NEW KEYTAB GENERATION

SAMBAXP 2025

Pavel Filipenský
Senior Software Engineer | Red Hat | Samba Team

ABOUT PAVEL

Samba maintainer together with Andreas Schneider at Red Hat since 2021

Samba Core Team member since 2022

WHAT IS KERBEROS KEYTAB

A keytab (short for “key table”) stores long-term keys for one or more principals.

```
klist -tKek /etc/krb5.keytab
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------
   1 04/04/2025 15:50:58 ADMEM$@SAMBA.ORG (aes256-cts-hmac-sha1-96)  (0xe53ebc199b9224ac92eb4035419194ce7c
   1 04/04/2025 15:50:58 host/admem.samba.org@SAMBA.ORG (aes256-cts-hmac-sha1-96)  (0xe53ebc199b9224ac92eb
   1 04/04/2025 15:50:58 host/ADMEM@SAMBA.ORG (aes256-cts-hmac-sha1-96)  (0xe53ebc199b9224ac92eb4035419194
```

Each entry consists of a timestamp (indicating when the entry was written to the keytab), a principal name, a key version number, an encryption type, and the encryption key itself.

HOW SAMBA USES KEYTAB

When SMB client accesses samba file server, the client:

- gets TGT from KDC via AS_REQ
- gets ST (service ticket) for cifs from KDC via TGS_REQ
- sends AP_REQ (with the ST) to Samba server

and Samba decrypts/verifies the ST using the Key from keytab (or from secrets.tdb)

RELATED SMB.CONF PARAMETERS

kerberos method (G)
Controls how kerberos tickets are verified.

- secrets only - use only the secrets.tdb for ticket verification (defau
- system keytab - use only the system keytab for ticket verification
- dedicated keytab - use a dedicated keytab for ticket verification
- secrets and keytab - use the secrets.tdb first, then the system keytab

Future changes: verification against a list of keytabs (for local KDC)

dedicated keytab file (G)
Specifies the absolute path to the kerberos keytab file when kerberos method is set to "dedicated keytab".

machine password timeout (G)
How often winbind should update the machine password.
The default is one week.

Not documented: the update happens only if 'secrets only' is used.

STARTED WITH BUGZILLA 6750 FROM 2009

After 'machine password timeout' /etc/krb5.keytab is not updated

It is great that samba has learned how to refresh the machine password,
but when it does this and doesn't update the /etc/krb5.keytab
it breaks every other kerberos service on the machine.

The keytab should be refreshed, but a better job is needed compared to
'net ads keytab create' the latter doesn't create entries for any
additional SPNs.

No idea how to handle multiple keytabs, my webserver for instance
has a apache-only keytab with just the various http SPNs in it.

WORKAROUNDS

- 'machine password timeout = 0'
  ... disables updating of the machine password

- 'kerberos method != secrets only' (secrets and keytab, system keytab, dedicated keytab)
  ... also disables the update

- crontab: 'net ads keytab create -P'
  ... need to compute the time of next change e.g. from 'SECRETS/MACHINE_LAST_CHANGE_TIME/' key in secrets.tdb

SYNC MACHINE PASSWORD TO KEYTAB (G)

```
"/path/to/keytab1:account_name:sync_upn:sync_spns:sync_etypes:sync_kvno:machine_password",
"/path/to/keytab2:spn_prefixes=imap,smtp:netbios_aliases:sync_kvno:machine_password",
"/path/to/keytab3:spns=wurst/brot@REALM,wurst2/brot@REALM:sync_kvno:machine_password"

[:spn_spec]+[:sync_etypes][:sync_kvno][:netbios_aliases][:additional_dns_hostnames][:machine_

account_name
sync_account_name
sync_upn
sync_spns
spn_prefixes=value1[,value2[...]]
spns=value1[,value2[...]]

sync_etypes      - "msDS-SupportedEncryptionTypes" is read from AD and is used to find the hi
                   common enc type for AD and KRB5 lib.
sync_kvno        - "msDS-KeyVersionNumber" from AD is used to set KVNO. If this option is mis
                   KVNO is set to -1.
netbios_aliases  - evaluated only for spn_prefixes
additional_dns_hostnames - evaluated only for spn_prefixes
machine_password - mandatory, if missing the entry is ignored.

(Example for future extension :gmsa_password for msDS-GroupManagedServiceAccount)
```

SYNC MACHINE PASSWORD SCRIPT (G)

```
sync machine password script (G)
     This is the full pathname to a script that will be run by winbindd(8)
     when a machine account password is updated.
```

- Machine password change triggers two keytab updates (prepare & finish phase)
- Every keytab update triggers two calls of this script (even without password change).

