Kerberos Keytab erstellen und Debug in UCS

Du möchtest dich gerne für unsere Hilfe erkenntlich zeigen . Gerne. Wir bedanken uns bei dir für deine Spende!

Spenden

Zum frei verfügbaren Apt-Repository

GITLAB:

Eine Keytab wird immer wieder mal benötigt, z.B. für Apache und Kerberosauth. Für SSH gibt es hier schon einen Artikel.

Handelt es sich nicht um eine Hostauth, muss für jede Funktion ein expliziter User in UCS angelegt werden, z.B. HTTP in diesem Beispiel. Der Host/VM wo der Dienst den man mit dem Ticketverahren erreichen möchte, muss nicht zwingend an die Domäne als solches gebunden sein. Es genügt auch nur den Dienst zu authentifizieren. Je nach Situation macht es die direkte Domänenanbindung natürlich leichter.

Keytab mittels Sambatools vom Masterserver exportieren. Z.B. auch für Kerberosticketlogin SSH und HTTP. Hier für den spezifischen Host wiki.deepdoc.at.

```
samba-tool user create krb-deepdoc-http --description="Unprivileged user for
the Wiki" --random-password
samba-tool user setexpiry krb-deepdoc-http --noexpiry
samba-tool spn add HTTP/deepdoc.at krb-deepdoc-http
samba-tool spn add HTTP/deepdoc.at@OSIT.CC krb-deepdoc-http
samba-tool domain exportkeytab --principal=HTTP/deepdoc.at /etc/keytabs/krb-
deepdoc-http.keytab
samba-tool domain exportkeytab --principal=host/deepdoc.at@OSIT.CC
/root/krb5.keytab  # für SSH
```

Das File kann man dann auf dem gewünschten Host in das Verzeichnis seiner Wahl kopieren. z.b. `/etc/apache2/krb5.keytab` Eigentümer und Rechte beachten. Den Inhalt kann man mit folgendem Befehl darstellen:

```
ktutil -k /etc/apache2/krb5.keytab list
```

Das dieser Befehl nicht auf allen Systemen funktioniert, wäre die Alternative die Keytab vorübergehend nach `/etc/krb5.keytab` zu kopieren. Dort kann man diese mit `ktutil list` anzeigen lassen.

Um am UCS-Server die SPN eines Benutzer anzuzeigen bedient man sich folgendem Befehl:

```
samba-tool spn list <username>
```

Der folgende Befehl zeigt die gesetzten Verschlüsselungsmethoden eines User für Kerberos an:

```
net ads enctypes set krb-deepdoc-http
```

Der Ouput könnte so aussehen:

```
[ ] 0x00000009 DES-CBC-CRC
[ ] 0x00000001 DES-CBC-MD5
[X] 0x00000003 RC4-HMAC
[X] 0x00000008 AES128-CTS-HMAC-SHA1-96
[X] 0x00000011 AES256-CTS-HMAC-SHA1-96
[ ] 0x00000010 AES256-CTS-HMAC-SHA1-96-SK
[ ] 0x00020000 RESOURCE-SID-COMPRESSION-DISABLED
```

Um am UCS Masterserver zu sehen welche Principal es der Zeit gibt, verwendest du diesen Befehl:

```
univention-s4search '(|(userPrincipalName=*)(servicePrincipalName=*))'
userPrincipalName servicePrincipalName
```

LDAP-Search in UCS mit TLS

```
ldapsearch -H ldaps://dc1.tux.lan:7636 -x -D
"uid=benno,cn=users,dc=tux,dc=lan" -W
```

Quellen

- https://help.univention.com/t/debugging-the-saml-kerbeors-authentication/8176
- https://help.univention.com/t/working-with-kerberos-principals-and-keytabs/30