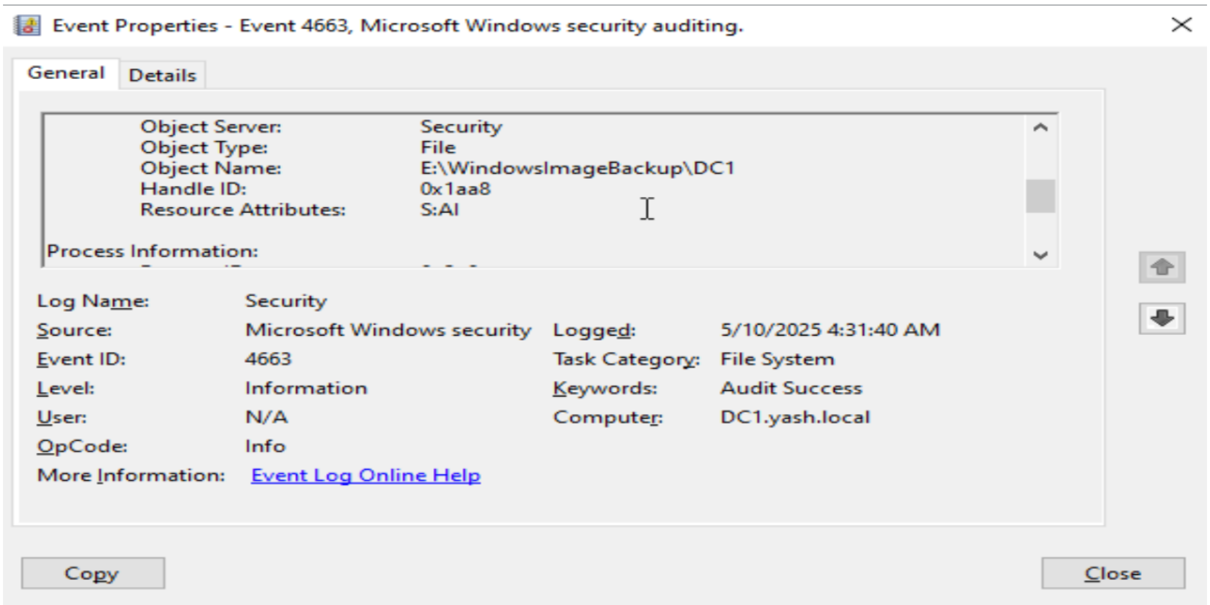
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:40 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System
Audit Success	5/10/2025 4:31:38 AM	Microsoft Win...	4663	File System

Event 4663, Microsoft Windows security auditing.

An attempt was made to access an object.

Subject:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/10/2025 4:31:40 AM
Event ID:	4663	Task Category:	File System
Level:	Information	Keywords:	Audit Success



Event Properties - Event 4663, Microsoft Windows security auditing.

Object Server: Security
Object Type: File
Object Name: E:\WindowsImageBackup\DC1
Handle ID: 0x1aa8
Resource Attributes: S:AI

Process Information:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	5/10/2025 4:31:40 AM
Event ID:	4663	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.yash.local
OpCode:	Info		
More Information:	Event Log Online Help		

4. Results and findings

After implementing advanced auditing and monitoring across Active Directory and sensitive file systems, several key observations and patterns were identified. These findings validate that auditing mechanisms are operational and capable of detecting unauthorized or anomalous activities. The events generated during simulation helped verify that critical changes—such as group membership alterations and sensitive file accesses—are being logged as intended.

- **Event Logs Successfully Captured Group Membership Changes:**
  Simulated addition of a user to the *Domain Admins* group triggered **Event ID 4732**, confirming that the "Audit Security Group Management" policy is correctly logging privileged group changes.

- **Object Modification Logs Were Generated Accurately:**
  Modifying an AD object (e.g., user description) triggered **Event ID 5136**, verifying that "Audit Directory Service Changes" is functioning correctly and tracking schema modifications.

- **SACLs on Domain Admins Group Captured Access Events:**
  Custom auditing set on the Domain Admins group resulted in **Event ID 4662** entries, confirming that access to high-privilege AD objects is being monitored effectively.

- **Sensitive Folder Access Tracked via Event ID 4663:**
  Accessing files in the audited directory generated **Event ID 4663**, including details such as username, object path, and type of access (read/write/delete).

- **No False Positives or Log Overhead Observed:**
  The auditing configuration was optimized, capturing critical actions without flooding logs with irrelevant data—ensuring efficiency and clarity in log review.

5. Recommendations

Based on the findings from this task, several improvements and best practices can be recommended to further enhance security posture, streamline monitoring, and minimize operational risk in Active Directory environments.

- **Integrate SIEM for Centralized and Real-Time Monitoring:**
  Forward AD and file access event logs to a SIEM to enable real-time alerts, correlation with other security events, and long-term storage.

- **Configure Custom Alerts for High-Value Events:**
  Set up alerts for events like **4732** and **5136**, especially when involving sensitive groups or schema changes, to detect potential insider threats or privilege escalation.

- **Limit Audit Scope to Critical Assets:**
  To reduce noise and improve performance, apply auditing only to sensitive folders and high-value AD objects rather than broad categories.

- **Document and Regularly Review Audit Policies:**
  Maintain documentation of applied audit settings and review them quarterly to align with changes in organizational structure, compliance, or risk profile.

- **Train Admins on Interpreting Security Logs:**
  Ensure IT staff and security analysts are trained to interpret audit logs effectively, including understanding key event IDs and correlating them with real-world attack scenarios.

6. Conclusions

The successful deployment of advanced auditing and monitoring mechanisms in the Active Directory environment has demonstrated a significant improvement in security visibility and operational control. Through careful planning and phased execution, we enabled granular audit policies and applied SACLs on critical AD objects and sensitive file locations. These configurations allowed for the accurate logging of vital events such as user additions to privileged groups (Event ID 4732), directory object modifications (Event ID 5136), and file access attempts (Event ID 4663), ensuring that all critical changes and interactions within the domain are now traceable and accountable.

The auditing process was tested using controlled simulations that mimicked potential attack vectors, such as unauthorized privilege escalation and access to confidential files. These simulations confirmed that the system was capable of generating appropriate alerts and logs, providing immediate insight into potentially malicious activities. Importantly, the auditing was configured in a way that balanced thoroughness with efficiency, avoiding log overflow or unnecessary noise, which can often hinder incident detection and analysis.

Moreover, this implementation forms the foundation for more advanced security operations such as SIEM integration, real-time alerting, and incident response workflows. By monitoring specific high-risk events and object access patterns, administrators are now equipped with the tools to detect threats early, investigate anomalies swiftly, and meet regulatory compliance requirements with documented audit trails.

In summary, this project not only improved monitoring capabilities but also enforced a culture of accountability and transparency within the IT infrastructure. It represents a strategic move toward proactive defense, where potential threats can be identified and mitigated before they escalate into serious incidents. The methodology and controls applied here can now serve as a baseline for broader security initiatives across the organization.