Prometheus: deleting users

This document is an attempt to provide a walkthrough of the procedure for finding accounts to delete, and deleting them.

This process be refined/partially automated as required, although it may be wise to keep it as a largely manual process.

Deletion entails removal of the user from prometheus itself and the four downstream stores that make up a DICE account (kdc, afs-pts, afs-vldb and sys-ldap). Note that it deletes the user's home directory, so use with caution.

Note that some command-line examples are split across multiple lines to aid readability

Useful background knowledge

- How prometheus lifecycle works
- Our policies for expiry (grace) and suspension periods

Selection of accounts to delete

Get a list of accounts eligible for deletion, sorted by eligible-for-deletion date:

```
prometheus-lifecycle --eligiblefordeletion --dates|sort -k5 > /tmp/eligible-for-deletion
```

This produces a file with lines in this format:

```
username: post-grace 2018-01-08 2018-09-05 2018-10-05
```

The dates here are 'account-end', 'grace-end' and 'eligible-for-deletion'. To describe these briefly:

- account-end: the date the account lost the entitlement to an account
- grace-end: account-end + grace-period
- eligible-for-deletion: account-end + grace-period + suspension period

Decide which accounts are to be deleted - this might be by selecting an arbitrary number of accounts, or by picking a date (e.g. accounts which have been eligible for deletion for 6 months). As the file generated above is ordered by eligible-for-deletion date, you can use `less -N` to display line numbers and select a cut off point.

Get a list of uuns from the file, e.g. to select the first 100 eligible accounts:

```
head -n100 /tmp/eligible-for-deletion | cut -d: -f1 > /tmp/uuns-to-delete
```

It may be wise at this stage to manually inspect the uuns marked for deletion.

Things you might want to check first

Backups

It might be worth checking that accounts to be deleted have been backed up. This can be done by using the `afsrest` command on the backup server (currently `pergamon`). First...

```
[pergamon]toby: nsu
[pergamon]root: . /etc/tibs.conf
[pergamon]root:
```

For a single user, `afsrest -q user.<uun>`

The `-q` option is documented in `man afsrest`:

```
 -q     Query restore. Used to find out what tapes perform a restore request.
```

To get backup details for a file of uuns, the following command will generate last backup details for each user, and put them in a file:

```
for i in $(cat /tmp/uuns-to-delete |xargs); do
 echo -n "$i: ";
 afsrest -q -n user.$i 2>&1|grep '^[0-9]';
done > /tmp/uuns-to-delete.afsrest
```

This file can then be checked to make sure that every user has a 'full' backup.

Downstream stores

A script called `downstream-store-summary` can be found in the co utils group space. This can be used to check on the existence of downstream store objects. e.g. using the file of uuns generated above (note that you have to `asu` to use this command):

```
for i in $(cat /tmp/uuns-to-delete |xargs); do
 /afs/inf.ed.ac.uk/group/cos/utils/prometheus/downstream-store-summary $i;
done > /tmp/uuns-to-delete.dss
```

There should be a line for every user looking like this:

```
<uun>: kdc(disabled) afs-pts afs-vldb sys-ldap
```

Prepare for deletion

There are a few stages to deleting accounts. They must all be done as an `/admin` principal, so authenticate with `asu` first. If you are deleting a large number of user accounts in one go, factor in that the maximum ticket lifetime for the `kadmin/admin` principal is 3 hours. You will not be able to make changes to the KDC once this ticket has expired.

Firstly, the prometheus objects need to have the account-granting entitlement(s) manually removed - if this is not done, the `delete-user` script will refuse to proceed. This can be done with the following command:

```
prometheus-lifecycle --removeallfixedentitlements --user <uun>
```

This can be done for a file of uuns, as generated above with:

```
for i in $(cat /tmp/uuns-to-delete|xargs); do
 prometheus-lifecycle --removeallfixedentitlements --user $i;
done
```

Before proceeding with deletions, the role expander conduit needs to run. This happens approximately hourly on week days, so the above can be done suitably in advance. However, it can also be run on demand using prometheus's eventqueue. For a single user:

```
prometheus-eventqueue --add Prometheus::Conduits::RoleExpander --args username=<uun>
```

To run it for all users, omit the `--args` argument, e.g.

```
prometheus-eventqueue --add Prometheus::Conduits::RoleExpander
```

The full run of the conduit takes about two to three minutes.

Progress can be tracked by using `tail -f /var/lcfg/log/prometheus.eventqueue` on the prometheus server (currently `redding`). An example of the above running to completion would look like this:

```
2019-02-07_15:46:04:255474
Running event: 625b2967c634d134982a219698e44239
Conduit: Prometheus::Conduits::RoleExpander
2019-02-07_15:47:59:719958
Deleting event: 625b2967c634d134982a219698e44239
```

The `Deleting event` line indicates that the event has completed.

Deletion

The next stage is to run the delete-user script. This does the following:

- deletes the user's afs-vldb entry and home directory
- deletes the user's afs-pts entry
- deletes the user's LDAP entry
- deletes the user's KDC entry

- deletes the user's identity and account objects from prometheus, leaving just a stub entity

`delete-user` can be found in the co utils group space:

```
/afs/inf.ed.ac.uk/group/cos/utils/prometheus/delete-user
```

It takes a single uun as the argument, so to delete a single user:

```
/afs/inf.ed.ac.uk/group/cos/utils/prometheus/delete-user <uun>
```

Or, for a file of uuns, as generated above:

```
for i in $(cat /tmp/uuns-to-delete|xargs); do
 /afs/inf.ed.ac.uk/group/cos/utils/prometheus/delete-user $i;
done
```

This generates a lot of output telling you what it's doing. It can also be quite slow - ~20s per user.

Finally, the remaining entity objects should be deleted from prometheus. This can be done using the `delete-entity-by-uun` script in the co utils directory.

So for a single user:

```
/afs/inf.ed.ac.uk/group/cos/utils/prometheus/delete-entity-by-uun <uun>
```

Or, for a file of uuns, as generated above:

```
for i in $(cat /tmp/uuns-to-delete|xargs); do
 /afs/inf.ed.ac.uk/group/cos/utils/prometheus/delete-entity-by-uun $i;
done
```

-- TobyBlake - 09 Oct 2018

This topic: DICE > PrometheusDeletingUsers
Topic revision: r5 - 07 Feb 2019 - 15:48:26 - TobyBlake