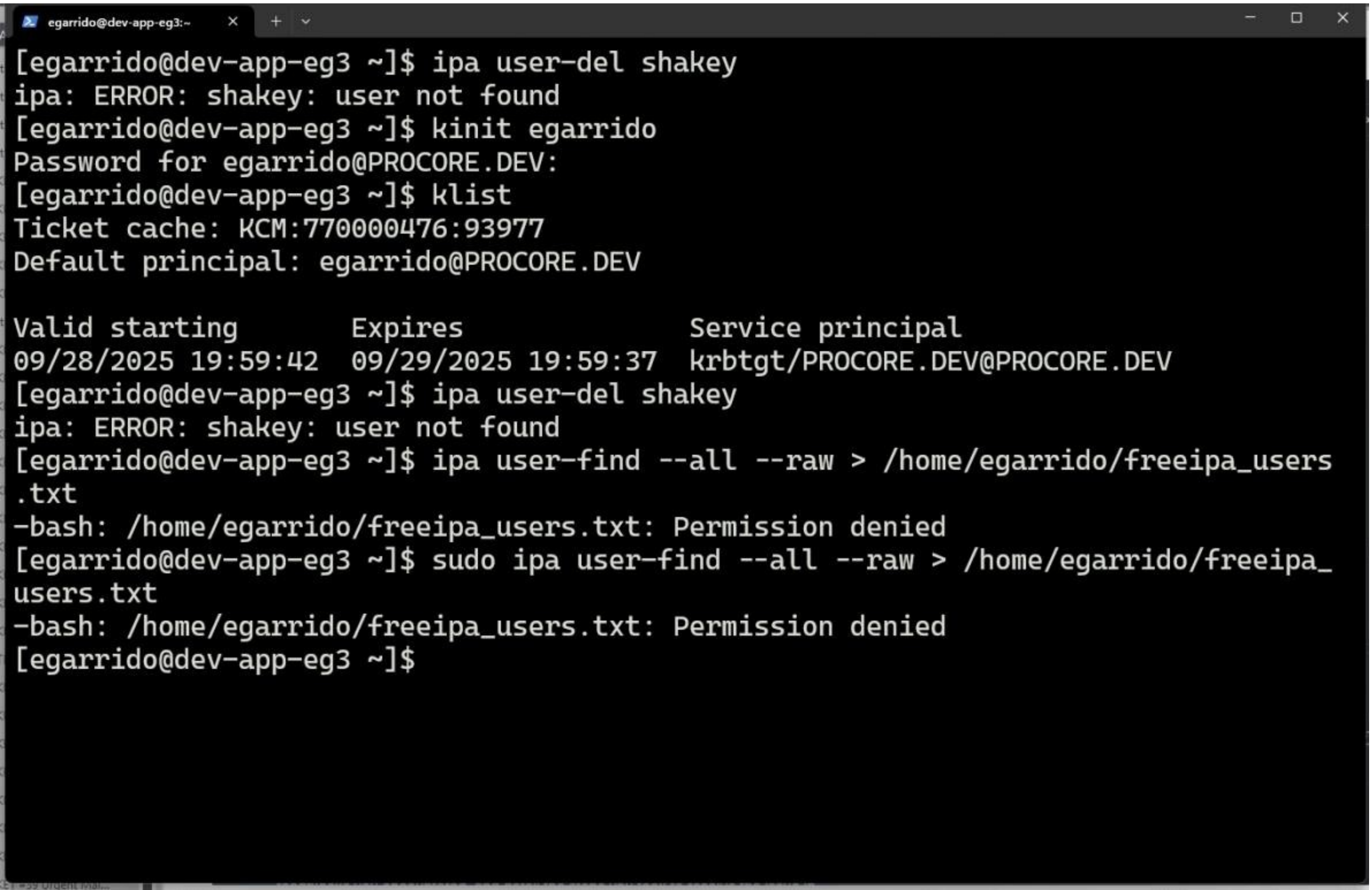
System Services and Identity Management Validation

This work focuses on validating core Linux services and centralized identity management in an enterprise-style environment. Key system components were verified to ensure consistency between installed packages, running services, and underlying operating system versions, reinforcing platform reliability across environments.

