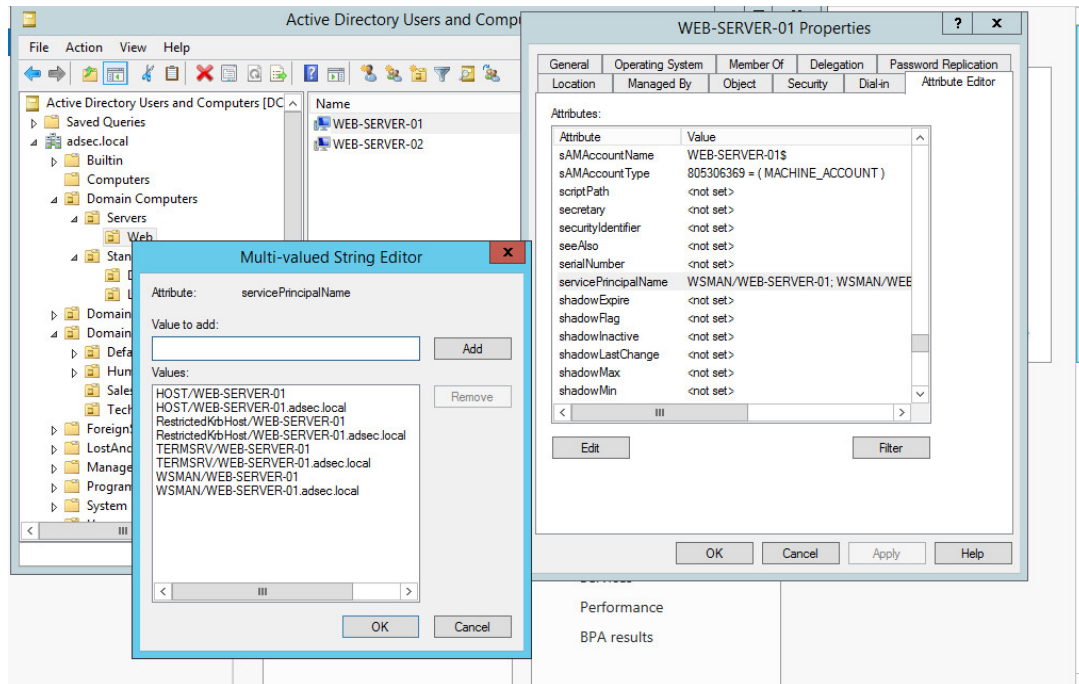


# Service Principal Name (SPN)

 [en.hackndo.com/service-principal-name-spn](https://en.hackndo.com/service-principal-name-spn)

Pixis

January 20, 2020



20 Jan 2020 · 8 min

This article focuses on SPN (Service Principal Names) in order to understand what they are and how they are used.

Author : **Pixis**

## What is an SPN

We are in an Active Directory environment. To understand what is an SPN, we must understand what the notion of service within an Active Directory is.

A service is actually a feature, a software, something that can be used by other members of the AD (Active Directory). You can have for example a web server, a network share, a DNS service, a printing service, and so on. To identify a service, we need at least two things. The same service can run on different hosts, so we need to specify **the host**, and a computer can host several services, so we need to specify **the service**, obviously.

It is by combining these information that we can accurately designate a service. This combination represents its **Service Principal Name**, or **SPN**. It looks like this:

`service_class/hostname_or_FQDN`

The service class is actually a somewhat generic name for the service. For example, all web servers are grouped in the “www” class and SQL services are in the “SqlServer” class.

If the service runs behind a custom port, or if you want to specify it to avoid any ambiguity, you can append it to the hostname:

```
service_class/hostname_or_FQDN:port
```

Optionally, you can name a SPN.

```
service_class/hostname_or_FQDN:port/arbitrary_name
```

For example, in my Active Directory, I have two hosts offering web services, **WEB-SERVER-01** and **WEB-SERVER-02**, and each of these two machines offers other services.

