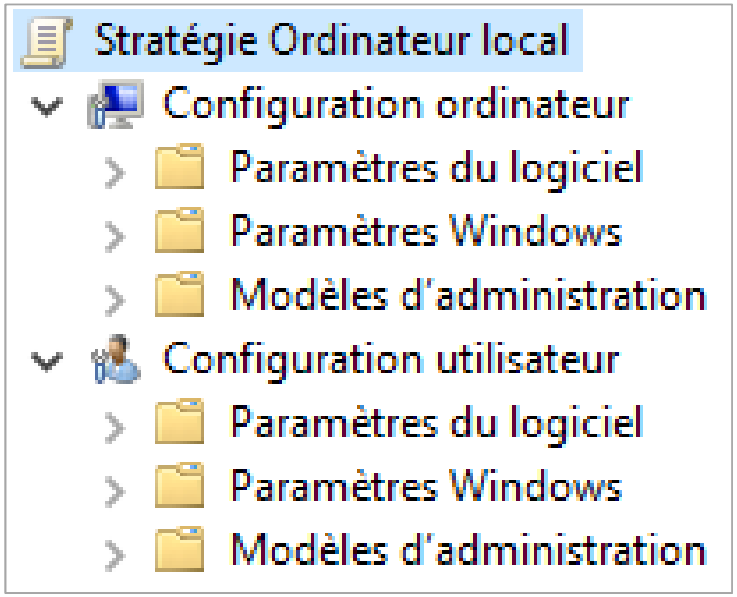
L’audit des GPO

Aurélien Bordes

SSTIC – 5 juin 2019

Rappels et contexte

- Les GPO (*Group Policy Object*) :
  - Sont apparues avec Windows 2000 et l'Active Directory
  - Permet d'appliquer des paramètres de configuration
  - Sont composées de deux parties :
    - Ordinateur
    - Utilisateur

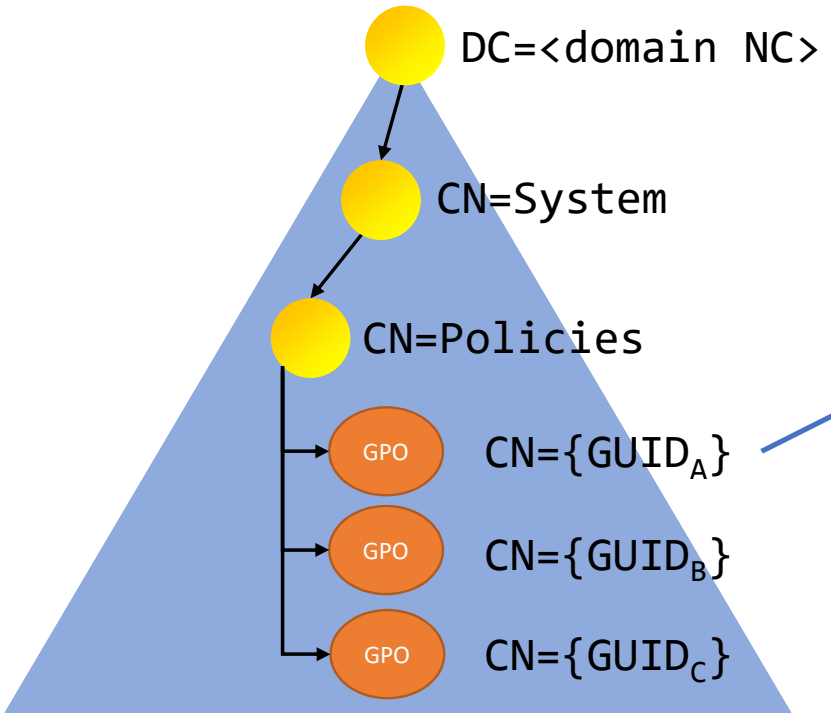


Présentation des GPO

- Vidéo

Définition des GPO (dans un domaine AD)

- Les GPO sont définies par des objets de classe **groupPolicyContainer** dans l'annuaire (AD)




```
cn
objectClass: groupPolicyContainer
displayName
nTSecurityDescriptor
versionNumber
gPCFunctionalityVersion
gPCFileSysPath
gPCMachineExtensionNames
gPCUserExtensionNames
gPCWQLFilter
```

Attributs de la classe `groupPolicyContainer` définissant une GPO

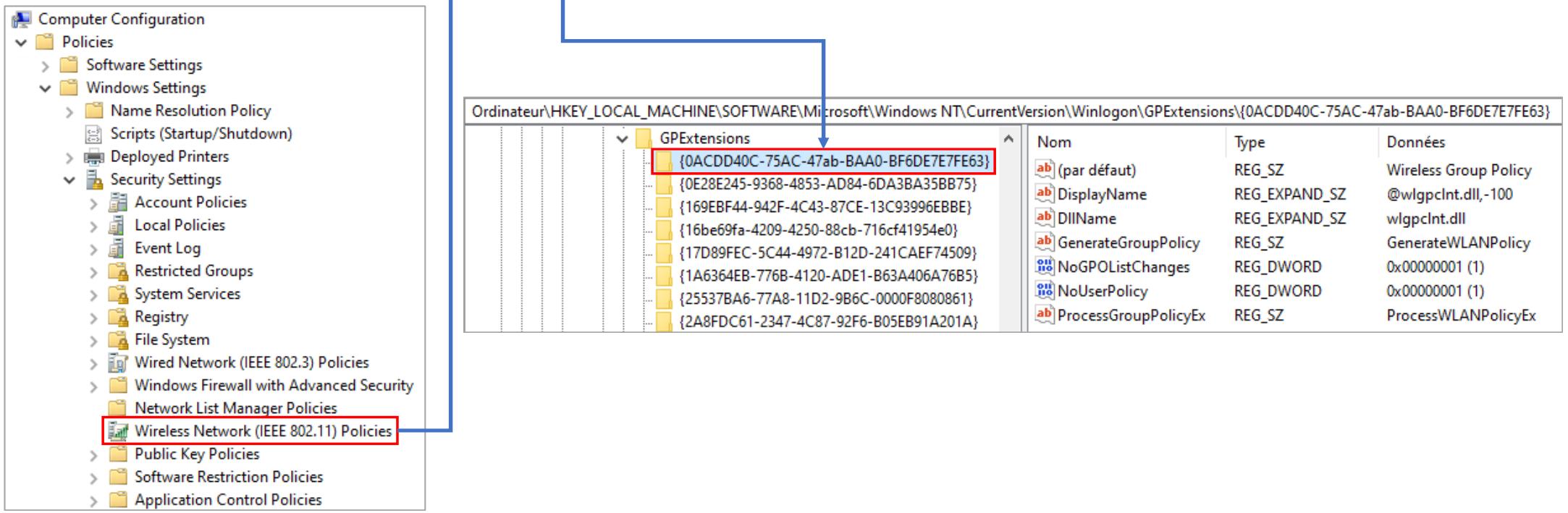
- **`cn`** : identifiant (de type `{GUID}`) de la GPO
- **`displayName`** : nom textuel
- **`nTSecurityDescriptor`** : descripteur de sécurité
- **`versionNumber`** : versions des parties Ordinateur/Utilisateur
- **`flags`** : options de désactivation des parties Ordinateur/Utilisateur
- **`gPCFunctionalityVersion`** : version fonctionnelle
- **`gPCMachineExtensionNames`** / **`gPCUserExtensionNames`** : CSE activés
- **`gPCFileSysPath`** : emplacement du répertoire de la GPO
- **`gPCWQLFilter`** : filtre WMI

CSE (*Client Side Extension*)

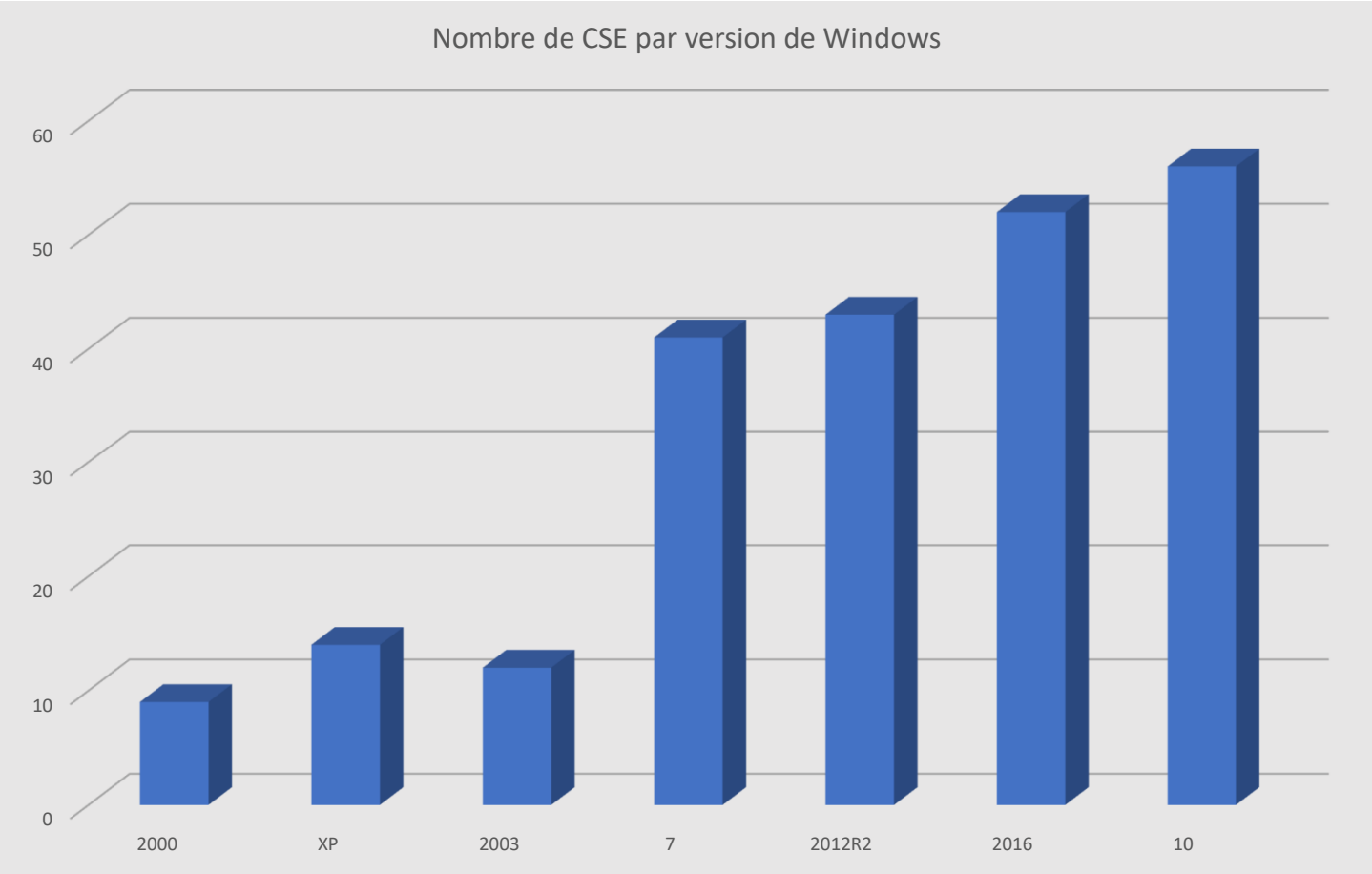
- L'infrastructure GPO n'est qu'un cadre pour la définition des GPO
- L'application des paramètres est dévolu aux CSE :
  - Bibliothèques installées sous Windows (environ 50 par défaut, extensible)
  - L'éditeur de GPO doit activer les CSE pour une GPO en indiquant le GUID du CSE dans les attributs :
    - **`gPCMachineExtensionNames`**
    - **`gPCUserExtensionNames`**

