

NSS + GDM Issue

1. GDM Requests a Dynamic User

When GDM starts up it attempts to launch the graphical login screen. For security isolation GDM requests a session for a systemd dynamic user named `gdm-greeter` from `systemd-logind`.

- Systemd dynamically allocated a UID (60578 in this case) and registered the username `gdm-greeter` to it.
- Logind triggers the creation of the user's slice and runtime directory

```
systemd[1]: Created slice User Slice of UID 60578.  
systemd-logind[426]: New session '1' of user 'gdm-greeter' with class 'greeter' and  
type 'wayland'.
```

2. Systemd Spawns the User Manager and Invokes PAM

To run the background GNOME session, systemd attempts to spawn the per-user systemd instance (`user@60578.service`).

Before launching the service, systemd must authenticate and initialize the user's environment using the PAM stack configured in `/etc/pam.d/systemd-user` (which inherits `/etc/pam.d/system-auth`).

3. pam_sss.so Gracefully Rejects the Dynamic User

First, the account block in the PAM stack runs `pam_sss.so`:

```
account    sufficient                                pam_sss.so
```

- `pam_sss` queries the SSSD daemon: "Do you have a user named `gdm-greeter`?"
- SSSD queries your LDAP server and finds nothing. SSSD replies: "No, this user is unknown to me."
- This generates the log entry:

```
1 (systemd)[508]: pam_sss(systemd-user:account): Access denied for user gdm-greeter: 10  
(User not known to the underlying authentication module)
```

- Because `pam_sss` is configured as `sufficient`, its failure is non-fatal. PAM ignores this rejection and falls through to the next module in the stack: `pam_unix.so`.

4. pam_unix.so Spawns unix_chkpwd

To verify the local account, pam_unix.so spawns the setuid helper binary /usr/bin/unix_chkpwd to check the user's password and shadow database info:

```
1 account      required                pam_unix.so
```

5. The Silent NSS Database Lookup Failure

Inside the C code of /usr/bin/unix_chkpwd, the program makes a standard glibc library call to look up the shadow password entry for the username:

```
1 getsnam("gdm-greeter");
```

To resolve this call, glibc reads your `/etc/nsswitch.conf` file to see which databases are registered under the shadow: line. It saw:

```
1 shadow: compat sss
```

Glibc began querying the modules in order:

1. compat (local files): It searched /etc/shadow for an entry starting with gdm-greeter:. Since gdm-greeter is a dynamic user, no such line exists in /etc/shadow. This returns:

```
NSS_STATUS_NOTFOUND.
```

2. sss (SSSD): It asked SSSD if it has a cached shadow record for gdm-greeter. SSSD does not. This returns NSS_STATUS_NOTFOUND.

Because systemd was missing from that line, glibc reached the end of the databases and stopped. It never queried nss-systemd (which is the only place where GDM's dynamic users are registered).

As a result, getsnam("gdm-greeter") returned NULL (No such entry).

6. PAM Crashes, Locking Out the Session

- unix_chkpwd realized it was completely blind to this user and threw an error:

```
unix_chkpwd[509]: could not obtain user info (gdm-greeter)
```

- Because unix_chkpwd failed, pam_unix.so returned a fatal error to PAM.
- Because pam_unix.so is required, the entire PAM transaction aborted:

```
(systemd)[508]: PAM PAM failed: Authentication service cannot retrieve authentication info
```

- Systemd saw the PAM initialization failure and immediately aborted spawning the user manager:

```
(systemd)[508]: user@60578.service: Failed to set up PAM session: Operation not permitted
(systemd)[508]: user@60578.service: Failed at step PAM spawning /usr/lib/systemd/systemd:
Operation not permitted
systemd[1]: Failed to start User Manager for UID 60578.
```

7. Crash and Lockout

Without a running systemd --user manager for UID 60578, the user-level D-Bus broker (org.freedesktop.systemd1) was never launched.

When the GDM Wayland session tried to initialize gnome-session, it attempted to talk to the systemd user manager over D-Bus. This lookup failed, causing the greeter worker to throw an unhandled assertion and crash (dumping core):

```
gnome-session-i[518]: Failed to start unit gnome-session@gnome.target:
GDBus.Error:org.freedesktop.DBus.Error.NameHasNoOwner: Name "org.freedesktop.systemd1" does
not exist
systemd-coredump[527]: Process 518 (gnome-session-i) of user 60578 dumped core.
```

GDM attempted to restart this sequence six times, failing every time, until it reached its failure threshold:

```
gdm[455]: Gdm: GdmLocalDisplayFactory: maximum number of display failures reached. Giving up.
```

At this point, GDM completely gave up on opening any graphical interfaces on your screen, leaving the system stuck in the console/tty mode.

By adding systemd back to the shadow: line in /etc/nsswitch.conf, the glibc call getsppam("gdm-greeter") was able to query nss-systemd, retrieve the dynamic user's shadow record, pass the PAM stack, start the user manager, and successfully launch the login screen.

Revision #1

Created 2026-07-17 12:48:22 UTC by admin

Updated 2026-07-17 13:07:26 UTC by admin