... more on using this in the clustered samba later

DEFAULT KEYTAB

4.20:

```
$ klist -ke /tmp/keytab |grep aes256-cts-hmac-sha1-96
   1 ADMEMIDMAPNSS$@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 host/ADMEMIDMAPNSS.addom.samba.example.com@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 host/ADMEMIDMAPNSS@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 restrictedkrbhost/ADMEMIDMAPNSS.addom.samba.example.com@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1
   1 restrictedkrbhost/ADMEMIDMAPNSS@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
```

4.21:

```
(account_name:sync_spns:spn_prefixes=host:sync_kvno)
$ klist -ke /tmp/keytab |grep aes256-cts-hmac-sha1-96
   1 ADMEMIDMAPNSS$@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 HOST/ADMEMIDMAPNSS.addom.samba.example.com@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 HOST/ADMEMIDMAPNSS@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 RestrictedKrbHost/ADMEMIDMAPNSS.addom.samba.example.com@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1
   1 RestrictedKrbHost/ADMEMIDMAPNSS@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 host/admemidmapnss.addom.samba.example.com@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
   1 host/ADMEMIDMAPNSS@ADDOM.SAMBA.EXAMPLE.COM (aes256-cts-hmac-sha1-96)
```

IMPLEMENTATION DETAILS

We store keys calculated from:
current password, old passsword, older passsword, next password

VNOs values without :sync_kvno option:
password: -1, old passsword: -2, older passsword: -3, next password: -4

If password is updated, keytab is synced twice:
when preparing password change (sending request to DC)
when finishing password change (got response from DC)

We first add new entries and then delete old entries.

without :sync_kvno it is more complicated:

- copy existing entries with VNO -1, -2, -3, -4 to VNO -11, -12, -13, -14
- remove entries with VNO -1, -2, -3, -4
- add new entries with VNO -1, -2, -3, -4
- remove old entries with VNO -11, -12, -13, -14

DEVELOPER TRACES (1/2)

```
$ net ads changetrustpw -d10 | grep KEYTAB_TRACE
prepare password change:
          operation principal VNO ETYPE KEY
KEYTAB_TRACE   nxt   COMPUTER$  -1 18    695788EAB24267...
KEYTAB_TRACE   nxt   COMPUTER$  -2 18    4E9285BB3BC959...
KEYTAB_TRACE   nxt   COMPUTER$  -3 18    16790C269F2DA4...
KEYTAB_TRACE   add   COMPUTER$ -11 18    695788EAB24267...
KEYTAB_TRACE   add   COMPUTER$ -12 18    4E9285BB3BC959...
KEYTAB_TRACE   add   COMPUTER$ -13 18    16790C269F2DA4...
KEYTAB_TRACE   rem   COMPUTER$  -1 18    695788EAB24267...
KEYTAB_TRACE   rem   COMPUTER$  -2 18    4E9285BB3BC959...
KEYTAB_TRACE   rem   COMPUTER$  -3 18    16790C269F2DA4...
KEYTAB_TRACE   add   COMPUTER$  -1 18    695788EAB24267...
KEYTAB_TRACE   add   COMPUTER$  -2 18    4E9285BB3BC959...
KEYTAB_TRACE   add   COMPUTER$  -3 18    16790C269F2DA4...
KEYTAB_TRACE   add   COMPUTER$  -4 18    56E22AEC6D5193...
KEYTAB_TRACE   rem   COMPUTER$ -11 18    695788EAB24267...
KEYTAB_TRACE   rem   COMPUTER$ -12 18    4E9285BB3BC959...
KEYTAB_TRACE   rem   COMPUTER$ -13 18    16790C269F2DA4...
```