CSE (*Client Side Extension*)

- gPCMachineExtensionNames:
  - [{**0ACDD40C-75AC-47ab-BAA0-BF6DE7E7FE63**}{…}];



Historique CSE



+ Autres

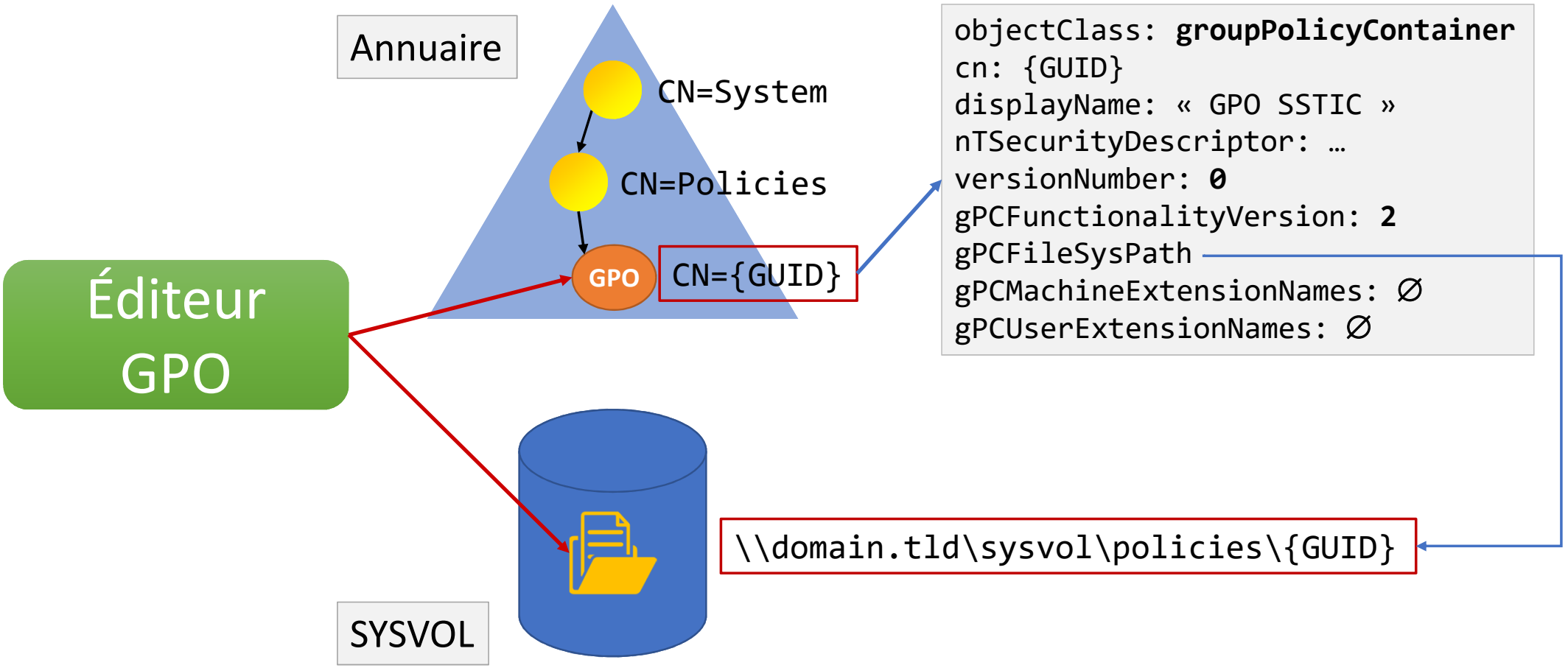
Stockages de paramètres

- Chaque CSE détermine l'emplacement de stockage de ses paramètres

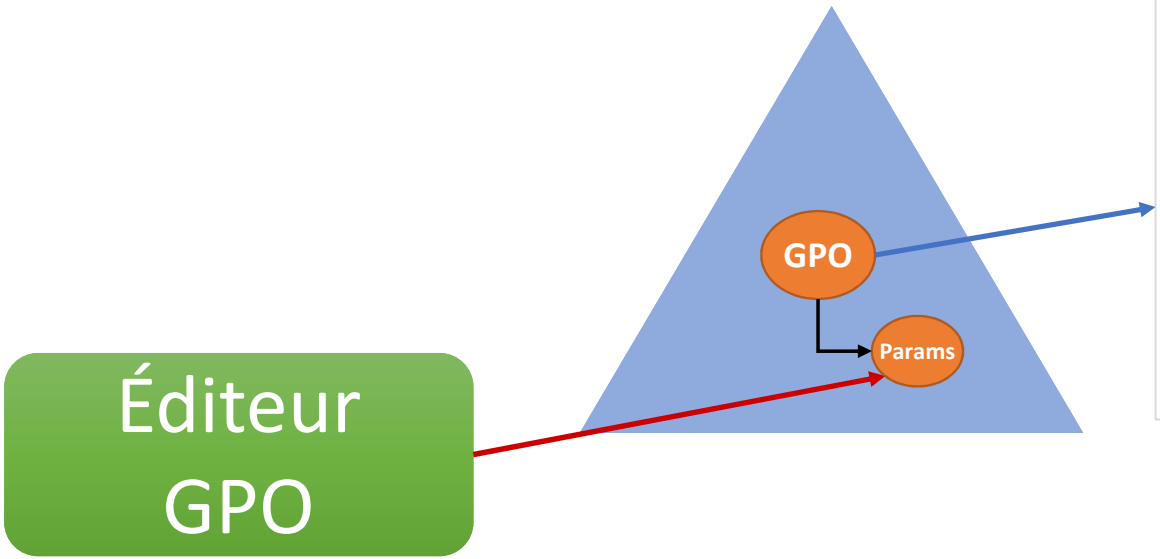
- Le stockage des paramètres d'une GPO peut être :
  - Dans l'annuaire, sous forme d'objets LDAP, fils de l'objet de la GPO
  - Dans l'annuaire, sous forme d'objets LDAP
  - Sous forme de fichier, dans le répertoire de la GPO (le plus utilisé)

- Répertoire de la GPO :
  - Répertoire de stockage propre à une GPO indiqué par le paramètre **`gPCFileSysPath`**
  - Toujours de la forme **`\\domain.tld\sysvol\policies\{GUID}`**

Fonctionnement : création

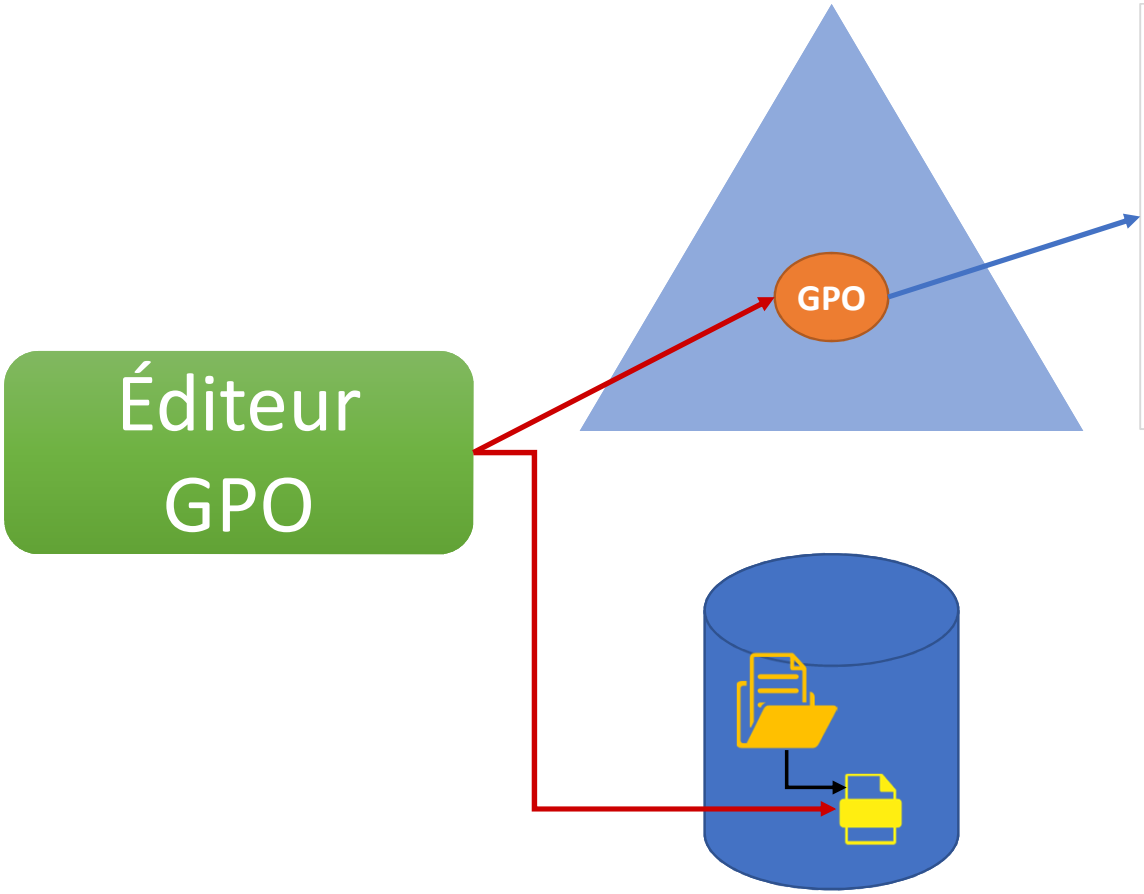


Fonctionnement : modification 1



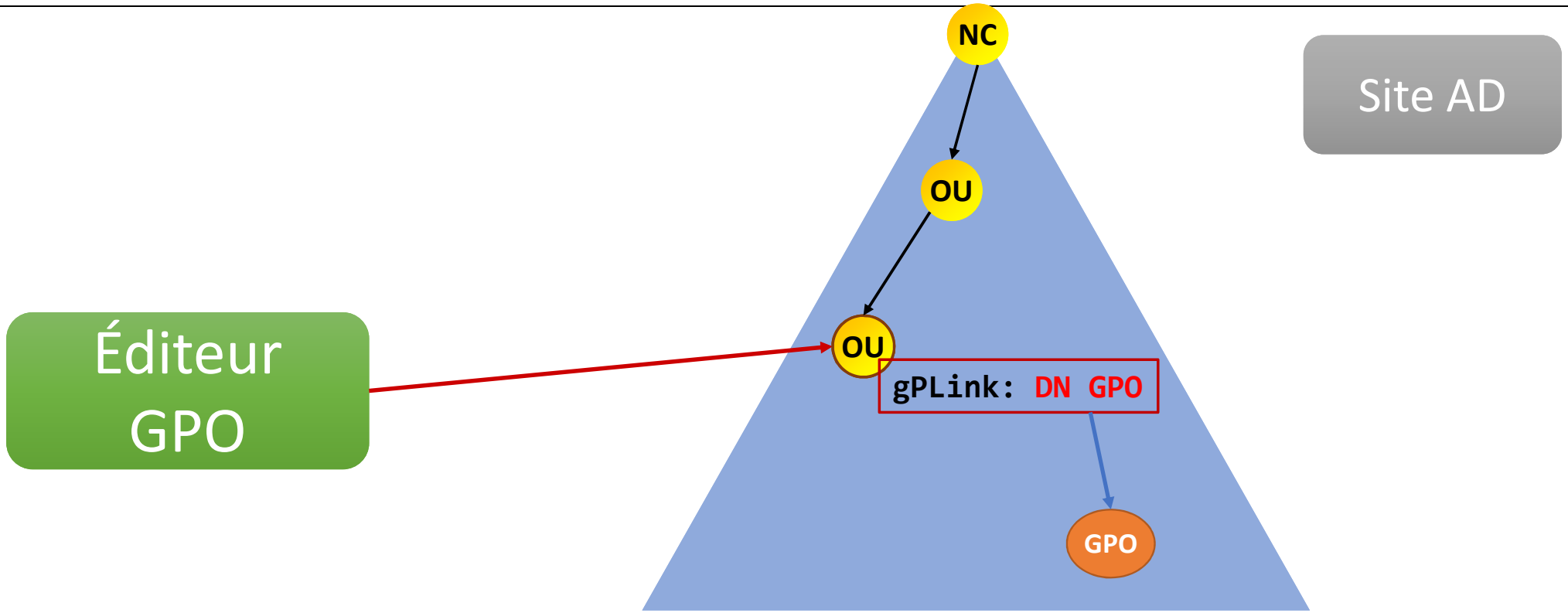

```
cn: {GUID}
displayName: « GPO SSTIC »
nTSecurityDescriptor: …
versionNumber: 1
gPCFunctionalityVersion: 2
gPCFileSysPath
gPCMachineExtensionNames: {CSE1}
gPCUserExtensionNames: ∅
```

