Configuring multiple SPNs for one Service Account in AD

You may sometimes need more than one Service Principal Name (SPN) for a Service Account in AD. For example:

- The Atlassian application is using a CNAME, but you need to support clients that don't perform hostname canonicalization. Kerberos for REST or Kerberos for Git (any client or script built on libcurl) is a prime example of this. For such clients to work, you will need to register two SPNs one way or another. You can either create a second service account for the non-canonicalized name and merge the keytabs in Kantega SSO, or register both SPNs to a single service account using the ktpass method described in this document.
- You prefer to have one service account for all your Atlassian applications. We don't recommend this, but it's possible.

Why we recommend one SPN per service account only

The problem with multi-SPN accounts and keytabs is that, whenever you need to update an SPN, there's a high risk of breaking existing keytab files used by *the other* applications.

For example, imagine Confluence, Bitbucket, Jira and Bamboo all using CNAMEs, with SPNs that are all registered to svc-atlassian@EXAMPLE.LOCAL:

- https://confluence.example.com HTTP/appsrv-prd111.a.example.com@EXAMPLE.LOCAL
- https://bitbucket.example.com HTTP/appsrv-prd222.a.example.com@EXAMPLE.LOCAL
- https://jira.example.com HTTP/appsrv-prd333.a.example.com@EXAMPLE.LOCAL
- https://bamboo.example.com HTTP/appsrv-prd444.a.example.com@EXAMPLE.LOCAL

Then a year down the line, the application server for Confluence dies and is restored on a new application server. The CNAME is moved accordingly to point to the new server: appsrv.prd777.b.example.com. For Kerberos to work, you will now need to remove the old SPN for Confluence and instead add:

- HTTP/appsrv.prd777.b.example.com@EXAMPLE.LOCAL

.... One *tiny* mistake when running ktpass, and the keytabs for Jira, Bamboo and Bitbucket are now invalid, and Kerberos no longer works in any of the Atlassian applications.

That said, if you're still convinced multiple SPNs is what you need, this document describes one way of achieving it.

Assume you want the following SPNs for Confluence:

- HTTP/wiki.example.com@EXAMPLE.LOCAL
- HTTP/confluence.example.com@EXAMPLE.LOCA

Step 1: Run ktpass to generate the initial keytab for the correct/canonical SPN:

```
ktpass /princ HTTP/wiki.example.com@EXAMPLE.LOCAL  /mapuser mqdom\MQ_S_CONFLUENCE /crypto AES256-SHA1 /pass *
/ptype KRB5_NT_PRINCIPAL /out C:\my.keytab
```

As this sets the account pass, the Kerberos key potentially changes, so kvno is increased by 1.

Step 2: Run ktpass again to add a key for the alias, *without setting the password again*:

```
ktpass /princ HTTP/confluence.example.com@EXAMPLE.LOCAL /mapuser mqdom\MQ_S_CONFLUENCE /crypto AES256-SHA1 /pass
* /ptype KRB5_NT_PRINCIPAL /in C:\my.keytab /out C:\my_merged.keytab -setpass
```

Note: Make sure to use the same password the second time.

Then simply upload C:\my_merged.keytab replacing the existing keytab, and things should now work using either hostname. The manage keytab page should now show you two keytab entries: One for each SPN/hostname.

Some further explanation of the second ktpass command:

- /princ will add the second SPN to the account if it's not already registered
- /in reads the keytab entries from the first ktpass run and will include them in the new output, so that it now contains both keys
- -setpass is the crucial part. It ensures ktpass doesn't actually update the account password and salt, as this would invalidate the keytab entry from step1 by regenerating the Kerberos key with a new salt (and also increase kvno by 1).
    - Note that you're still asked for a password and must use the same password as the first time. The password is needed to generate the second keytab entry, but again, without updating the account itself.

There are more ways of doing this with ktpass. For further information, refer to the official Microsoft documentation: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ktpass

To initially test this from your local machine with only a browser, you can add both DNS names to your local hosts file (unless this causes secondary problems with vhosts etc). This overrides DNS and causes each name to be temporarily treated as a canonical name by the browser when it tries to acquire Kerberos tickets (the test page may give a warning as the server will have a different view on this than your modified hosts file). Then log into Confluence using the host name you wish to test, and, and run the Kerberos test page, e.g.:

1. https://confluence.example.com
2. https://wiki.example.com

The SPN listed under "Your browser sent the following Kerberos token in the test page should now reflect the Confluence hostname/URL you used. When you use DNS, only #2 should appear when tested from the browser.