Un nom de principal de service, *service principal name* (SPN) en anglais, est un identifiant ou alias, tel qu’un enregistrement de type "CNAME" dans un contexte DNS. Il fait partie d’une liste de noms de principaux de service, enregistrée dans les attributs d’un objet Active Directory, sous le nom "servicePrincipalName".

Les noms de principaux de services sont utilisés pour permettre une authentification mutuelle entre un client d’application et un service utilisant Kerberos. En effet, lorsqu’un client d’application se connecte à un service distant, le client d’application demande un ticket de service auprès du domaine, qui le redirige vers le service Kerberos. Le service Kerberos recherche alors dans l’annuaire Active Directory le nom de principal de service qui lui est présenté afin de fournir au client d’application un ticket approprié.

Un nom de principal de service permet d’identifier l’instance d’un service sur un serveur et respecte le paterne "<classe>/<hôte>:<port>/<surnom>" qui est composé des éléments suivants :

* **La classe du service** : Un code générique qui correspond au service. Exemple : Pour un serveur *web*, la classe du service est "www".
* **Le nom d’hôte**: Le nom d’hôte, *hostname* en anglais, ou FQDN du serveur sur lequel le service est exécuté.
* **Le port logique** : Le port sur lequel le service est en écoute. Celui-ci est facultatif, il permet d’éviter toute ambiguïté ou de déclarer un port qui n’est pas le port d’écoute par défaut de la classe.
* **Le surnom**: Celui-ci est facultatif.

Par exemple, un nom principal de service pour un serveur *web* hébergé sur le serveur "WEB-SERVER-01.adsec.local", qui écouté sur le port par défaut peut être : "www/WEB-SERVER-01.adsec.local".

Le script PowerShell suivant permet de lister les objets du domaine Active Directory ayant un ou plusieurs noms principaux de services :

$search = New-Object DirectoryServices.DirectorySearcher([ADSI]"")

$search.filter = "(servicePrincipalName=\*)"

$results = $search.Findall()

foreach($result in $results) {

$userEntry = $result.GetDirectoryEntry()

Write-host "Object : " $userEntry.name "(" $userEntry.distinguishedName ")"

Write-host "List SPN :"

foreach($SPN in $userEntry.servicePrincipalName)

{

Write-Host $SPN

}

Write-host ""

}

Le filtre suivant permet de lister uniquement les utilisateurs du domaine Active Directory ayant un ou plusieurs noms de principaux de services :

$search.filter = "(&(objectCategory=person)(objectClass=user)(servicePrincipalName=\*))"

Documentation :

* <https://learn.microsoft.com/fr-fr/windows/win32/ad/service-principal-names>
* <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772815(v=ws.10)#service-principal-names>