Fonctionnement : modification 2

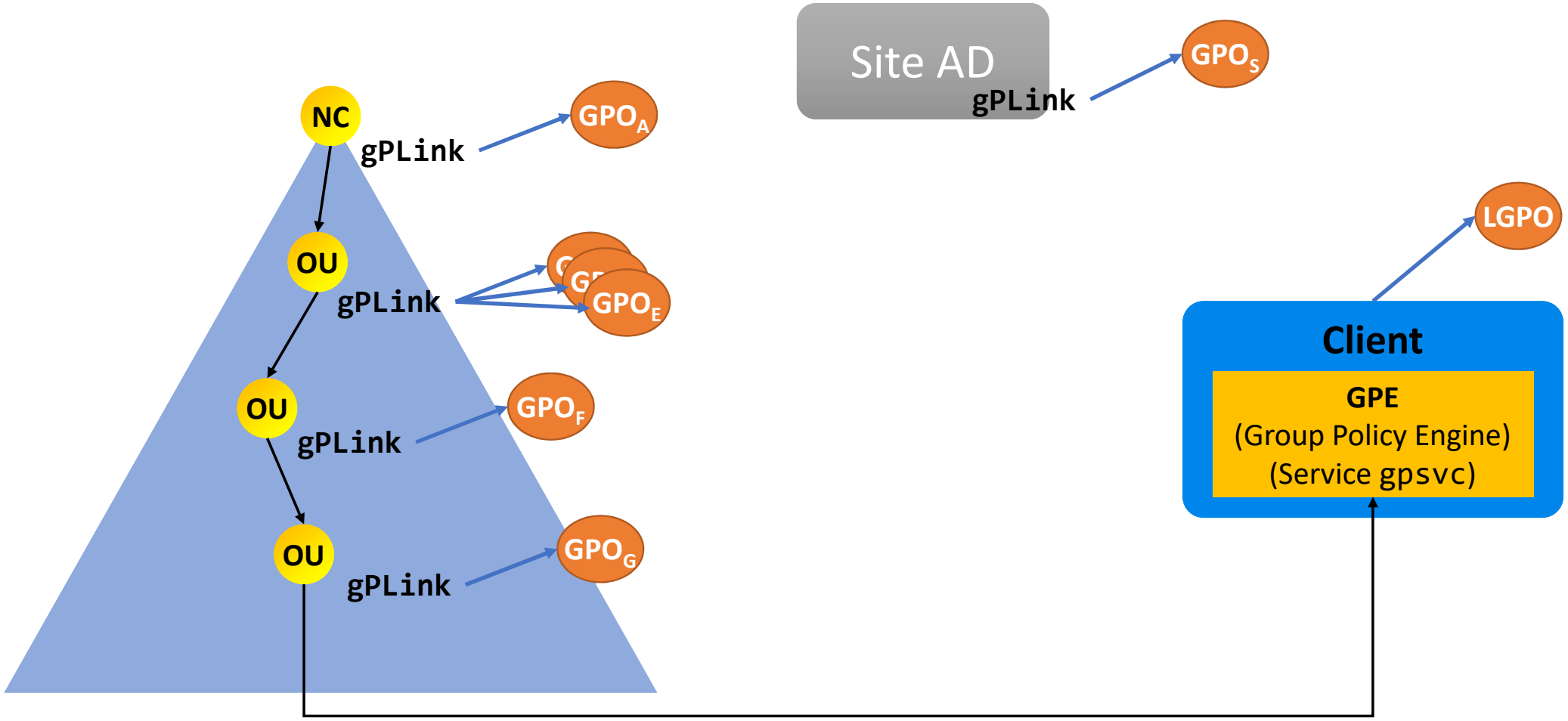



```
cn: {GUID}
displayName: « GPO SSTIC »
nTSecurityDescriptor: …
versionNumber: 2
gPCFunctionalityVersion: 2
gPCFileSysPath
gPCMachineExtensionNames: {CSE1};{CSE2}
gPCUserExtensionNames: ∅
```

Fonctionnement : liaison d'une GPO



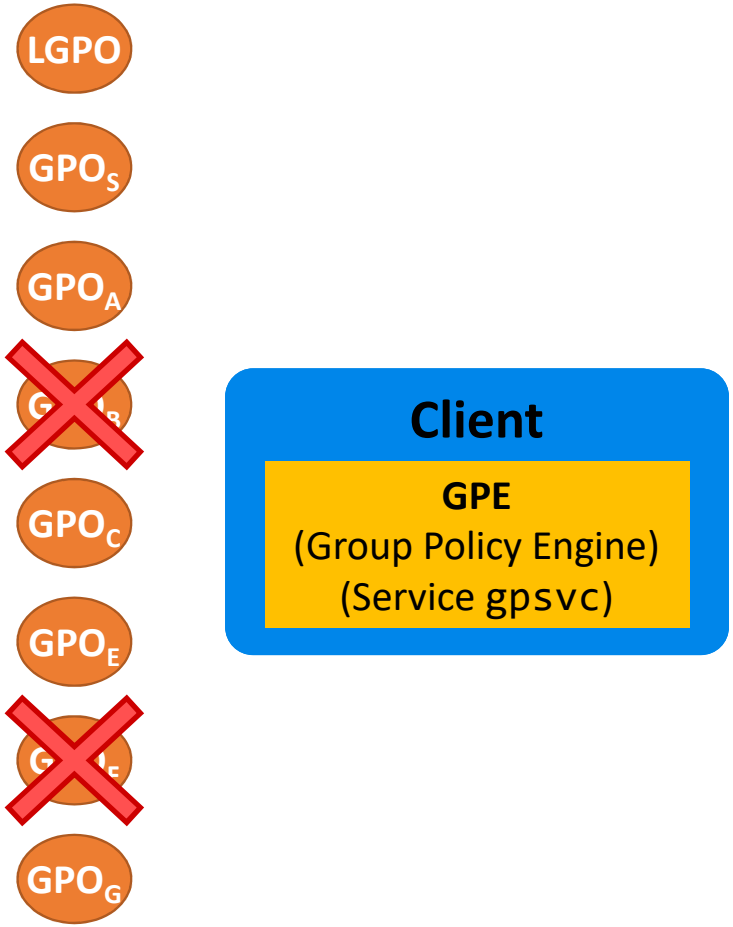
Fonctionnement : application, identification des GPO



Fonctionnement : filtrage

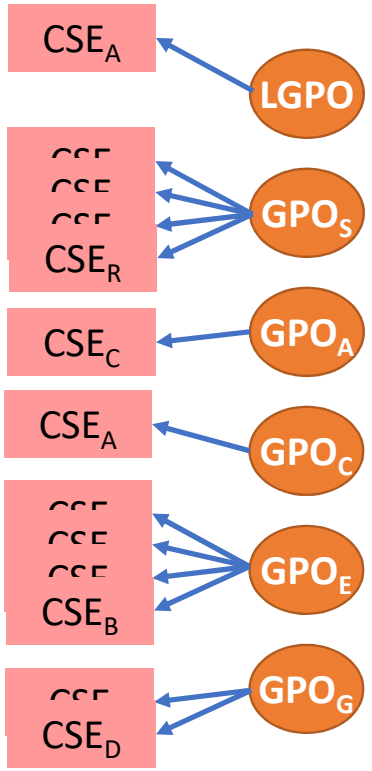
Filtrage sur :

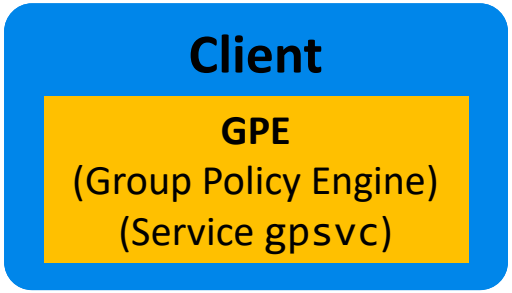
- Niveau fonctionnel (**`gPCFunctionalityVersion`**)
- Activation (**`flags`**)
- Ne doit pas être vide (**`version`**)
- Filtrage de sécurité (**`ntSecurityDescriptor`**)
- Filtrage WMI (**`gpcWQLFilter`**)



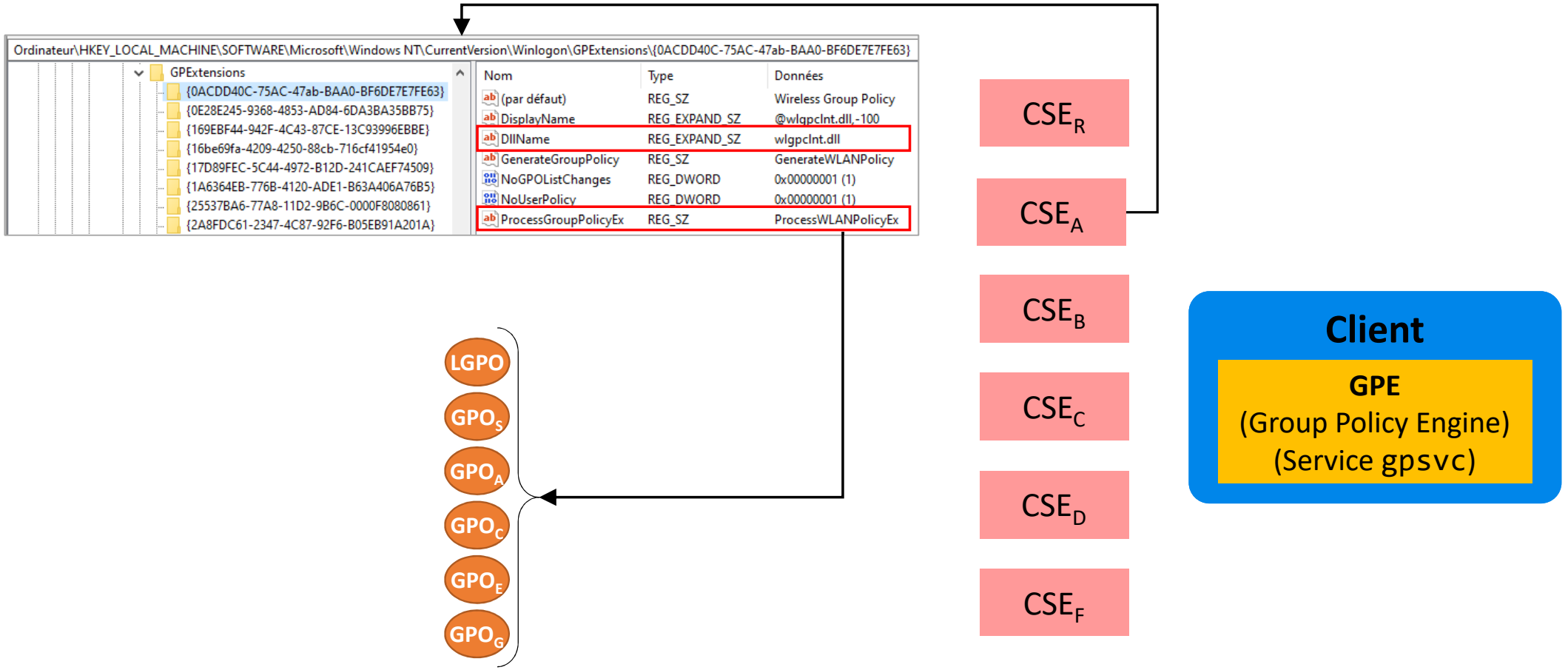
Fonctionnement : inventaire des CSE

Récupération, pour chaque GPO, de la liste des CSE activés (**`gPCMachineExtensionNames`**)





