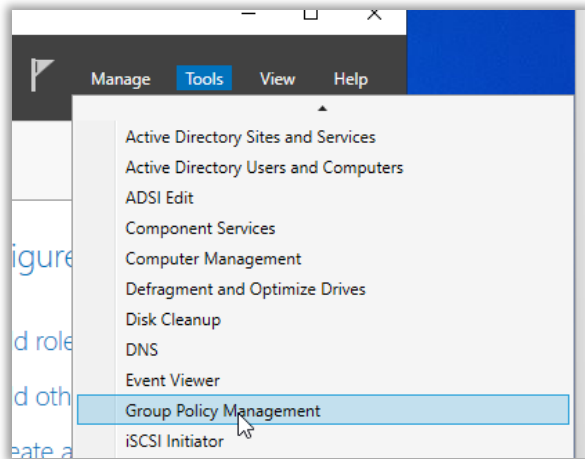


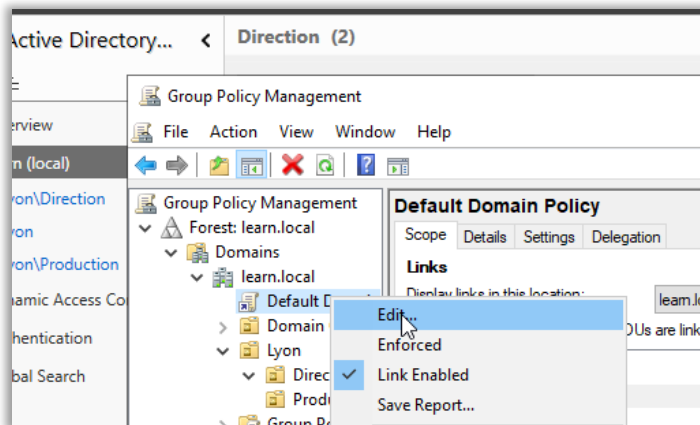
# Créer un audit pour tracer un administrateur

Dans cet exemple, on trace la gestion des comptes utilisateurs.

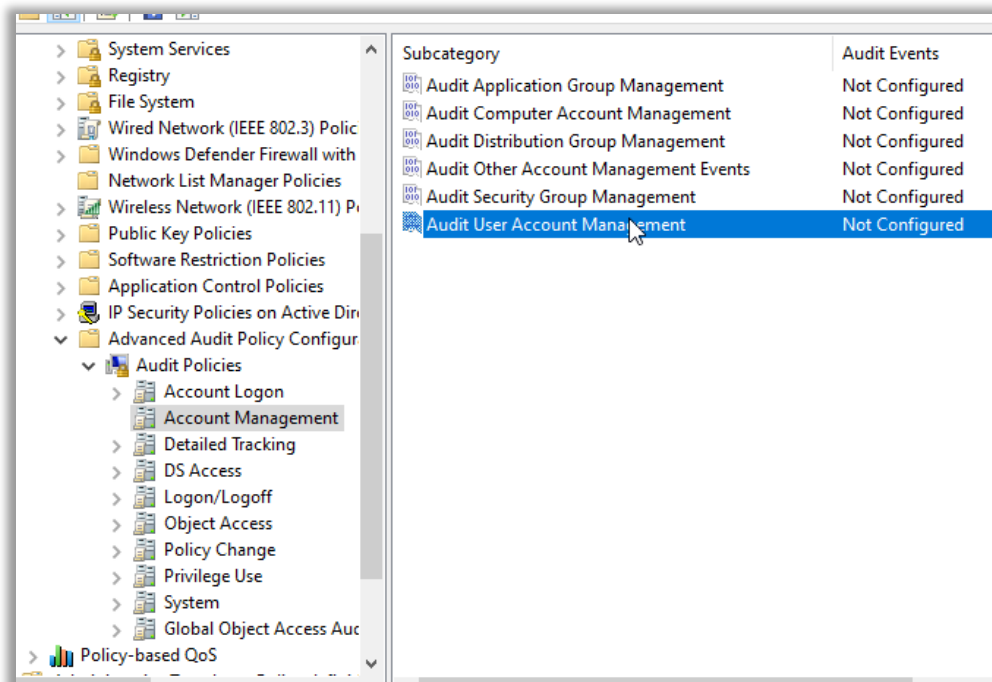
Sur le Windows Server sous *Tools*, cliquer sur *GPO*.