Identity and authentication workflows were examined through interaction with a centralized directory service. User account queries, Kerberos authentication validation, and directory attribute inspection confirm proper integration between client systems and the identity provider. Group membership, privilege assignments, and policy metadata were reviewed to ensure access controls are correctly applied and enforced.

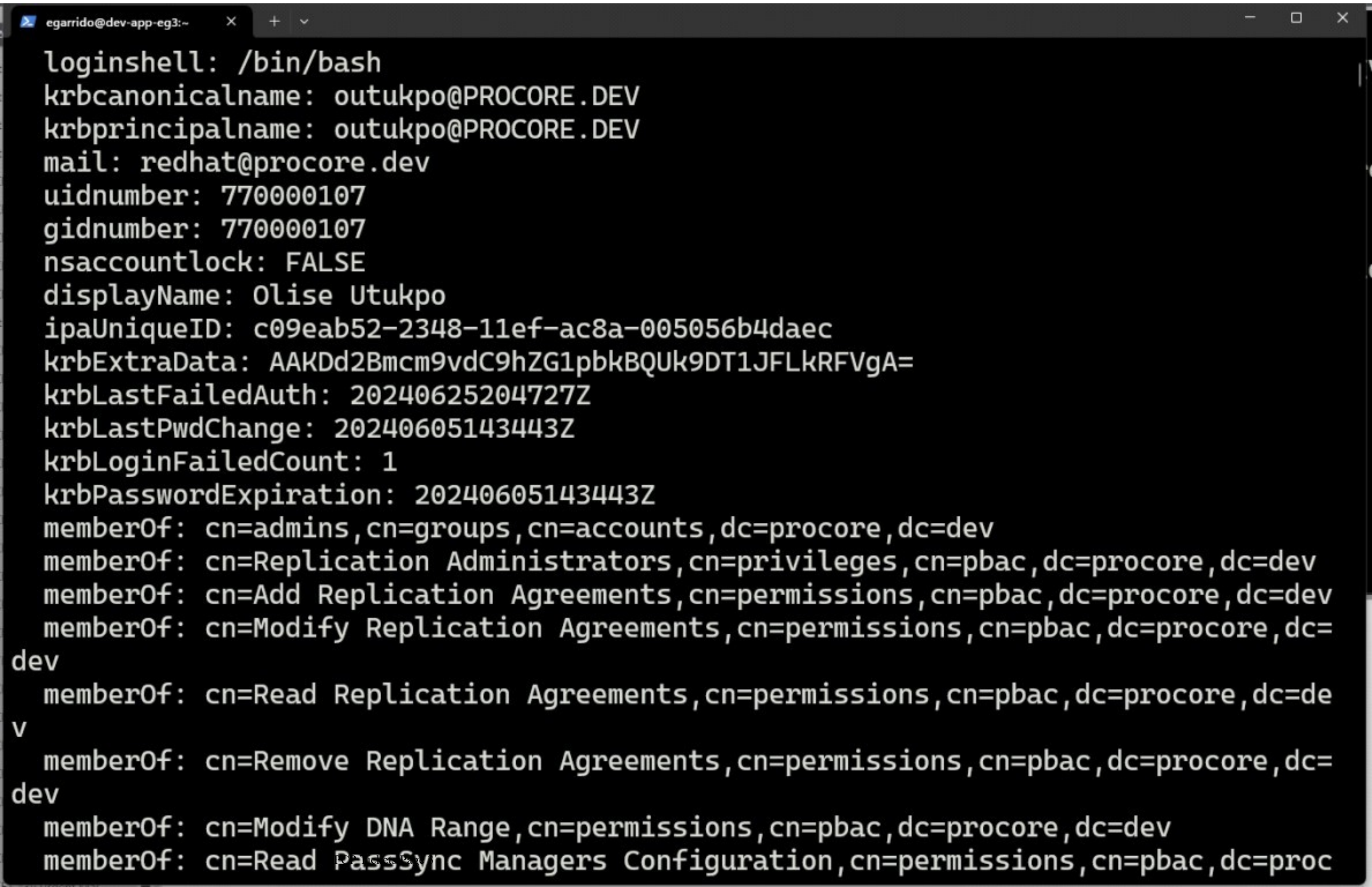
Together, these activities demonstrate practical system administration tasks including service verification, authentication troubleshooting, directory inspection, and permission awareness. The results provide confidence in system readiness, authentication reliability, and adherence to standard enterprise Linux and identity management practices.