Fonctionnement : appel des CSE



Audit de la configuration

Scénarios d'attaque envisagés

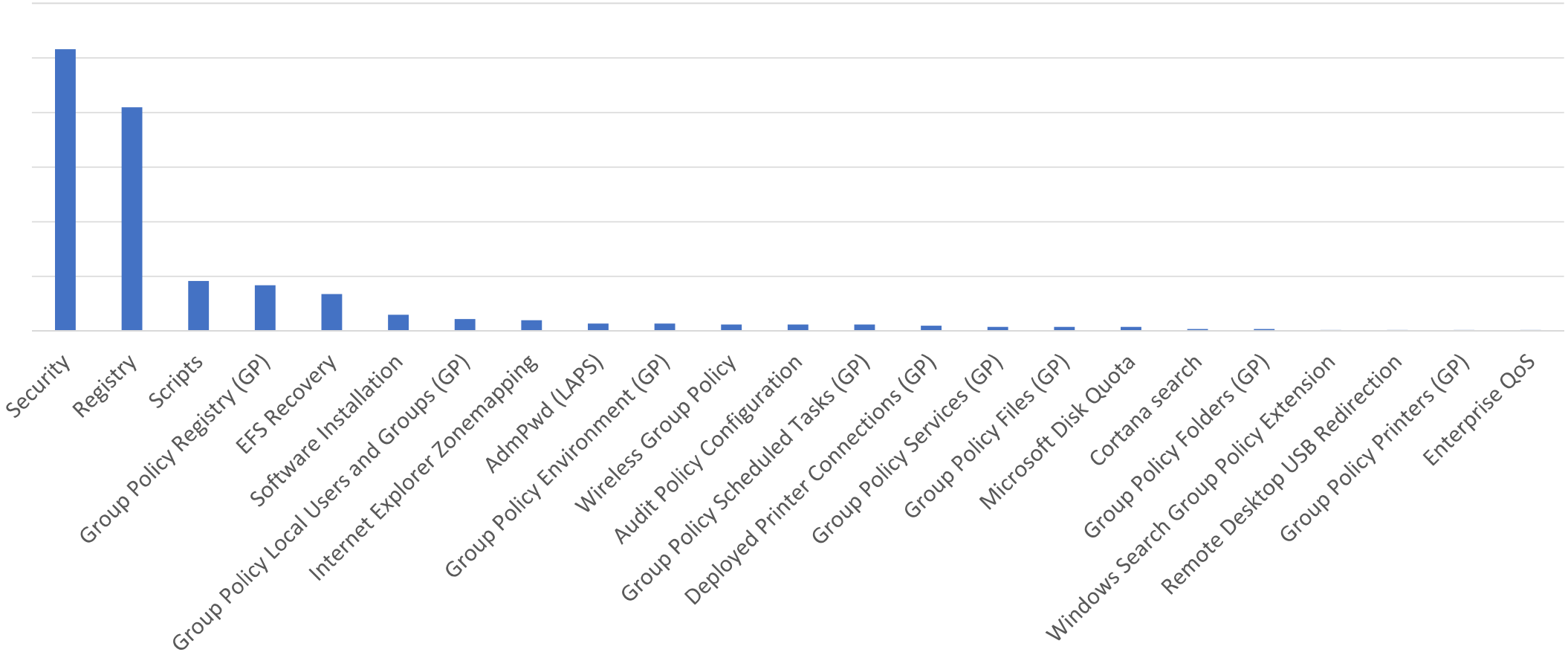
- Mettre à 0 la révision (GPO considérée comme vide)
- Modifier la révision :
  - Désynchronisation entre l'annuaire LDAP et le répertoire SYSVOL
  - Perturbation des mécanismes de cache
- Modifier le niveau fonctionnel (doit toujours être à 2)
- Déplacer le répertoire de la GPO
- Modifier les identifiants des CSE

- Modifier les permissions

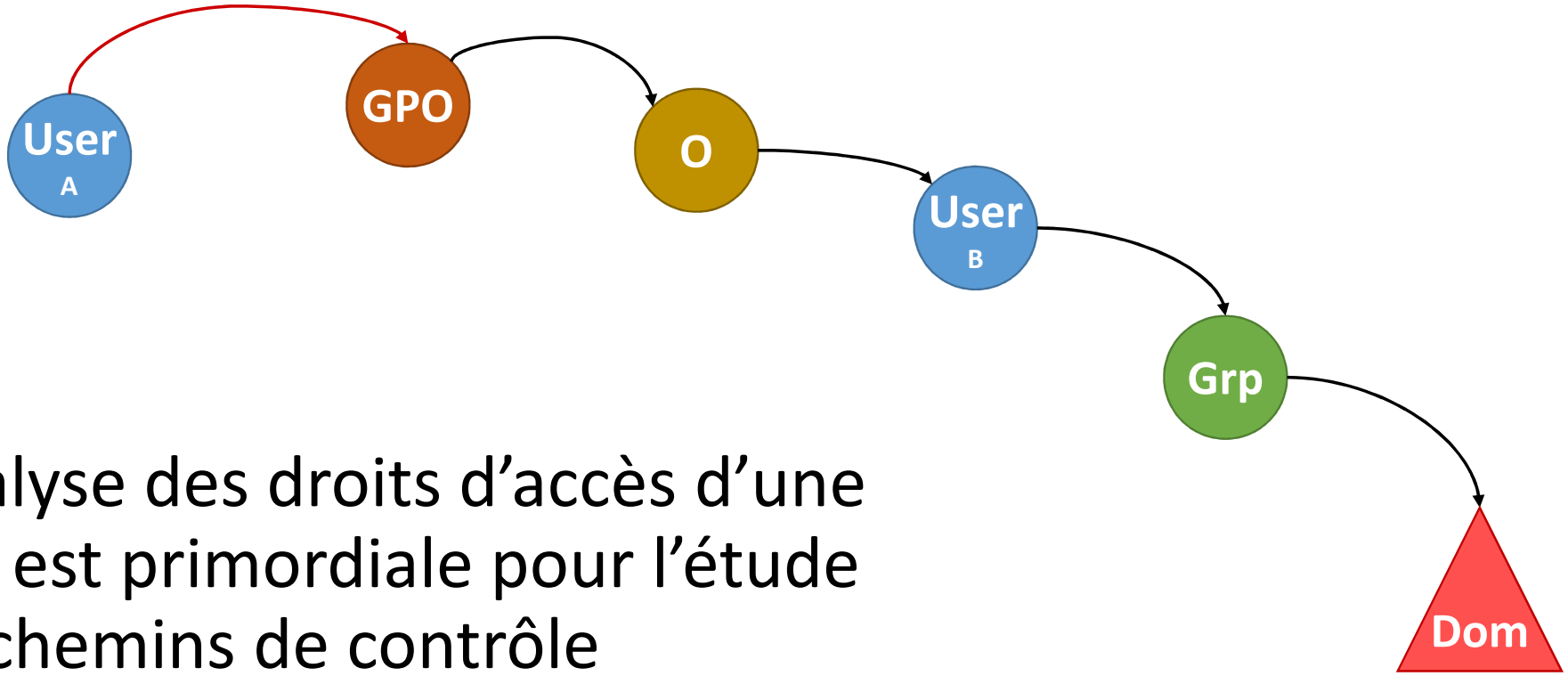
Démo : gpocheck 1/2

- Vidéo

Répartition des CSE

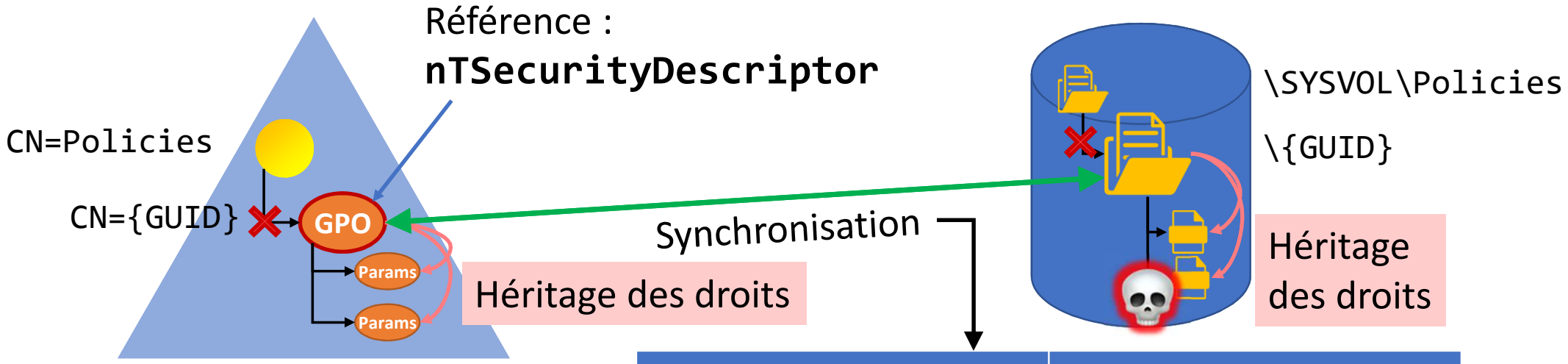


Importances des droits des GPO



- L'analyse des droits d'accès d'une GPO est primordiale pour l'étude des chemins de contrôle

Cas particulier des droits



Éditeur GPO

IsACLConsistent()
MakeACLConsistent()

Droits AD	Droits NTFS
DS_READ_PROP & DS_LIST	FILE_READ_DATA FILE_LIST_DIRECTORY
DS_WRITE_PROP	FILE_WRITE_DATA FILE_ADD_FILE FILE_ADD_SUBDIRECTORY
DS_CREATE_CHILD	ADD_SUBDIRECTORY FILE_ADD_FILE
DS_DELETE_CHILD	FILE_DELETE_CHILD