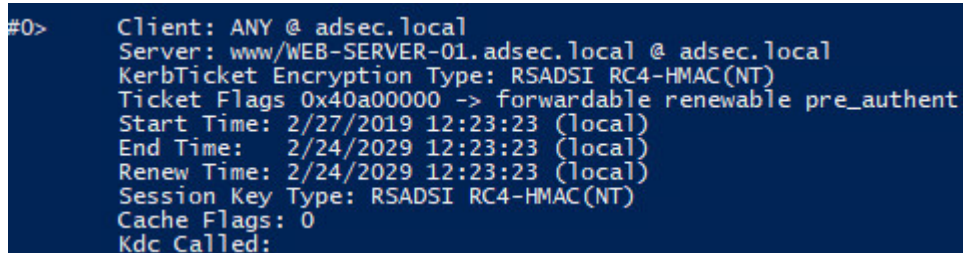
If I want to designate the web server on **WEB-SERVER-01**, the SPN looks like this:

```
www/WEB-SERVER-01
```

or

```
www/WEB-SERVER-01.adsec.local
```

In real life, here's the SPN of a service in a Kerberos ticket:



```
#0> Client: ANY @ adsec.local
Server: www/WEB-SERVER-01.adsec.local @ adsec.local
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time: 2/27/2019 12:23:23 (local)
End Time: 2/24/2029 12:23:23 (local)
Renew Time: 2/24/2029 12:23:23 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called:
```

This ticket was created after someone asked for **www** service on **WEB-SERVER-01** in **adsec.local** domain.

## Examples

---

There are a large number of service classes, here is a list of built-in one from the [Microsoft documentation](#).

#### Built-in SPNs Recognized for Computer Accounts

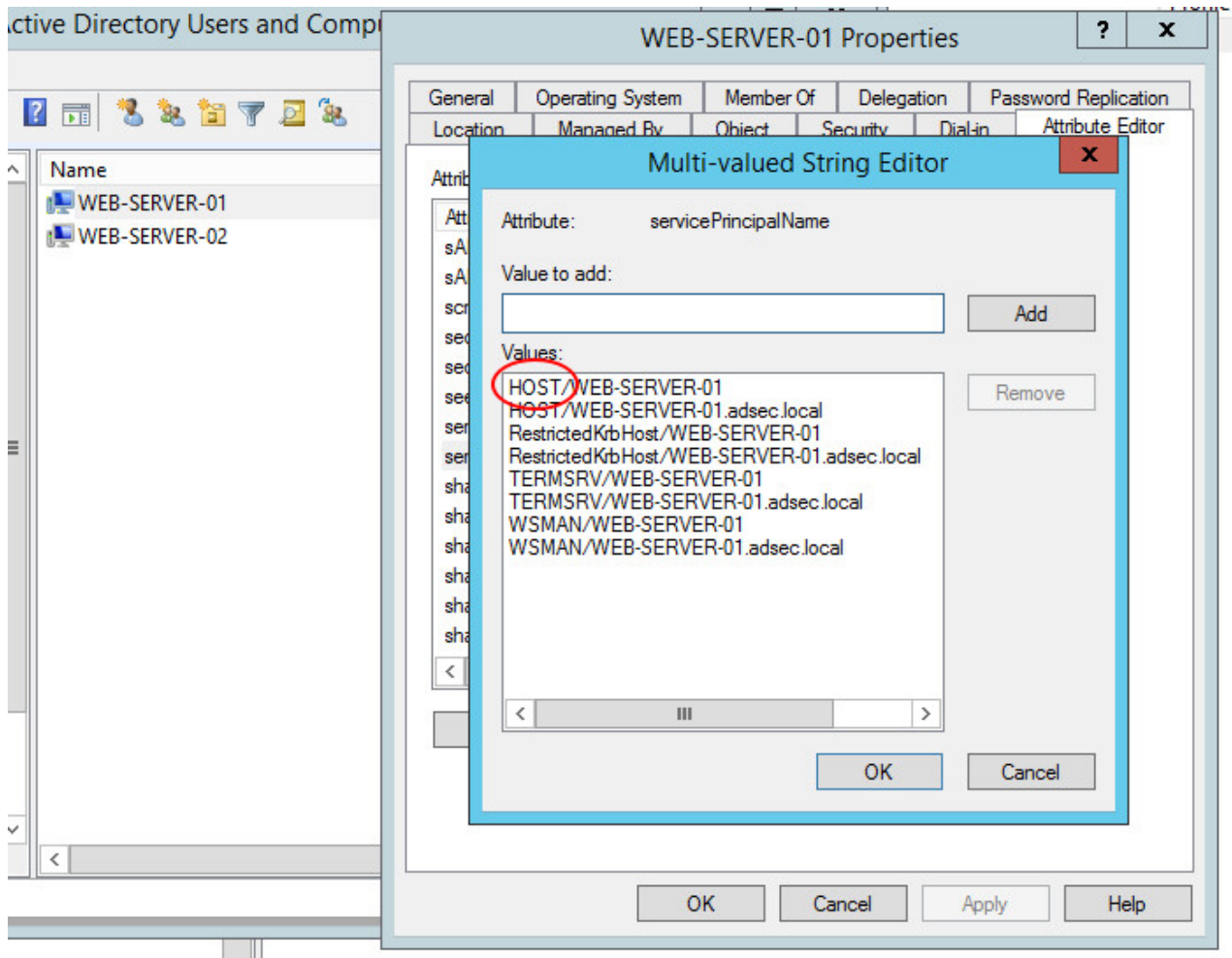
SPN	SPN	SPN	SPN
alerter	http	policyagent	scm
apppmgmt	ias	protectedstorage	seclogon
browser	iisad	rasman	snmp
cifs	min	remoteaccess	spooler
cisvc	messenger	replicator	tapisrv
clipsrv	msiserver	rpc	time
dcom	mcsvc	rpclocator	trksvr
dhcp	netdde	rpcss	trkwks
dmserver	netddedsm	rsvp	ups
dns	netlogon	samss	w3svc
dnscache	netman	scardsvr	wins
eventlog	nmagent	scesrv	www
eventsystem	oakley	schedule	
fax	plugplay		