The session shows an attempt to remove a FreeIPA user that does not exist in the directory, followed by a successful Kerberos authentication using a valid domain account. The active Kerberos ticket cache is displayed, confirming a valid Ticket Granting Ticket for the domain. Subsequent user enumeration commands demonstrate directory visibility, while permission-denied errors during output redirection highlight standard Linux file ownership and write-permission enforcement.



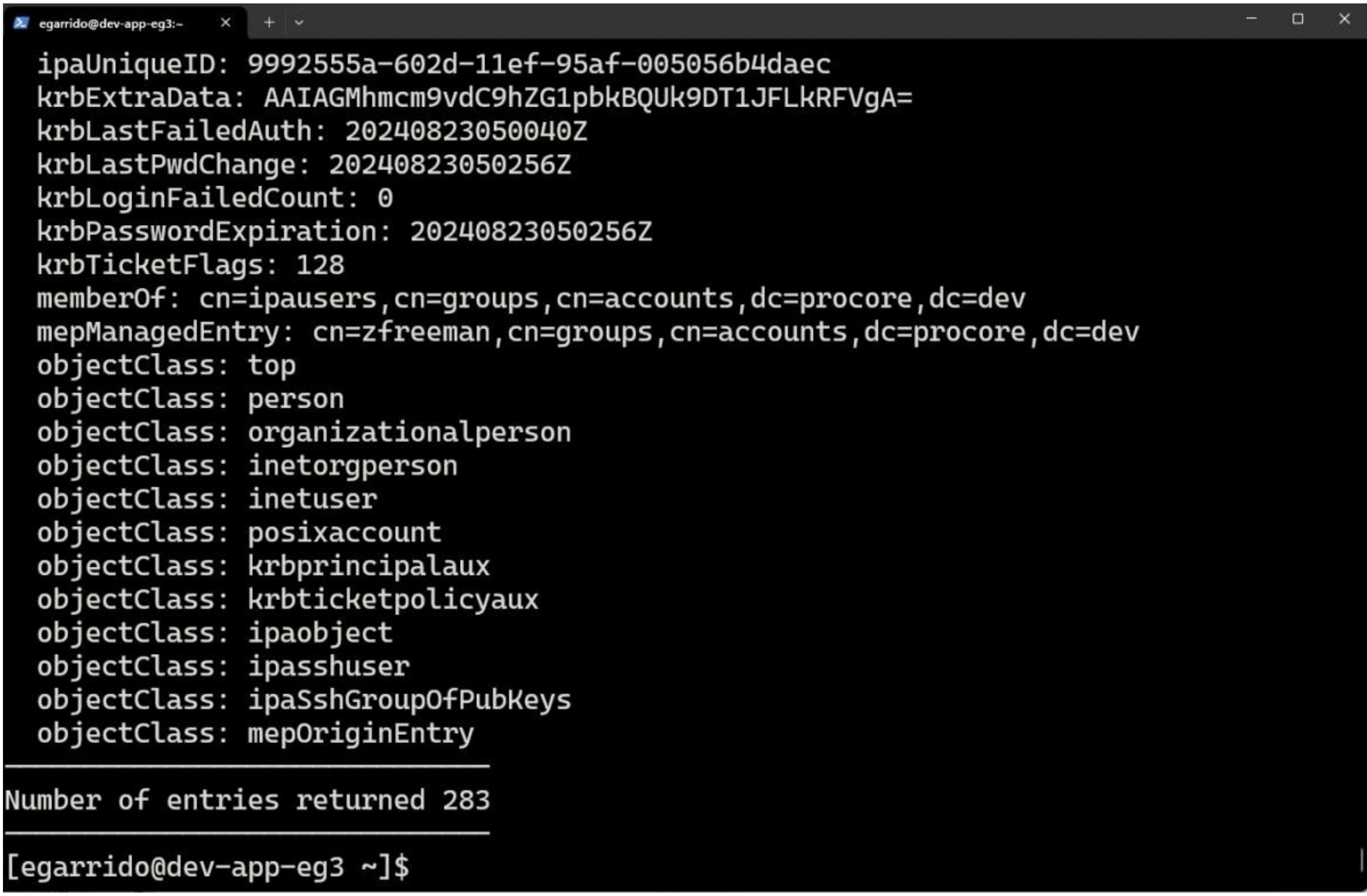
```
[egarrido@dev-app-eg3 ~]$ ipa user-del shakey
ipa: ERROR: shakey: user not found
[egarrido@dev-app-eg3 ~]$ kinit egarrido
Password for egarrido@PROCORE.DEV:
[egarrido@dev-app-eg3 ~]$ klist
Ticket cache: KCM:770000476:93977
Default principal: egarrido@PROCORE.DEV

Valid starting       Expires              Service principal
09/28/2025 19:59:42  09/29/2025 19:59:37  krbtgt/PROCORE.DEV@PROCORE.DEV
[egarrido@dev-app-eg3 ~]$ ipa user-del shakey
ipa: ERROR: shakey: user not found
[egarrido@dev-app-eg3 ~]$ ipa user-find --all --raw > /home/egarrido/freeipa_users
.txt
-bash: /home/egarrido/freeipa_users.txt: Permission denied
[egarrido@dev-app-eg3 ~]$ sudo ipa user-find --all --raw > /home/egarrido/freeipa_
users.txt
-bash: /home/egarrido/freeipa_users.txt: Permission denied
[egarrido@dev-app-eg3 ~]$
```