Points de contrôle descripteur de sécurité

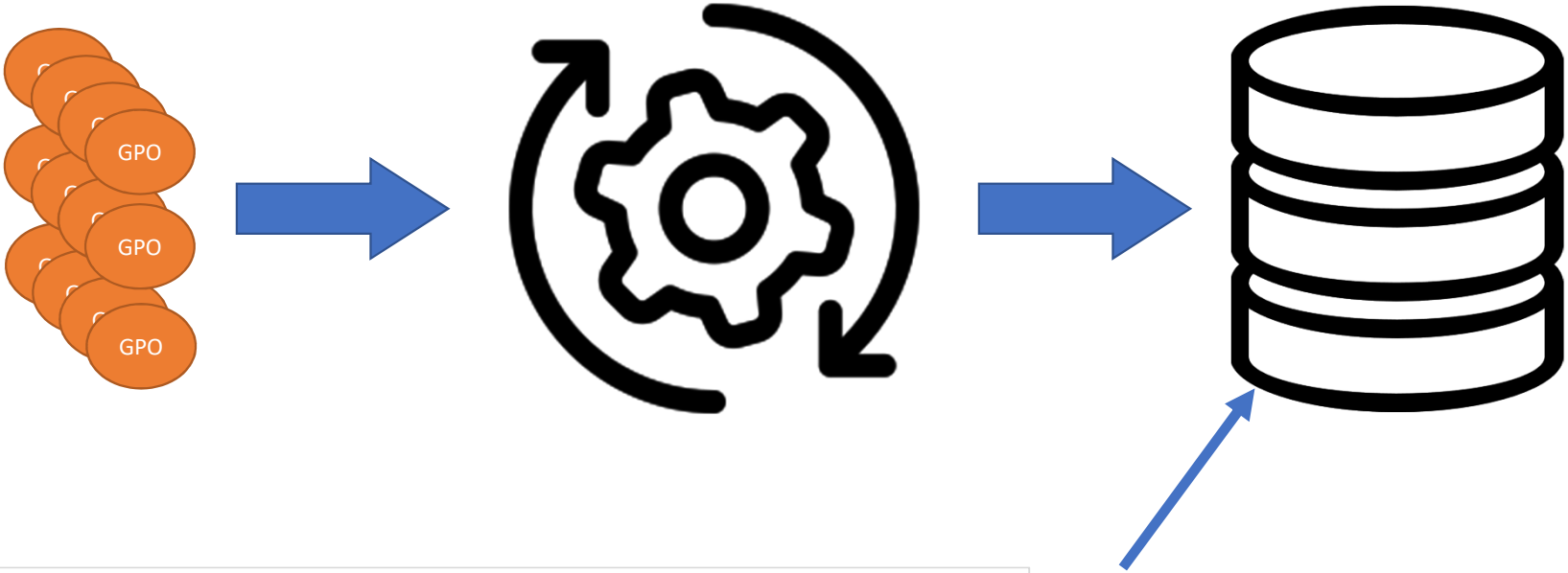
- Les droits sur une GPO sont donnés par l'attribut **`nTSecurityDescriptor`** de son objet LDAP
- La synchronisation ne concerne que le répertoire racine de la GPO dans le SYSVOL
- Pour s'assurer que ces droits soient l'unique référence :
  - Synchronisation entre l'objet GPO dans l'annuaire et le répertoire NTFS dans le SYSVOL
  - Que les droits soient correctement hérités et qu'il n'existe pas d'ACE explicite

Démo : gpocheck 2/2

- Vidéo

Audit des paramètres

Principe

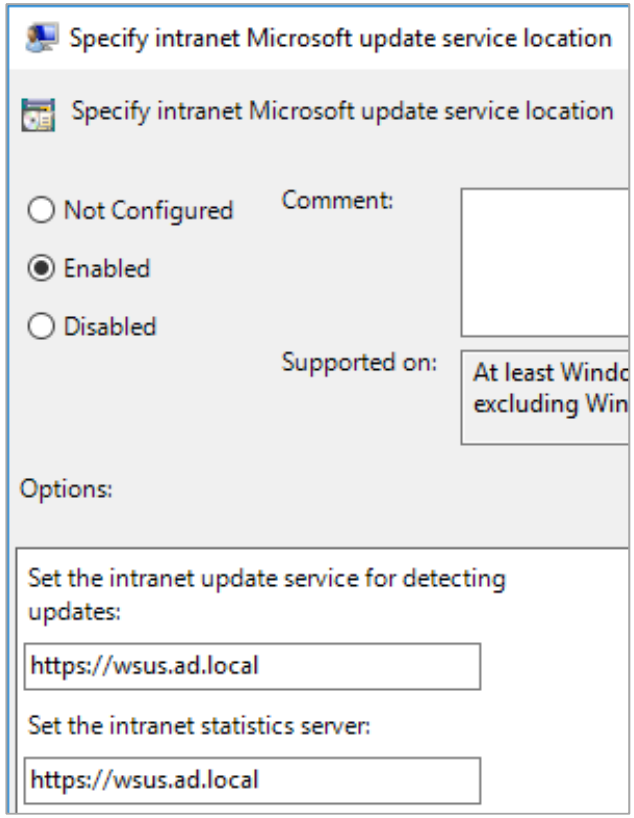



```
SELECT * FROM [gpo]
   WHERE params LIKE '%TerminalService%'
    AND value LIKE 'NLA = disabled'
```

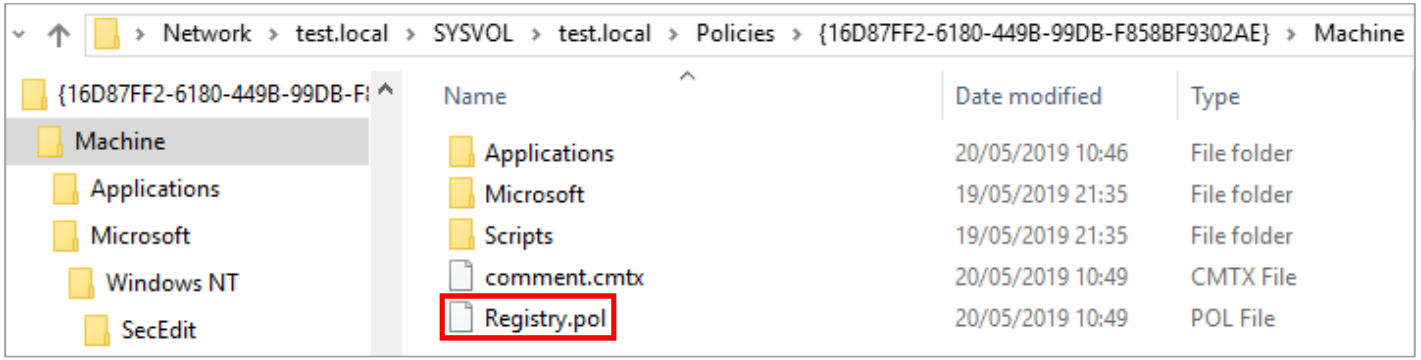
1ère piste : depuis les données de la GPO

- Récupérer les paramètres depuis :
  - Les objets LDAP
  - Les fichiers dans le SYSVOL

CSE Registry



CSE : {35378eac-683f-11d2-a89a-00c04fbbcfa2} (Registre)



Modèles d'administration (.admx / .adml)

