Pre-Seeding Users for First Boot

Jakub Hrozek

January 2013

Centralized user accounts

- Companies tend to centralize their user accounts instead of using machine-local accounts stored directly on the clients
    - Allows for centralized distribution of UIDs/GIDs
    - Centralized account control, password policies, ...
- The identity servers are a critical part of corporate infrastructure
    - Usually reachable on internal network or VPN only
- Credentials must be cached for logins from outside the internal network

Authenticating using cached credentials

- The SSSD can authenticate a roaming user even without having access to the identity server using cached credentials
- The cached credential is typically a hashed user password stored during the last online login
- Stored in the sssd cache when the `cache_credentials` option is set to `true`

Cached credentials for firstboot

- First time logins may pose a chicken-and-egg problem if performed outside VPN
- Scenario: A remote user is mailed a laptop and needs to login
- How do they authenticate using cached credentials before they are able to cache their credentials?
  - The credentials need to be **pre-seeded** for the first time login to work

Preseeding credentials using sss_seed

- The sss_seed utility can be used to create an entry in the SSSD cache along with a cached password
- The pre-seeded password does not have to be the same as the real one
  - The first online authentication would overwrite the pre-seeded password with a real one
- Can be run manually after a new system is installed or in a kickstart in the %post section
- sss_seed should be ran after the SSSD is configured so that the SSSD config file is already present

sss_seed interactive example

- Use case: IT engineer prepares the laptop before shipping it to a remotee
- If the user information (UID, GID, shell) can be obtained from the directory, it will be used automatically
- In that case, the user only needs to provide the password to preseed

```
# sss_seed -i -n jdoe -D example.com
Enter temporary password:
Enter temporary password again:
Temporary password added to cache entry for jdoe
```

sss_seed interactive example

- If the information cannot be retrieved from the directory, they can be prompted for interactively

```
# sss_seed -i -n jdoe -D example.com
Enter UID:12345
Enter GID:54321
Enter user comment (gecos):John Doe
Enter home directory:/home/jdoe
Enter user login shell:/bin/bash
Enter temporary password:
Enter temporary password again:
User cache entry created for jdoe
Temporary password added to cache entry for jdoe
```

sss_seed non-interactive example

- Add a user automatically
  - Use case: in kickstart during the `%post` phase
- Should be ran after `authconfig` as the SSSD config file needs to be generated first

-
  ```
  # sss_seed -D example.com -u 12345 -g 54321 -n jdoe -c
  "John Doe" -s /bin/sh -p /root/jdoe.pwd
  ```
- If not provided with the `-p` option, the password will be prompted for interactively