Windows: Log and Alert When Accounts are Created

With a focus on admin account creation

Type of Systems: Windows AD Domain Controller
Necessary Skills: Use of the Group Policy and Event Viewer tools, and a centralized logging forwarder (Splunk or Syslog).

Complete Goal: To log when new user accounts are created and send those logs to the centralized logging server.

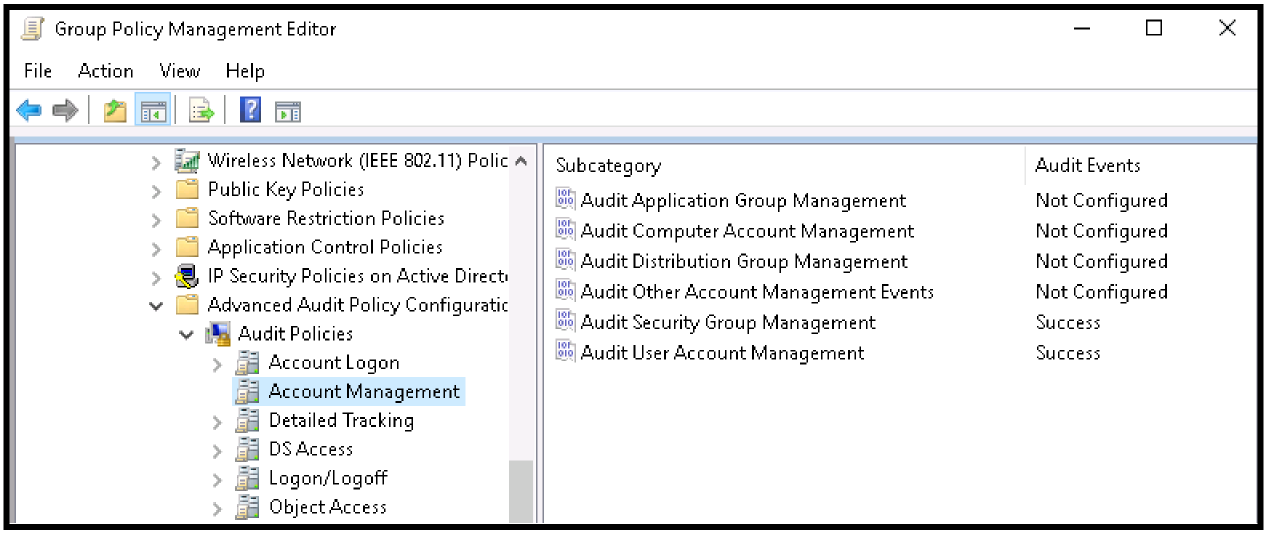
Steps:

1. Log in to the AD domain controller as the domain admin.
2. Open the Group Policy Management Console (CMD: `gmpc`).
3. In the directory pane on the left, navigate: *Forest: (domainName) > Domains > (domainName)*
   When *(domainName)* is the AD domain name.
4. Right click on “Default Domain Policy” and select “Edit.”
5. Navigate to *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options*
6. Open “Audit: Force audit policy subcategory settings” and enable it.
7. Navigate to *Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management*
8. Open “Audit User Account Management,” and enable “Success.” This logs account creation.
9. Open “Audit Security Group Management,” and enable “Success.” This logs when a user account is added to a group.
10. After changing the group policy, you must refresh the policy on the domain. Use CMD: `gpupdate /force`
11. If you want to check for account events, open event viewer (CMD: `eventvwr`). Navigate to *Windows Logs > Security*. If you see events with IDs 4720 (account created), 4724 (account’s password was changed), or 4738 (account was changed), this means that we are logging account creation. If you see events with IDs 4732 (A user was added to a group), or 4735 (A group was changed), this means we are logging group management.
12. To add account creation events to the centralized logging server, you need to add the security log to your forwarder. The log is located at: *C:\Windows\System32\winevt\Logs\Security.evtx*

Relevant Info:

- When a group of computers are part of an AD domain, users work differently from non-AD users. Specifically, when you create an AD user, by default they only have basic user privileges. When you add them to a group, you give them additional privileges. Therefore, an admin user cannot be created in a single step. An account is created, then it is added to one or all of the admin groups. When looking at the logs, if you see ID 4720 **followed by** 4732, that means an admin account has been created.

Appendix:


Group Policy Management Editor
File
Action
View
Help
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directo
Advanced Audit Policy Configuratic
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access

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
Audit User Account Management	Success

Step 9: Your Group Policy window should look like this after you set the two account management policies.