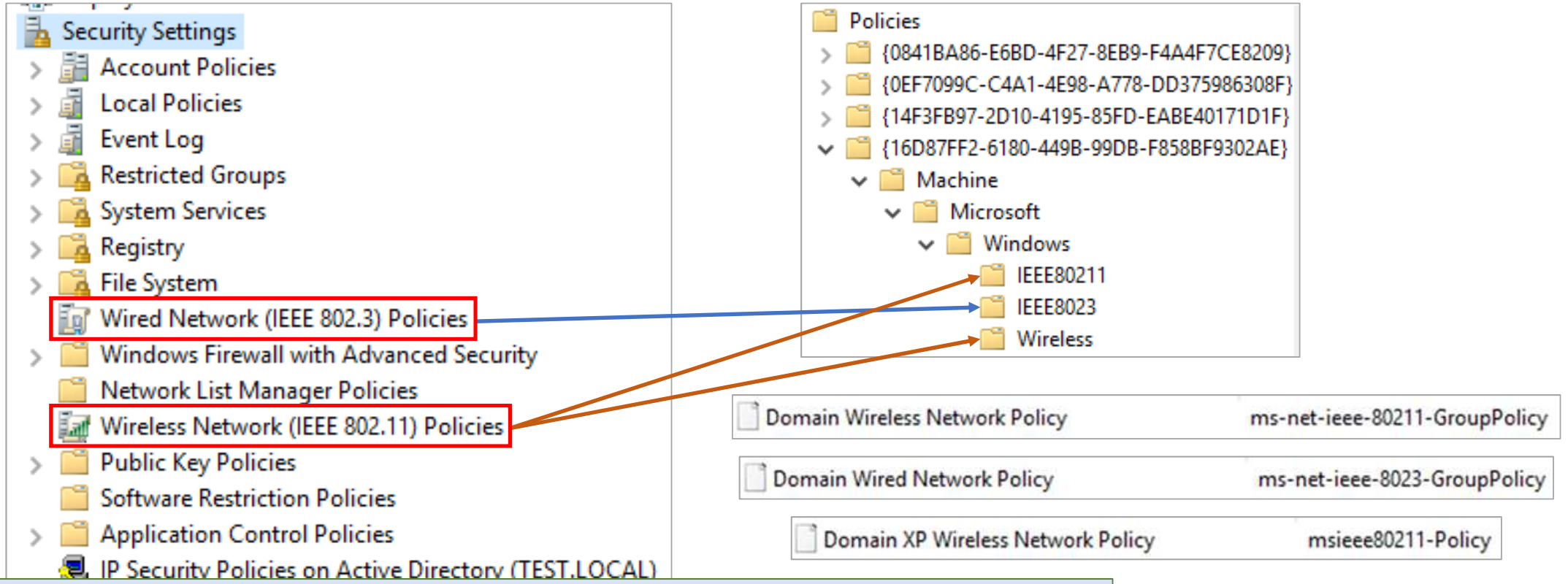
Fichier Registry.pol

Registry.pol

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   50 52 65 67 01 00 00 00 5B 00 53 00 6F 00 66 00   PReg....[.S.o.f.
00000010   74 00 77 00 61 00 72 00 65 00 5C 00 50 00 6F 00   t.w.a.r.e.\.P.o.
00000020   6C 00 69 00 63 00 69 00 65 00 73 00 5C 00 4D 00   l.i.c.i.e.s.\.M.
00000030   69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00   i.c.r.o.s.o.f.t.
00000040   5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00   \.W.i.n.d.o.w.s.
00000050   5C 00 53 00 61 00 66 00 65 00 72 00 00 00 3B 00   \.S.a.f.e.r...;.
00000060   00 00 3B 00 00 00 00 00 3B 00 00 00 00 00 3B 00   ..;.....;.....;.
00000070   5D 00 5B 00 53 00 6F 00 66 00 74 00 77 00 61 00   ].[.S.o.f.t.w.a.
00000080   72 00 65 00 5C 00 50 00 6F 00 6C 00 69 00 63 00   r.e.\.P.o.l.i.c.
00000090   69 00 65 00 73 00 5C 00 4D 00 69 00 63 00 72 00   i.e.s.\.M.i.c.r.
000000A0   6F 00 73 00 6F 00 66 00 74 00 5C 00 57 00 69 00   o.s.o.f.t.\.W.i.
000000B0   6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 72 00   n.d.o.w.s.\.S.r.
000000C0   70 00 56 00 32 00 00 00 3B 00 00 00 3B 00 00 00   p.V.2...;...;...
```

Registry Key	Registry Value	Value Type	Data
Software\Policies\Microsoft\Windows\Safer			
Software\Policies\Microsoft\Windows\SrpV2			
Software\Policies\Microsoft\Windows\WindowsUpdate	WUServer	REG_SZ	https://wsus.ad.local
Software\Policies\Microsoft\Windows\WindowsUpdate	WUStatusServer	REG_SZ	https://wsus.ad.local
Software\Policies\Microsoft\Windows\WindowsUpdate	UpdateServiceUrlAltern...	REG_SZ	
Software\Policies\Microsoft\Windows\WindowsUpdate\AU	UseWUServer	REG_DWORD	00000001

Paramètres de sécurité : politiques réseau

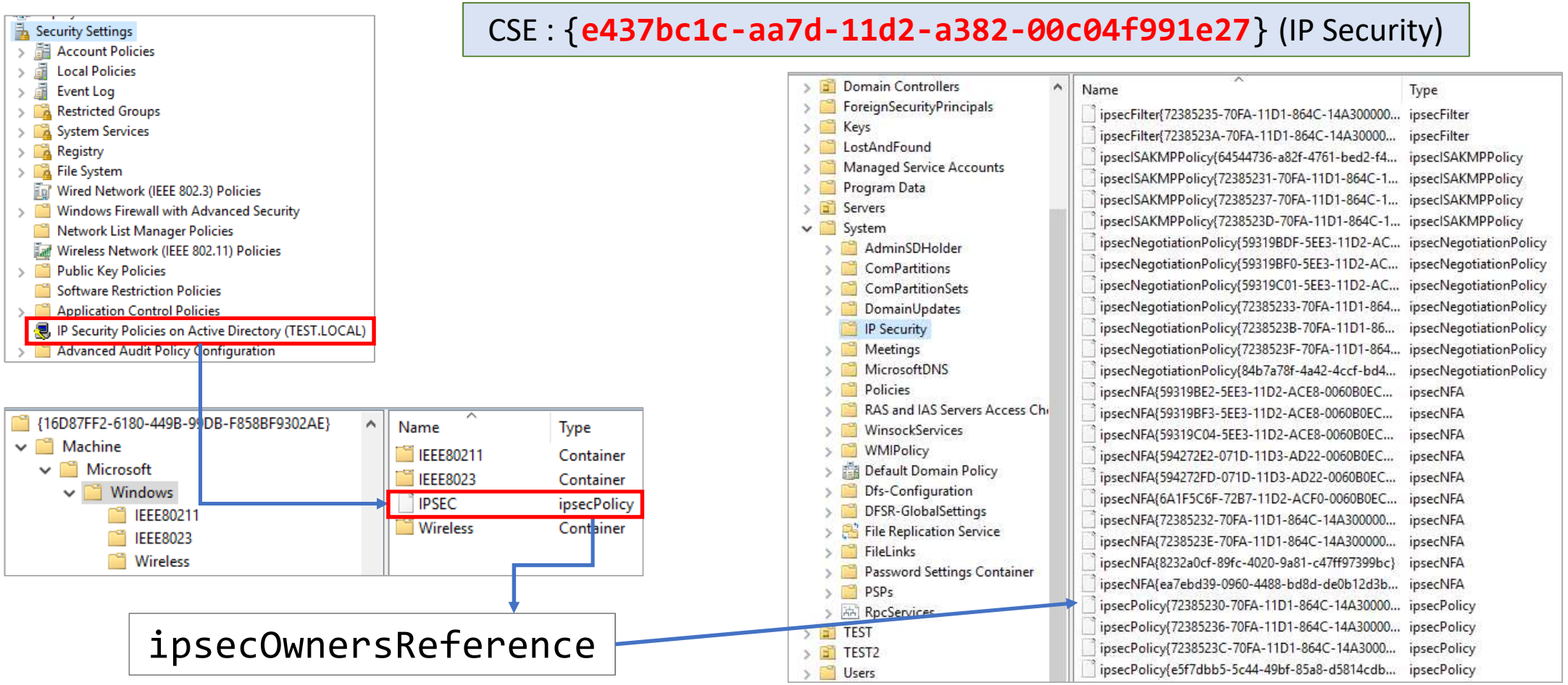


CSE : {**0acdd40c-75ac-47ab-baa0-bf6de7e7fe63**} (Wireless Group Policy)

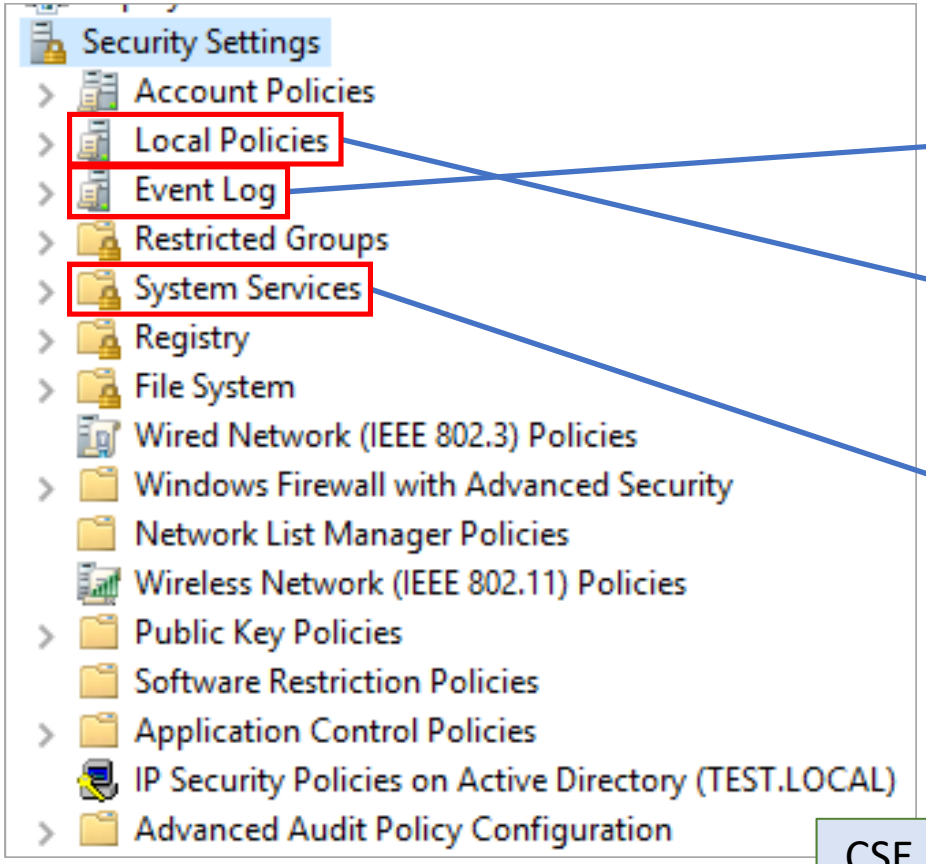
CSE : {**b587e2b1-4d59-4e7e-aed9-22b9df11d053**} (802.3 Group Policy)

Paramètres de sécurité : politiques IPsec

CSE : {e437bc1c-aa7d-11d2-a382-00c04f991e27} (IP Security)



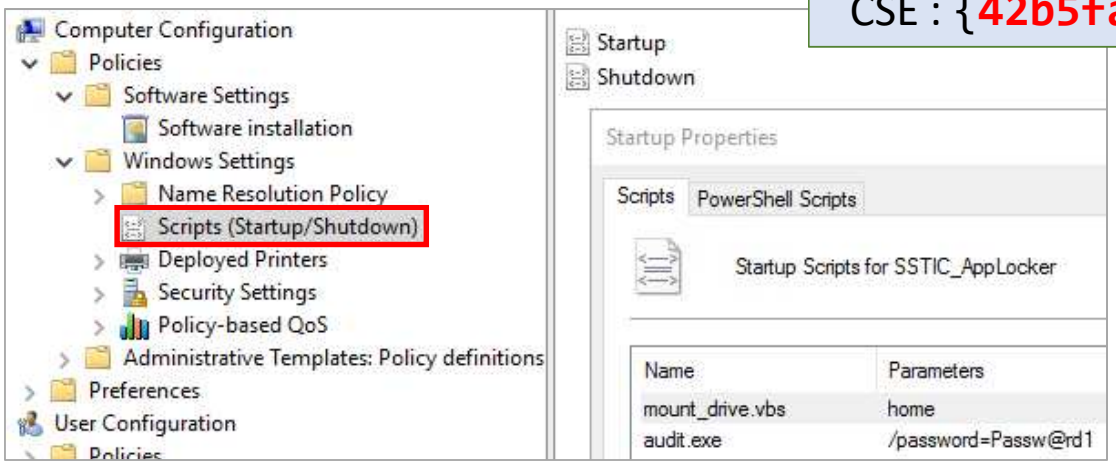
Paramètres de sécurité




```
\Machine\Microsoft\Windows NT\SecEdit\GptTmpl.inf

[Security Log]
MaximumLogSize = 99968

[Registry Values]
MACHINE\Software\...\System\ScForceOption=4,1
MACHINE\System\...\LmCompatibilityLevel=4,4

