SPN configurations for Kerberos Authentication – A quick reference

techcommunity.microsoft.com/t5/iis-support-blog/spn-configurations-for-kerberos-authentication-a-quick-reference/ba-p/330547

Many people consider configuring Kerberos authentication and making it work as a daunting task. One of the reasons for this is different configuration elements involved in the process.

One such important configuration is setting the appropriate SPN.

There are three important elements that needs to be considered while setting the Kerberos SPN for our application. I have listed them below:

1.How users will browse the application?

Users can browse the application with machine name or with a custom domain name. In most of the cases browsing with machine name does not need an SPN registered. But there are few exceptions.

2.The application pool identity

3.How server is going to decrypt the Kerberos token forwarded by the client.

There are two important properties under

system.webServer/security/authentication/windowsAuthentication

- **useAppPoolCredentials:** When we have useAppPoolCredentials set to true, server will decrypt the Kerberos traffic using application pool identity.
- **useKernelMode:** When we have useKernelMode set to true, server will decrypt the Kerberos traffic using machine account.

Even with good understanding of Kerberos workflow and above-mentioned elements, sometimes people get confused on what SPN to set.

I have included the below table, which can be a quick reference for the SPN's needed for different combinations of host name and application pool identities.

URL	Use Kernel Mode	Use App pool Credentials	Application pool Identity	SPN requirement

Browsed with machine name	True	False	Machine account	No additional SPN's are needed HOST SPN will be sufficient
Browsed with machine name	True	False	Custom domain account	No additional SPN's are needed HOST SPN will be sufficient
Browsed with machine name	False	True	Machine account	No additional SPN's are needed HOST SPN will be sufficient
Browsed with machine name	False	True	Custom domain account	Setspn –a HTTP/<machine name> <custom account name>
Browsed with machine name	True	True	Machine account	No additional SPN's are needed HOST SPN will be sufficient
Browsed with machine name	True	True	Custom domain account	Setspn –a HTTP/<machine name> <custom account name>
Browsed with custom host name	True	False	Machine account	Setspn –a HTTP/<custom host name> <machine name>
Browsed with custom host name	True	False	Custom domain account	Setspn –a HTTP/<custom host name> <machine name>
Browsed with custom host name	False	True	Machine account	Setspn –a HTTP/<custom host name> <machine name>
Browsed with custom host name	False	True	Custom domain account	Setspn –a HTTP/<custom host name> <custom account name>

Browsed with custom host name	True	True	Machine account	Setspn –a HTTP/<custom host name> <machine name>
Browsed with custom host name	True	True	Custom domain account	Setspn –a HTTP/<custom host name> <custom account name>
Browsed with machine name	False	False	Machine account	No additional SPN's are needed HOST SPN will be sufficient
Browsed with machine name	False	False	Custom domain account	Setspn –a HTTP/<machine name> <custom account name>
Browsed with custom host name	False	False	Machine account	Setspn –a HTTP/<custom host name> <machine name>
Browsed with custom host name	False	False	Custom domain account	Setspn –a HTTP/<custom host name> <custom account name>

Hope this helps.