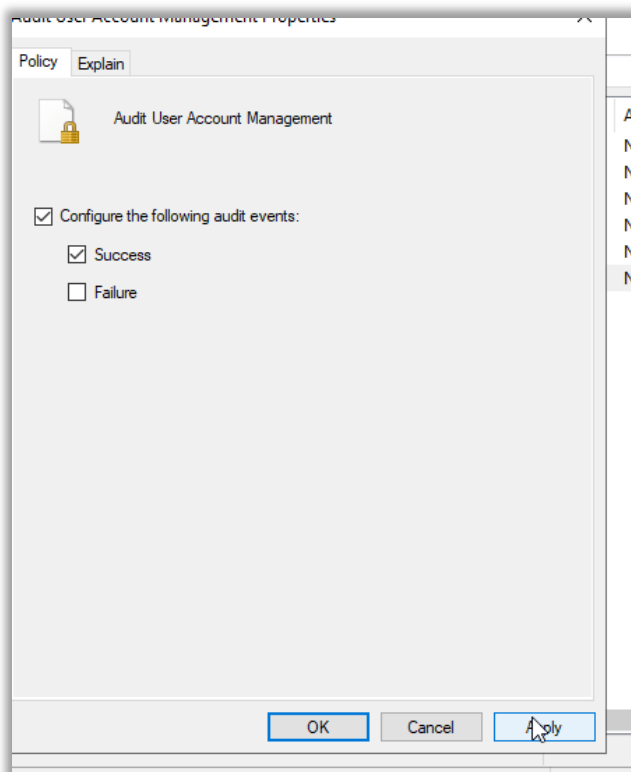
Clique-droite sur *Default Domain Policy* et choisir *Éditer*. Cela est le GPO qui s'applique partout dans le forêt en pas que sur un UO.



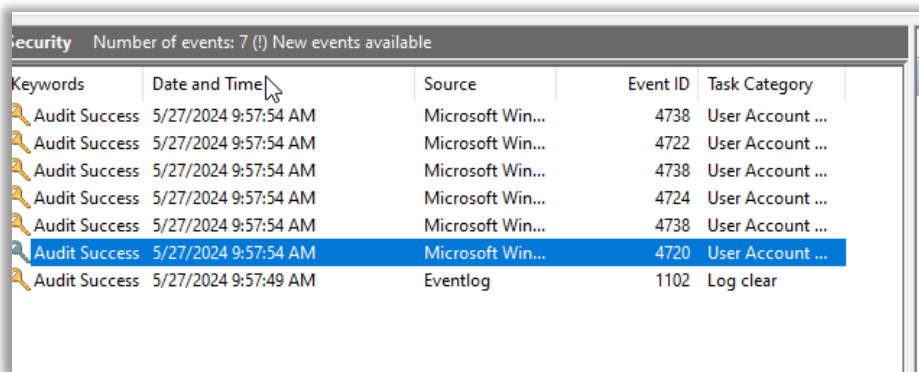
Sous *Computer Management/Policies/Windows Settings/Advanced Audit Policy Configuration/Account Management*, double clique sur *Audit User Account Management*.



Crocher l'option et *Succès*, puis *Appliquer*.

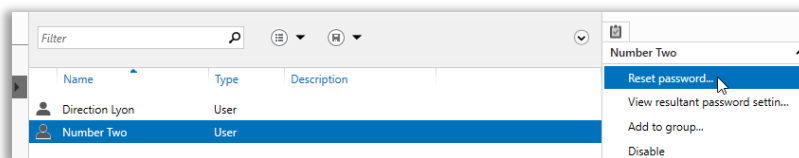


Créer un nouvel utilisateur et regarder dans le log.