[Service General Setting]
"AppIDSvc",2,""
```

CSE : {**827d319e-6eac-11d2-a4ea-00c04f79f83a**} (Security)

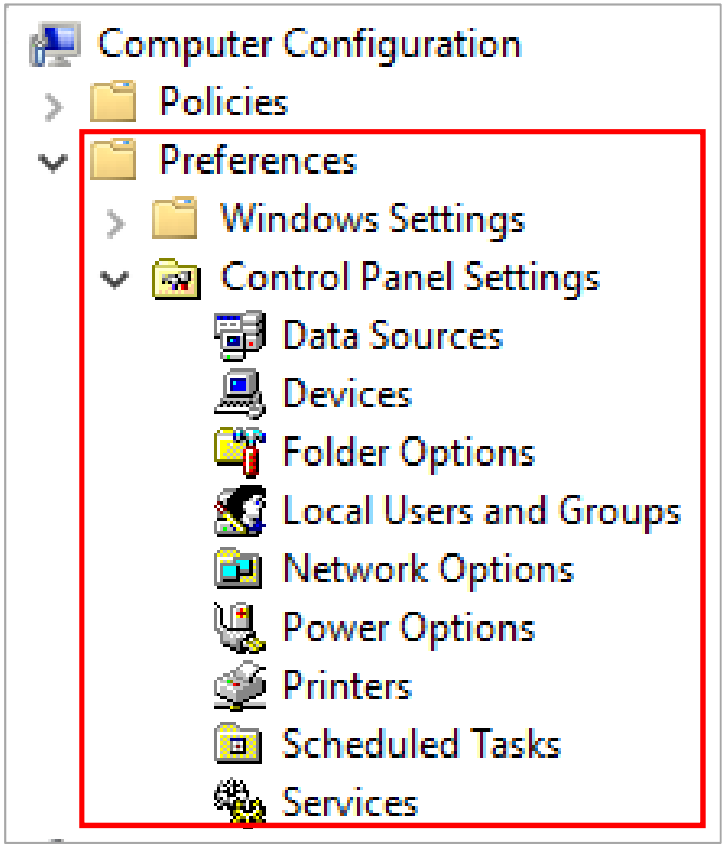
Scripts



CSE : {**42b5faae-6536-11d2-ae5a-0000f87571e3**} (Scripts)

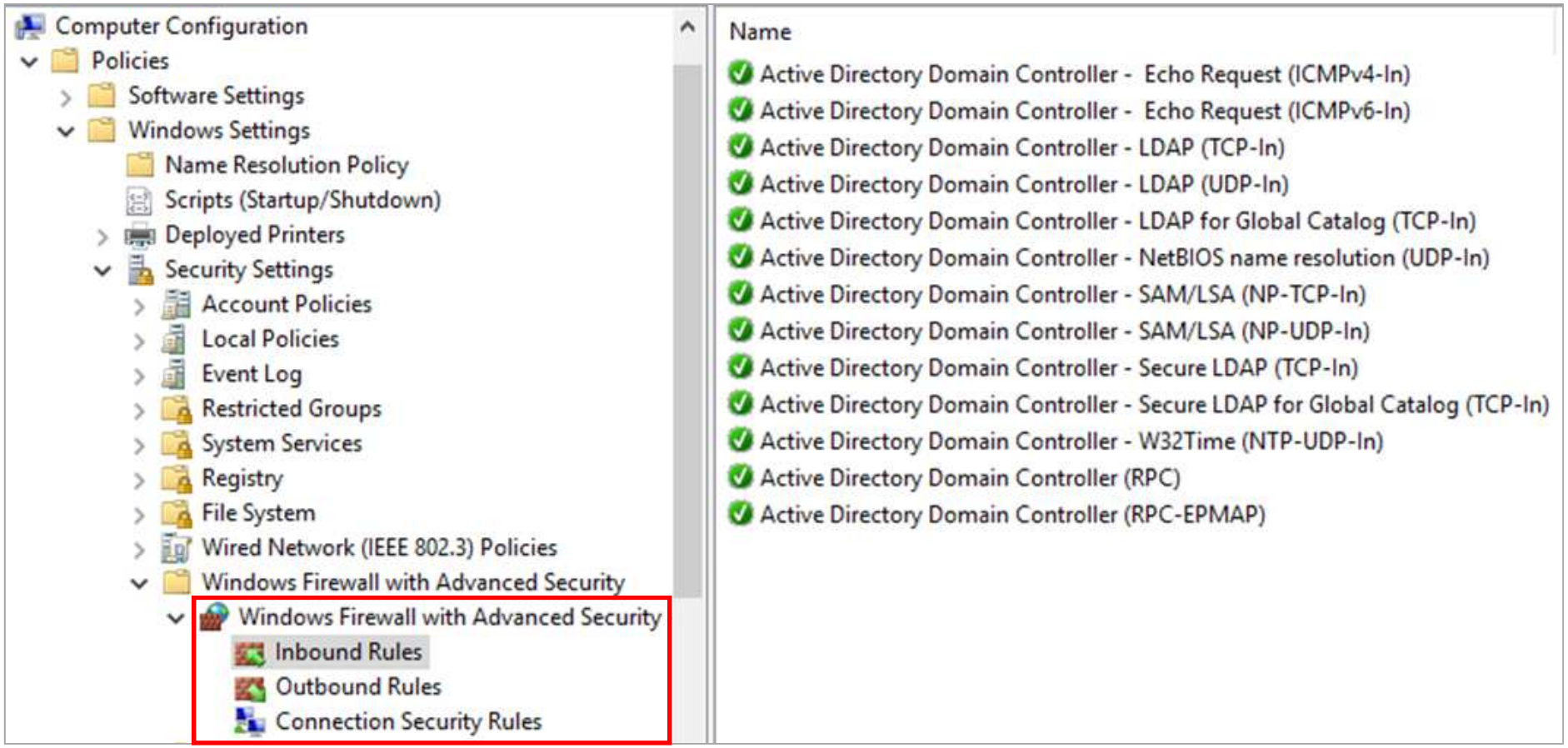
```
\Machine\Scripts\scripts.ini

[Startup]
0CmdLine=mount_drive.vbs
0Parameters=home
1CmdLine=audit.exe
1Parameters=/password=Passw@rd1
```

GPO de préférence




```
\Machine\Preferences\

  IniFiles\IniFiles.xml
  Groups\Groups.xml
  NetworkOptions\NetworkOptions.xml
  ScheduledTasks\ScheduledTasks.xml
  Services\Services.xml
  …
```

Règles du pare-feu



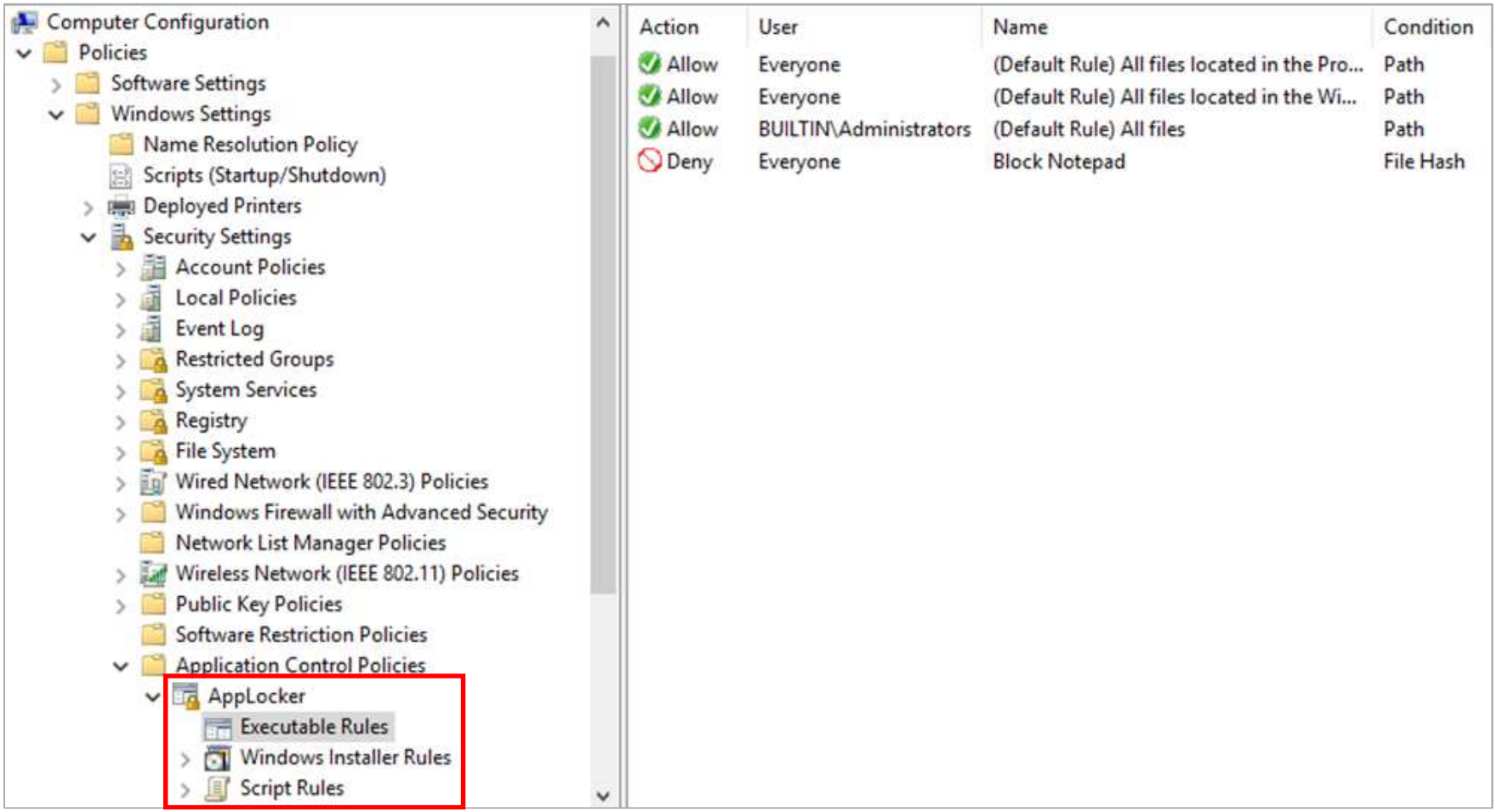
Règles du pare-feu

Registry Key	Registry Value	Value Type	Data
SOFTWARE\Policies\Microsoft\WindowsFirewall	PolicyVersion	REG_DWORD	0000021a
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile	EnableFirewall	REG_DWORD	00000001
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile	DefaultOutboundAction	REG_DWORD	00000000
SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile	DefaultInboundAction	REG_DWORD	00000001
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-ICMP6-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=58|ICMP6=128:*|Name=@ntdsmsg.dll,-1031|Desc=@ntdsmsg.dll,-1032|...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-ICMP4-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=1|ICMP4=8:*|Name=@ntdsmsg.dll,-1027|Desc=@ntdsmsg.dll,-1028|Em...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	W32Time-NTP-UDP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPort=123|App=%systemroot%\System32\svchost.exe|Name=@ntd...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-NB-Datagram-U...	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPort=138|App=System|Name=@ntdsmsg.dll,-1011|Desc=@ntdsms...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-NP-TCP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=445|App=System|Name=@ntdsmsg.dll,-1010|Desc=@ntdsmsg....
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-NP-UDP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPort=445|App=System|Name=@ntdsmsg.dll,-1009|Desc=@ntdsms...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-LDAPGCSEC-T...	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=3269|App=%systemroot%\System32\lsass.exe|Name=@ntdsms...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-LDAPGC-TCP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=3268|App=%systemroot%\System32\lsass.exe|Name=@ntdsms...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-LDAPSEC-TCP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=636|App=%systemroot%\System32\lsass.exe|Name=@ntdsmsg...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-LDAP-UDP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=17|LPort=389|App=%systemroot%\System32\lsass.exe|Name=@ntdsms...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-LDAP-TCP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=389|App=%systemroot%\System32\lsass.exe|Name=@ntdsmsg...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-RPCEPMAP-TC...	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=RPC-EPMap|App=%systemroot%\system32\svchost.exe|Svc=r...
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	ADDS-RPC-TCP-In	REG_SZ	v2.26|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=RPC|App=%systemroot%\System32\lsass.exe|Name=@ntdsms...

```
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules - ADDS-NP-TCP-In
   v2.26|Action=Allow|Active=TRUE|Dir=In|
   Protocol=6|LPort=445|
   App=System|Name=@ntdsmsg.dll,-1010|Desc=@ntdsmsg.dll,-1023|
   EmbedCtxt=@ntdsmsg.dll,-1026|
```

CSE : {35378eac-683f-11d2-a89a-00c04fbbcfa2} (Registre)

Règles AppLocker



Règles AppLocker

Registry Key	Registry...	Value Type	Data
Software\Policies\Microsoft\Windows\SrpV2\Appx			
Software\Policies\Microsoft\Windows\SrpV2\Dll			
Software\Policies\Microsoft\Windows\SrpV2\Exe\921cc481-6e17-4653-8f75-050b80acca20	Value	REG_SZ	<FilePathRule Id="921cc481-6e17-4653-8f75-050b80acca20" Name="(...
Software\Policies\Microsoft\Windows\SrpV2\Exe\a61c8b2c-a319-4cd0-9690-d2177cad7b51	Value	REG_SZ	<FilePathRule Id="a61c8b2c-a319-4cd0-9690-d2177cad7b51" Name="(...
Software\Policies\Microsoft\Windows\SrpV2\Exe\aa0c648f-a19f-497f-8f34-70c7f0fd135a	Value	REG_SZ	<FileHashRule Id="aa0c648f-a19f-497f-8f34-70c7f0fd135a" Name="Den...
Software\Policies\Microsoft\Windows\SrpV2\Exe\fd686d83-a829-4351-8ff4-27c7de5755d2	Value	REG_SZ	<FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(D...
Software\Policies\Microsoft\Windows\SrpV2\Msi			<FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(D...
Software\Policies\Microsoft\Windows\SrpV2\Script			<FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(D...

HKLM\Software\Policies\Microsoft\Windows\SrpV2\Exe\aa0c648f-a19f-497f-8f34-70c7f0fd135a - Value