We recognize a few service classes, such as **CIFS** for services related to file sharing, **DNS**, **WWW** which we've already discussed, or **spooler** which includes printing services.

This list is not exhaustive, for example, there is no **SqlServer**, which is usually found in AD environments, or the **LDAP** class of directory services.

## Edge case - HOST

There is a special case that we encounter in SPN attributes of an object in AD, it is the **HOST** SPN .



**HOST** SPN is not really a service class. It's a group of service classes, a kind of alias that groups together a large number of SPNs. The elements it groups together are defined in the Active Directory's "SPN-Mappings" attribute. These classes can be listed with the following command:

```
Get-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=HALO,DC=NET" -properties sPNMappings
```

```
PS C:\Users\Administrator> Get-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=ADSEC,DC=LOCAL" -properties sPNMappings

DistinguishedName : CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,DC=ADSEC,DC=LOCAL
Name              : Directory Service
ObjectClass       : nTDSservice
ObjectGUID        : 48747387-b607-4e02-8672-10792e79864b
sPNMappings       : {host=alerter,appmgmt,cisvc,clipsrv,browser,dhcp,dnscache,replicator,eventlog,eventsystem,policyag
nt,oakley,dmserver,dns,mcsvc,fax,msiserver,ias,messenger,netlogon,netman,netdde,netddedsm,nmagent,p
lugplay,protectedstorage,rasman,rpclocator,rpc,rpcss,remoteaccess,rsup,samss,scardsvr,scsrv,seclog
on,scm,dcom,cifs,spooler,snmp,schedule,tapisrv,trksrv,trkws,ups,time,wins,www,http,w3svc,iisadmin,
msdct}
```

Thus, if a user ever looks for **www** SPN on **WEB-SERVER-01**, Active Directory will look for **www/WEB-SERVER-01** but it will also look for **HOST/WEB-SERVER-01**. If the host has **HOST** SPN then it means it has **www** SPN (and many others).

**Note:** This SPN (**HOST**) remains a bit of a mystery to me. When generating a Silver Ticket, if you decide that the SPN is **HOST**, then you can perform certain tasks such as managing services or managing scheduled tasks. However, although **CIFS** is included in the **SPN-**

`Mappings` attribute, I was not able to access the `C$` share of the remote host.

After asking about it on [Bloodhound's slack](#), [@pyrotek3](#) ([ADSecurity.org](#)) answered me this:

I have seen the same thing. You would think that HOST would handle most things for the Windows system, but there are certain types of calls that need more than HOST since its a catch-all. I only figured out what worked through trial and error (and lots of testing). From what I have seen HOST can provide SPN coverage and is a "catch-all" for standard system SPNs so the same SPNs don't have to be registered on every system. For "privileged" type activity, using CIFS seems to be required. For Silver Tickets, you can use whatever SPN you want (provided the system will respond) since the DC isn't involved and the SPNs registered on the computer account in AD doesn't really matter (since you create the ticket and connect directly to the system bypassing the DC and AD). It has been a while since I dug into this.

If anyone can clarify this, feel free to share it via comments or by contacting me on Twitter ([@HackAndDo](#)).