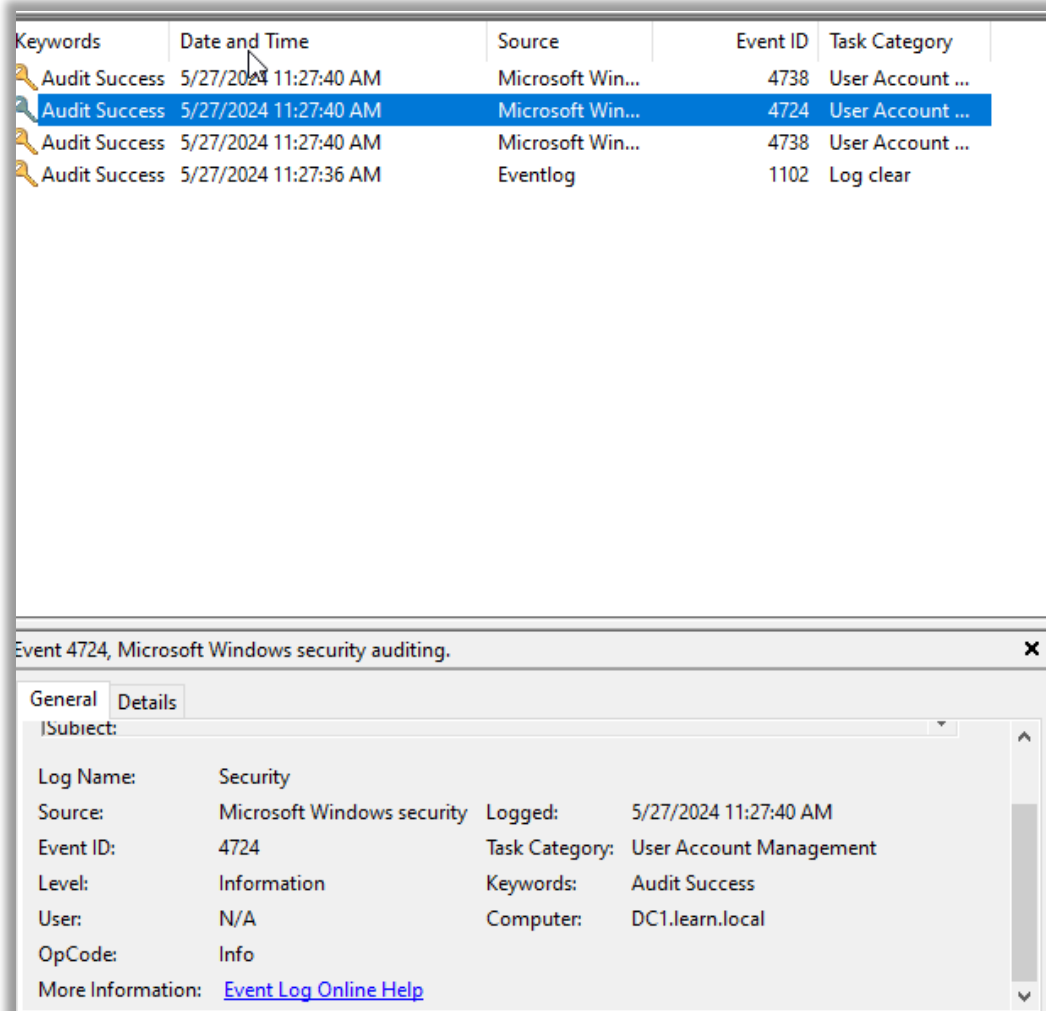
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/27/2024 9:57:54 AM	Microsoft Win...	4738	User Account ...
Audit Success	5/27/2024 9:57:54 AM	Microsoft Win...	4722	User Account ...
Audit Success	5/27/2024 9:57:54 AM	Microsoft Win...	4738	User Account ...
Audit Success	5/27/2024 9:57:54 AM	Microsoft Win...	4724	User Account ...
Audit Success	5/27/2024 9:57:54 AM	Microsoft Win...	4738	User Account ...
Audit Success	5/27/2024 9:57:54 AM	Microsoft Win...	4720	User Account ...
Audit Success	5/27/2024 9:57:49 AM	Eventlog	1102	Log clear

Cet événement est pour créer un utilisateur. Si on réinitialise le mot de passe on a alors :



Name	Type	Description
Direction Lyon	User	
Number Two	User	

- Reset password...
- View resultant password settin...
- Add to group...
- Disable



Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/27/2024 11:27:40 AM	Microsoft Win...	4738	User Account ...
Audit Success	5/27/2024 11:27:40 AM	Microsoft Win...	4724	User Account ...
Audit Success	5/27/2024 11:27:40 AM	Microsoft Win...	4738	User Account ...
Audit Success	5/27/2024 11:27:36 AM	Eventlog	1102	Log clear

Event 4724, Microsoft Windows security auditing.

General		Details	
Subject:			
Log Name:	Security	Logged:	5/27/2024 11:27:40 AM
Source:	Microsoft Windows security	Task Category:	User Account Management
Event ID:	4724	Keywords:	Audit Success
Level:	Information	Computer:	DC1.learn.local
User:	N/A		
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		