```
<FileHashRule
  Id="aa0c648f-a19f-497f-8f34-70c7f0fd135a" Name="Deny notepad" Description=""
  UserOrGroupSid="S-1-1-0" Action="Deny">
  <Conditions>
    <FileHashCondition>
      <FileHash Type="SHA256" Data="0x4115113c2800122296d1ea1f97c26c33701ec14b002e96b60746e70c49ef9d85"
      SourceFileName="notepad.exe" SourceFileLength="243200"/>
    </FileHashCondition>
  </Conditions>
</FileHashRule>
```

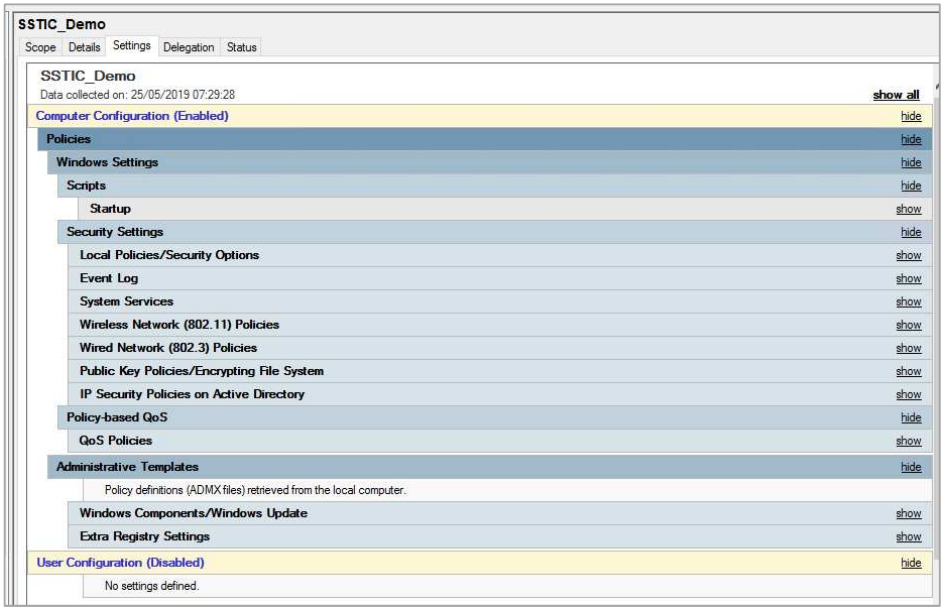
CSE : {**35378eac-683f-11d2-a89a-00c04fbbcfa2**} (Registre)

1ère piste : depuis les données de la GPO

- Bilan de la méthode :
  - Données facilement récupérables :
    - Objets LDAP
    - Fichiers dans le SYSVOL
  - Solution qui nécessite :
    - Une connaissance des différents formats
    - Le développement de parseurs spécifiques
  - Logique des paramètres des GPO à comprendre et à reconstruire

2e piste : depuis les exports XML

- Le moteur d'édition des GPO permet l'export d'un rapport d'une GPO donnée contenant tous les paramètres définis



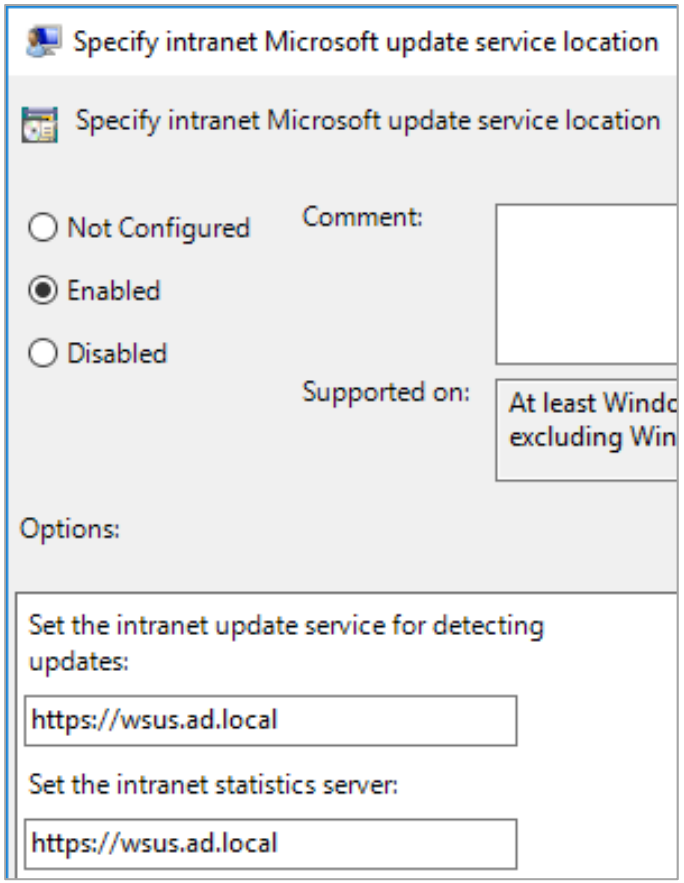
Format HTML

```
PS> Get-GPOReport -ReportType Html
```

Format XML

```
PS> Get-GPOReport -ReportType Xml
```

Exemple détaillé : modèles d'administration

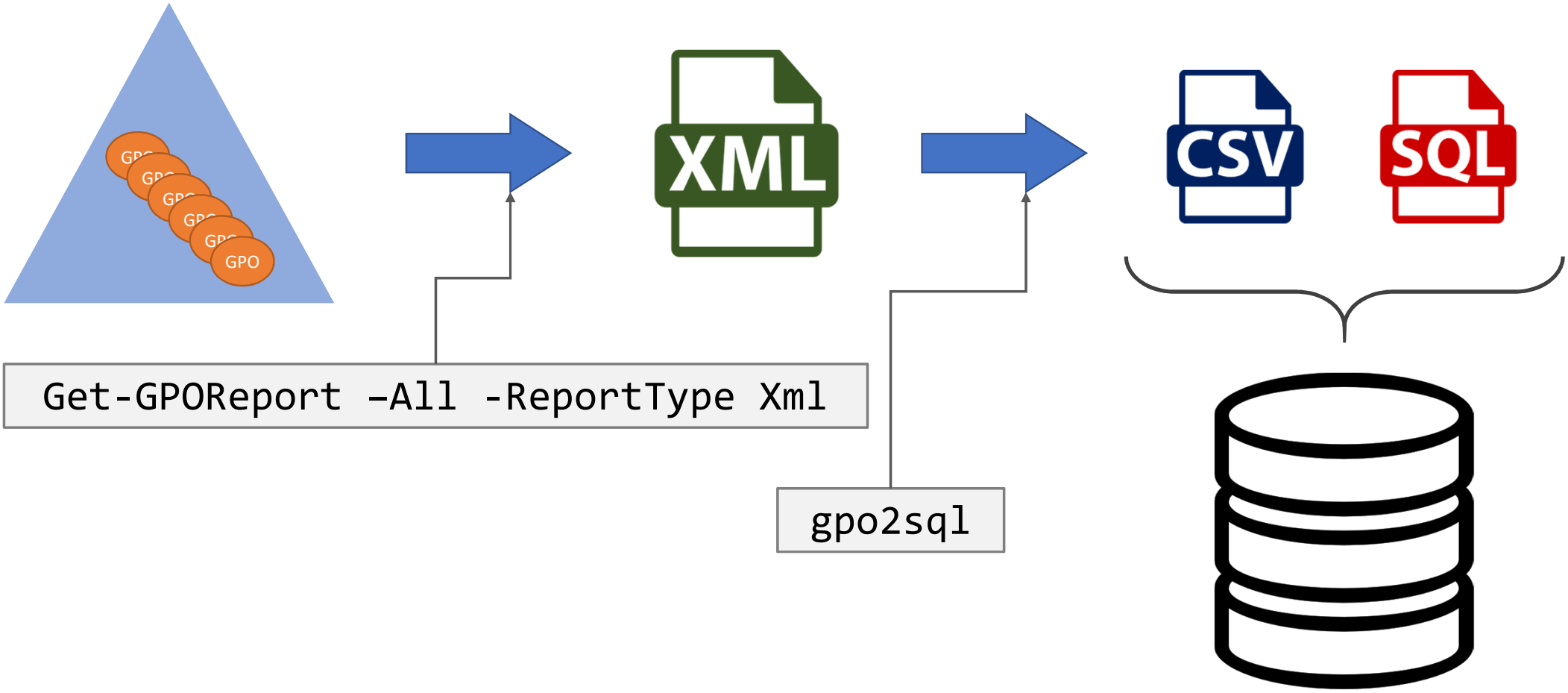



```
<GPO>
 <Computer>
  <ExtensionData>
   <Extension>
    <q1:Policy>
     <q1:Name>Specify intranet Microsoft update service location</q1:Name>
     <q1:State>Enabled</q1:State>
     <q1:EditText>
      <q1:Name>Set the intranet update service for detecting updates:</q1:Name>
      <q1:State>Enabled</q1:State>
      <q1:Value>https://wsus.ad.local</q1:Value>
     </q1:EditText>
     <q1:EditText>
      <q1:Name>Set the intranet statistics server:</q1:Name>
      <q1:State>Enabled</q1:State>
      <q1:Value>https://wsus.ad.local</q1:Value>
     </q1:EditText>
    </Extension>
    <Name>Registry</Name>
   </q1:Policy>
  </ExtensionData>
 </Computer>
</GPO>
```

Exemple détaillé : AppLocker


```
<GPO>
 <Computer>
  <ExtensionData>
   <Extension>
    <q11:RuleCollection Type="Exe">
     <q11:FilePathRule Id="fd686d83-a829-4351-8ff4-27c7de5755d2" Name="(Default Rule) All files" UserOrGroupSid="S-1-5-32-544«
       Action="Allow">
      <q11:Conditions>
       <q11:FilePath Path="*" />
      </q11:Conditions>
     </q11:FilePathRule>
     <q11:FileHashRule Id="4fc79b42-1865-4910-aee5-0bca51f62a7b" Name="Block Notepad" UserOrGroupSid="S-1-1-0" Action="Deny">
      <q11:Conditions>
       <q11:FileHash Type="Sha256">
        <q11:FileInformation Name="notepad.exe" Length="243200" />
       </q11:FileHash>
      </q11:Conditions>
     </q11:FileHashRule>
    </q11:RuleCollection>
   </Extension>
   <Name>Application Control Policies</Name>
  </ExtensionData>
 </Computer>
</GPO>
```

Processus d'export GPO et d'import SQL



Démo : gpo2sql

- Vidéo

2e piste : depuis les exports XML

- Bilan :
  - Nécessite une conversion avec les RSAT GPO
  - Il faut aimer analyser des fichiers XML…
  - Logique des paramètres GPO respectées
  - Quelques paramètres non exportés dans le fichier XML

Conclusion

- Encore du travail de développement…
- Résultats :
  - Configuration : Souvent, il existe des déviances
  - Paramètres : …

- Présentation ici de l'audit des GPO (configuration et paramètres) depuis les données de l'AD et du SYSVOL
  - Mais il faut auditer également l'application sur chaque ordinateur

Liens

- gpocheck
  - https://github.com/aurel26/gpocheck
- gpo2sql
  - https://github.com/aurel26/gpo2sql
- Liste des CSE
  - https://github.com/aurel26/gpolist

Questions ?

aurelien26 (at) free.fr