netwrix

How to Audit the 5 Most Important Active Directory Changes

www.netwrix.com | Toll-free: 888.638.9749

Table of Contents

Introduction

Active Directory is the central identity store and authentication provider for most networks today making it hugely critical to security. In this white paper I'll discuss the 5 most important changes affecting the security of Active Directory, show you how to audit these events using native auditing and point out the limitations and gaps you should be aware before depending on these events.

Since domain controllers generate the events covered in this white paper, you need to enable audit policies on the Default Domain Controller Security Policy GPO.

#1 – Group Membership Changes

Active Directory groups control access to resources throughout your domain. This includes not just permissions on file servers but also in SharePoint, Exchange, SQL Server and other applications that integrate with AD – including cloud applications. Therefore you need an audit trail of group membership changes and you need to review changes to important groups like AD's built-in privileged groups and other custom groups you identify as having significant access to resources and applications within your environment.

To audit group membership changes you need to enable the "Audit Security Group Management" audit policy and then look for events 4728, 4732 and 4756 which cover new members added to global, local and universal groups. These events indicate who made the change, which group was affected and who the new member is.

You should also monitor changes to a group's scope (Global, Local or Universal) or type (Security/Distribution/Application). Scope changes can suddenly allow a group to be granted access in other trusting domains or have members from other trusted domains. A rogue privileged user, counting on you only monitoring security group changes, could change a Security group to a Distribution group, add an unauthorized member and change it back to a Security group. To catch all scope and type changes on groups review occurrences of event ID 4764.

#2 – Group Policy Changes

Group Policy objects control domain level security settings as well as security configuration of member servers and workstations throughout your domain. So to be secure and compliant you need to be aware of any changes affecting Group Policy and that includes more than just changes to Group Policy objects themselves. Organizational Units (as well as Sites and the root of the domain) have Group Policy related attributes that can impact the application of Group Policy on the users and computers within that OU.

To audit these events you need to enable the "Audit directory service changes" and "Audit directory service access" policies. Then you must configure object level auditing with Active Directory Users and Computers.

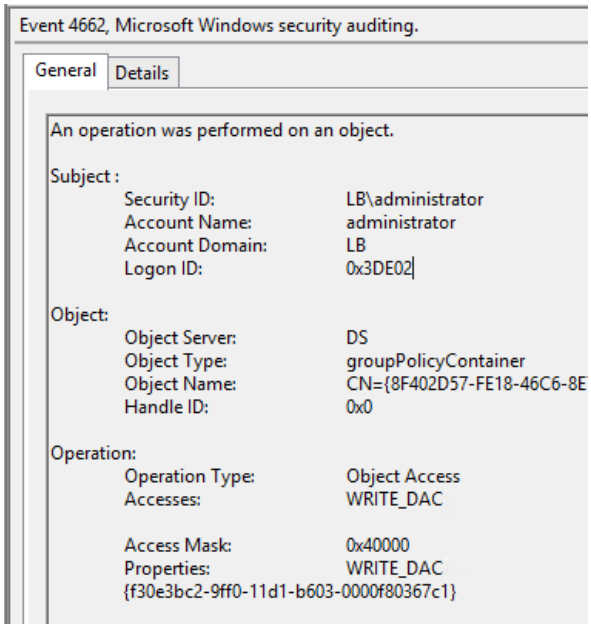
Here's what you should enable at the root of the domain:

Who	Object type	Object Permissions	Property Permissions	Success/Failure
Everyone	Descendant **organizationalUnit** objects	Modify Permissions		Success
Everyone			Write gpOptions	Success
Everyone			Write gpLink	Success
Everyone	Descendant **groupPolicyContainer** objects	Write All Properties		Success
Everyone		Modify Permissions		Success
Everyone	This object only	Modify Permissions		Success
Everyone			Write gpOptions	Success
Everyone			Write gpLink	Success

Note that these audit specs also include the necessary object level auditing for AD permission changes, which we'll discuss below.

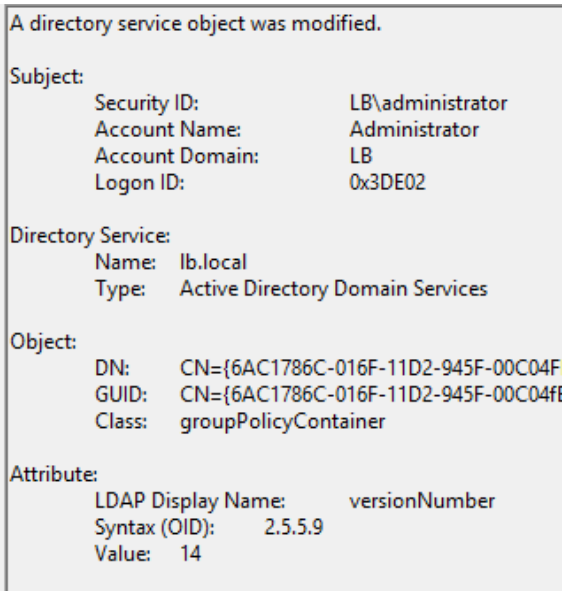
Now that you've enabled system and object level auditing let's talk about auditing three aspects of GPO management: modifying permissions to the GPO, modifying GPO settings and deleting a GPO.

The permissions on a GPO control who can edit the GPO and can be used for security filtering to limit the application of the GPO to a subset of users or computers. To find permission changes to GPOs look for event ID 4662, as shown below, where the Object Type is groupPolicyContainer (AD schema name for GPO) and the Properties include WRITE_DAC which means "Modify Permissions".