DEVELOPER TRACES (2/2)

```
        finish password change:
KEYTAB_TRACE   nxt   COMPUTER$  -1 18    695788EAB24267...
KEYTAB_TRACE   nxt   COMPUTER$  -2 18    4E9285BB3BC959...
KEYTAB_TRACE   nxt   COMPUTER$  -3 18    16790C269F2DA4...
KEYTAB_TRACE   nxt   COMPUTER$  -4 18    56E22AEC6D5193...
KEYTAB_TRACE   add   COMPUTER$ -11 18    695788EAB24267...
KEYTAB_TRACE   add   COMPUTER$ -12 18    4E9285BB3BC959...
KEYTAB_TRACE   add   COMPUTER$ -13 18    16790C269F2DA4...
KEYTAB_TRACE   add   COMPUTER$ -14 18    56E22AEC6D5193...
KEYTAB_TRACE   rem   COMPUTER$  -1 18    695788EAB24267...
KEYTAB_TRACE   rem   COMPUTER$  -2 18    4E9285BB3BC959...
KEYTAB_TRACE   rem   COMPUTER$  -3 18    16790C269F2DA4...
KEYTAB_TRACE   rem   COMPUTER$  -4 18    56E22AEC6D5193...
KEYTAB_TRACE   add   COMPUTER$  -1 18    56E22AEC6D5193...
KEYTAB_TRACE   add   COMPUTER$  -2 18    695788EAB24267...
KEYTAB_TRACE   add   COMPUTER$  -3 18    4E9285BB3BC959...
KEYTAB_TRACE   rem   COMPUTER$ -11 18    695788EAB24267...
KEYTAB_TRACE   rem   COMPUTER$ -12 18    4E9285BB3BC959...
KEYTAB_TRACE   rem   COMPUTER$ -13 18    16790C269F2DA4...
KEYTAB_TRACE   rem   COMPUTER$ -14 18    56E22AEC6D5193...
```

MACHINE PASSWORD UPDATES TRIGGERS

- winbindd doing regular updates (machine password timeout)
- net ads/rpc changetrustpw
- rpcclient --machine-pass -c change_trust_pw
- wbinfo --change-secret

KEYTAB GENERATION TRIGGERS

- net ads join
- net ads keytab create
- net changesecretpw -f (this changes machine password only in secrets.tdb, not in DC)

UPDATING KEYTAB IN CLUSTERED SAMBA (1/2)

```
sync machine password script (G)


This is the full pathname to a script that will be run by winbindd(8)
when a machine account password is updated.  If keytabs should be generate
in clustered environments it is recommended to update them on all nodes.
You can set the config option to
/usr/share/ctdb/scripts/winbind_ctdb_updatekeytab.sh in clustering case.
It is also needed to activate the 46.update-keytabs.script in ctdb, it
re-creates the keytab during the ctdb recovered event:


onnode all ctdb event script enable legacy 46.update-keytabs.script


Example:
sync machine password script = /usr/share/ctdb/scripts/winbind_ctdb_update
```

UPDATING KEYTAB IN CLUSTERED SAMBA (2/2)

```
$ cat source3/script/winbind_ctdb_updatekeytab.sh


#!/bin/sh
onnode -p connected "net ads keytab create --option='sync machine
password script='"
```

```
$ cat ctdb/config/events/legacy/46.update-keytabs.script

#!/bin/sh
    ...
case "$1" in
recovered)
    net ads keytab create --option='sync machine password script='
    ;;
esac
```

FIXED ISSUES (1/2)

samba-4.21.1
BUG 15715: Samba 4.21.0 broke FreeIPA domain member integration.

FreeIPA in domain member configuration:

- updates the machine password
- updates the keytab
- wants samba to consume the keytab via: 'kerberos method = dedicated keyta
- calls 'net changesecretpw -f' to update the password also in secrets.tdb

But that started to fail! Since the command triggered a keytab creation
with a default content which was trying to read SPNs from a DC,
but there was no connection to DC.

Solution:
sync machine password to keytab = disabled

FIXED ISSUES (2/2)

```
samba-4.21.4:
BUG 15759: net ads create/join/winbind producing unix dysfunctional keytab


Breaks sshd for kerberos/gssapi login  (needs 'host' principal)
Breaks sssd for connecting to ldap   (needs 'COMPUTER$' principal)


Default keytab in 4.21.0: sync_spns:sync_kvno
Default keytab in 4.21.4: account_name:spn_prefixes=host:sync_spns:sync_kv

- Add new keytab specifiers  (sync_upn, sync_account_name)
- allow multiple specifiers
```