Final project report for "Account Tidying" (349)

Project Description

Following on from the our data tidy-up and implementation of prometheus lifecycle, we now have a large number of accounts which are disabled. We need to tidy up these and establish, and automate where possible, the processes for what happens in the future.

In the following text, "downstream accounts" refers to entries in the KDC, AFS-PTS, AFS-VLDB (and home directory data) and "System" LDAP (rfe 2307).

The following steps should be taken:

- Firstly, communicate our account deletion policy to all users.
- Establish, and fix if necessary, what discrepancies we have between prometheus data and downstream accounts.
- Decide what to do with user data which is not in home directories.
- Delete all downstream accounts which predate implementation of lifecycle.
- Ensure we have adequate tools and reporting for dealing with post-grace/post-suspension accounts.
- Decide what data, if any, we keep in prometheus following account deletion.

It's envisaged that this project will be cross-unit, involving infrastructure, user support and services.

Project page

Project updates

Implementation

The work undertaken on this project is detailed on the updates page. This report will not repeat this information, but will instead summarise matters with respect to the steps identified in the original project description.

Firstly, communicate our account deletion policy to all users.

We have a number of user-facing documention pages which explain our user account policies. The project felt that existence of the pages did not necessarily mean that users had read them, so we agreed that a regular informational email should be sent to sys-announce. The email looks like this.

This email will be sent twice-yearly, towards the beginning of each semester (mid-October and mid-February). The first such email was sent on 7th February 2019.

Establish, and fix if necessary, what discrepancies we have between prometheus data and downstream accounts.

Delete all downstream accounts which predate implementation of lifecycle.

These two issues were inter-related. The introduction of prometheus lifecycle in January 2015 meant that, from that point on, all expired accounts were in a consistent state, had been through a grace period, and had expiry dates kept in prometheus. Anything prior to this was less constrained, even considering that prometheus was itself seeded with data from downstream LDAP.

All downstream user accounts are now consistent with the data held in prometheus.

Decide what to do with user data which is not in home directories.

This is a bit of a thorny issue. See this and this for a description of this problem. This project recommends that this be forked into a separate project, or is dealt with operationally within the Services unit

Ensure we have adequate tools and reporting for dealing with post-grace/post-suspension accounts.

The prometheus-lifecycle command line tool provides details of accounts that have expired (both in grace period and beyond). The new `--eligiblefordeletion` flag now reports on all accounts which have gone past their suspension period and hence can be considered for deletion.

A page has been written to summarise the steps in deleting users.

It is the intention that tools and documentions will be revised in conjunction with us-unit, as appropriate.

Decide what data, if any, we keep in prometheus following account deletion.

We will keep no data in prometheus following account deletion.

Summary of deletions

- 6616 prometheus entities with no downstream objects
- 3213 afs-pts entries and prometheus entities with no identity object
- 729 downstream account objects which were not in prometheus (mostly <= 2011)
- 3052 accounts which expired prior to lifecycle (introduced 2015-01-24)
- 1035 unactivated accounts which are no longer entitled to an account (all unused and with empty home directories)
- 2539 accounts (post-lifecycle)

At time of writing, there are 1590 accounts eligible for deletion.

Effort spent

The project took approximately 165 hours in total.

Future Considerations

Much of the work in this project has taken place within the infrastructure unit. Ongoing account deletions will take place, regularly, as a collaboration between inf-unit and us-unit to aid with knowledge transfer and ensure that procedures and documentation are adequate.

This project identified the need to consider file system implications for deleted accounts, both in terms of files left in areas outwith user home directories and in AFS ACLs. It was considered outwith the scope of this project to address this, but it should not be forgotten about. It is recommended that a separate project be created.

Prometheus has some support for multiple identities and accounts for people, and also for machines and standalone entities, with more support to come. Deletion of accounts for people with multiple identities/accounts should just work. Host-based and other accounts will need to be dealt with separately.

-- TobyBlake - 07 Feb 2019

This topic: DICE > FinalProjectReport349
Topic revision: r2 - 07 Feb 2019 - 16:31:06 - TobyBlake