As you can see from this event, Windows does not provide the display name of the GPO – only it's GUID. This is an example of the limitations with native auditing. To figure out the Display Name of the GPO you'll need to go to Active Directory Users and Computers and add Display Name as a column. Then select the System\Policies folder and you'll see a list of all the GPOs in the domain with their GUID and Display Name which you can then cross reference. In addition to the GUID/Display Name issue, the standard event 4662 only tells you that the GPOs permissions where change and who changed them - It fails to tell you what permission were changed. In the example event above, Everyone was granted the authority to edit the GPO which could be very dangerous.

Auditing changes to GPO settings is equally as unhelpful. Setting changes are logged in event 5136 with Class as "groupPolicyContainer" and Attribute LDAP Display Name as "versionNumber".



While this event tells you that a specified user (noted in the "Subject" section of the event detail) modified a GPO, it does not tell you which setting(s) within that GPO where modified much less their before and after values. And again you must translate the GUID in the event to the Display Name of the GPO to really understand which GPO was affected.

Finally, you should also monitor for deletions of GPOs since that could wipe out entire collection of critical security settings. Look for event ID 5141, again with the Class as "groupPolicyContainer".

#3 – AD Permission Changes

With the object level audit policy specified in the figure above, AD will also log permission changes to any object within the domain. Such permission changes are very important to review because they indicate that some level of access to AD objects was delegated. Permission changes in AD can be just as powerful as making someone a member of the Domain Admins group. For instance, if someone grants the Everyone group Full Control to the root of the domain – you would want to know. Permission changes to OUs or domain roots are logged just like GPO permission changes described above but the Object Type will be either "organizationalUnit" or "domainDNS". You need to investigate these permission changes to make sure privileged authority over AD has not been weakened. However we encounter the same limitation with native auditing affecting GPO permission changes. AD tells us Bob changed the permission on the organizational unit but not what the new permissions are. You will have to look at the security settings of the object in AD and assess whether the current permissions are appropriate.

4 – New and Enabled User Accounts

New user accounts represent a new set of credential with access to your environment. It pays to review these additions to AD so that you can promptly respond to inappropriate accounts, accounts created outside normal controls or event backdoor accounts created by APTs and other attackers. Similarly, accounts that were previously disabled but suddenly enabled require review as well, since they should be fairly uncommon and represent the same risk as newly created accounts.

To track these and other changes to AD user accounts enable the "Audit user account management" audit policy. Then look for event ID 4720 (user account creation) and 4722 (user account enabled). These events are pretty straightforward but be aware of a false positive situation: when you initially create a user account, AD creates the account as disabled, makes several initial updates to it and then immediately enables it. Therefore you will always see a somewhat bogus occurrence of 4722 associated with each new account created and need to ignore these.

5 – Trust Relationship Changes

Trust relationship changes are infrequent but have massive security ramifications. When you trust another domain or forest your computers now accept the identity of all of those users. And if you resources where permission are granted to Everyone or Authenticated Users, the users of the newly trusted domain now instantly inherit those permissions.

To audit trust relationships enable the "Audit authentication policy changes" audit policy and then look for event IDs 4706, 4707, 4716, 4865, 4866 and 4867. Together these events cover all changes to trust relationships. Be aware that Windows logs duplicates of some events and does not always use the terms "trusted" and "trusting" correctly. Again these events should be a trigger for you to investigate the new status of trust relationships in Active Directory Domains and Trusts.

Getting Handle on Your AD Changes

While not an exhaustive list of everything you should audit in Active Directory, it is a good start. You will need to watch the security log of each domain controller in your environment because security events are not replicated between domain controllers. Events are simply logged on the domain controller that happened to service the client request. As you can see native auditing alerts you to important changes but frequently leaves out crucial details that you must investigate for yourself. I encourage you to compare native auditing with the capabilities of Netwrix Auditor for Active Directory which provides detailed insight into exactly who made what change, when and where in Active Directory. Once a change has been identified, Netwrix Auditor for Active Directory alerts IT administrators in real-time and gives the ability to roll-back unwanted changes and restore deleted objects with just a few clicks. The 'state-in-time auditing' feature provides a complete visibility of how your Active Directory was configured in the past (days/moths/years ago). Other features of Netwrix Auditor for Active Directory include long-term storage of audit data, password expiration alerting, inactive user tracking, Windows Server auditing, event log management and user activity video recording. If you just need a simple tool that keeps you notified on changes to Active Directory, I suggest you try Netwrix Change Notifier for Active Directory. It's a 100% free tool that provides basic monitoring and reporting capabilities on Active Directory changes.

About Randy Franklin Smith

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and Active Directory security who specializes in Windows and Active Directory security. He performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations.

Certifications:

- Certified Information Systems Auditor (CISA)
- Microsoft Security Most Valuable Professional (MVP)
- Systems Security Certified Professional (SSCP)

Industry Memberships:

- Information Systems Security Association (ISSA)
- Information Systems Audit and Control Association (ISACA)
- Center for Internet Security (CIS)

About Netwrix Corporation

Netwrix Corporation provides a market-leading visibility and governance platform for on-premises, hybrid and cloud IT environments. More than 150,000 IT departments worldwide rely on Netwrix to detect insider threats on premises and in the cloud, pass compliance audits with less expense and increase productivity of IT security and operations teams. Founded in 2006, Netwrix has earned more than 90 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more information, visit www.netwrix.com

Netwrix Corporation, 300 Spectrum Center Drive, Suite 1100, Irvine, CA 92618, US

netwrix.com/social

Toll-free: 888-638-9749 Int'l: +1 (949) 407-5125 EMEA: +44 (0) 203-318-0261