## In practice

---

Here is a small PowerShell script that allows you to list the SPNs present in Active Directory. The filter used is `(servicePrincipalName=*)` which returns results with not empty `servicePrincipalName` attribute.

```
$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 ""
}
```

Here's the result in my lab:

```

PS C:\Users\jdoe> $search = New-Object DirectoryServices.DirectorySearcher([ADSI] "")
PS C:\Users\jdoe> $search.Filter = "<servicePrincipalName=*"
PS C:\Users\jdoe> $results = $search.FindAll()
PS C:\Users\jdoe> foreach($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 ""
>> }
>> }
Object : DC-01 < CN=DC-01,OU=Domain Controllers,DC=adsec,DC=local >
List SPN :
TERMSRV/DC-01
TERMSRV/DC-01.adsec.local
Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC-01.adsec.local
ldap/DC-01.adsec.local/ForestDnsZones.adsec.local
ldap/DC-01.adsec.local/DomainDnsZones.adsec.local
DNS/DC-01.adsec.local
GC/DC-01.adsec.local/adsec.local
RestrictedKrbHost/DC-01.adsec.local
RestrictedKrbHost/DC-01
RPC/fe46da82-9d8b-4ccb-8726-4d2f9cf2c5f9._msdcs.adsec.local
HOST/DC-01/ADSEC
HOST/DC-01.adsec.local/ADSEC
HOST/DC-01
HOST/DC-01.adsec.local
HOST/DC-01.adsec.local/adsec.local
E3514235-4B06-11D1-AB04-00C04FC2DCD2/fe46da82-9d8b-4ccb-8726-4d2f9cf2c5f9/adsec.local
ldap/DC-01/ADSEC
ldap/fe46da82-9d8b-4ccb-8726-4d2f9cf2c5f9._msdcs.adsec.local
ldap/DC-01.adsec.local/ADSEC
ldap/DC-01
ldap/DC-01.adsec.local
ldap/DC-01.adsec.local/adsec.local
Object : support account < CN=support account,OU=Technicals,OU=Domain Users,DC=adsec,DC=local >
List SPN :
FAKE/SERVICE
Object : DESKTOP-01 < CN=DESKTOP-01,OU=Desktops,OU=Standard,OU=Domain Computers,DC=adsec,DC=local >
List SPN :
TERMSRV/DESKTOP-01
TERMSRV/DESKTOP-01.adsec.local
RestrictedKrbHost/DESKTOP-01
HOST/DESKTOP-01
RestrictedKrbHost/DESKTOP-01.adsec.local
HOST/DESKTOP-01.adsec.local

```

The different objects with at least one SPN attribute set are displayed.

If we wanted to only see the user accounts that have one (or more) SPNs, here is a possible solution:

```

$search = New-Object DirectoryServices.DirectorySearcher([ADSI] "")
$search.filter = "(&(objectCategory=person)(objectClass=user)
(servicePrincipalName=*))"
$results = $search.Findall()
foreach($result in $results)
{
    $userEntry = $result.GetDirectoryEntry()
    Write-host "User : " $userEntry.name "(" $userEntry.distinguishedName ")"
    Write-host "SPNs"
    foreach($SPN in $userEntry.servicePrincipalName)
    {
        $SPN
    }
    Write-host ""
}

```

Here's the result in my lab:



```

PS C:\Users\jdoe> $search = New-Object DirectoryServices.DirectorySearcher([ADSI]"")
PS C:\Users\jdoe> $search.Filter = "&(objectCategory=person)(objectClass=user)(servicePrincipalName=*)"
PS C:\Users\jdoe> $results = $search.FindAll()
PS C:\Users\jdoe> foreach($result in $results) {
>> $userEntry = $result.GetDirectoryEntry()
>> Write-Host "User : " $userEntry.name "<" $userEntry.distinguishedName ">"
>> Write-Host "List SPN :"
>> foreach($SPN in $userEntry.servicePrincipalName) {
>> Write-Host $SPN
>> }
>> Write-Host ""
>> }
>> }
User : krbtgt < CN=krbtgt,CN=Users,DC=adsec,DC=local >
List SPN :
kadmind/changepw
User : support account < CN=support account,OU=Technicals,OU=Domain Users,DC=adsec,DC=local >
List SPN :
FAKE/SERVICE
PS C:\Users\jdoe>

```

This request will come in handy for an attack that we will describe in another article, **kerberoasting**.

## Conclusion

---

This short post helped me clarify what an SPN is. It's not a complicated thing, however I found the documentation was always vague.

If you have any clarifications or corrections, feel free to share them, as always!