The output shows detailed FreeIPA user account attributes, including the assigned login shell, Kerberos principal information, email address, UID and GID values, and account lock status. It also displays authentication metadata such as last successful and failed login attempts, password change and expiration timestamps, and failure counts. The lower portion lists group and privilege memberships, indicating administrative and replication-related roles assigned to the account within the FreeIPA domain.



```
  loginshell: /bin/bash
  krbcanonicalname: outukpo@PROCORE.DEV
  krbprincipalname: outukpo@PROCORE.DEV
  mail: redhat@procore.dev
  uidnumber: 770000107
  gidnumber: 770000107
  nsaccountlock: FALSE
  displayName: Olise Utukpo
  ipaUniqueID: c09eab52-2348-11ef-ac8a-005056b4daec
  krbExtraData: AAKDd2Bmcm9vdC9hZG1pbkBQUk9DT1JFLkRFVgA=
  krbLastFailedAuth: 20240625204727Z
  krbLastPwdChange: 20240605143443Z
  krbLoginFailedCount: 1
  krbPasswordExpiration: 20240605143443Z
  memberOf: cn=admins,cn=groups,cn=accounts,dc=procore,dc=dev
  memberOf: cn=Replication Administrators,cn=privileges,cn=pbac,dc=procore,dc=dev
  memberOf: cn=Add Replication Agreements,cn=permissions,cn=pbac,dc=procore,dc=dev
  memberOf: cn=Modify Replication Agreements,cn=permissions,cn=pbac,dc=procore,dc=
dev
  memberOf: cn=Read Replication Agreements,cn=permissions,cn=pbac,dc=procore,dc=de
v
  memberOf: cn=Remove Replication Agreements,cn=permissions,cn=pbac,dc=procore,dc=
dev
  memberOf: cn=Modify DNA Range,cn=permissions,cn=pbac,dc=procore,dc=dev
  memberOf: cn=Read PassSync Managers Configuration,cn=permissions,cn=pbac,dc=proc
```

Extended FreeIPA directory attributes are displayed for a user account, including unique identifiers, Kerberos authentication and password policy metadata, and group membership within the domain. The listing confirms the account is associated with standard LDAP object classes for POSIX users, Kerberos principals, SSH access, and IPA-specific schema, followed by a summary showing the total number of entries returned by the directory query.



```
  ipaUniqueID: 9992555a-602d-11ef-95af-005056b4daec
  krbExtraData: AAIAGMhmcm9vdC9hZG1pbkBQUk9DT1JFLkRFVgA=
  krbLastFailedAuth: 20240823050040Z
  krbLastPwdChange: 20240823050256Z
  krbLoginFailedCount: 0
  krbPasswordExpiration: 20240823050256Z
  krbTicketFlags: 128
  memberOf: cn=ipausers,cn=groups,cn=accounts,dc=procore,dc=dev
  mepManagedEntry: cn=zfreeman,cn=groups,cn=accounts,dc=procore,dc=dev
  objectClass: top
  objectClass: person
  objectClass: organizationalperson
  objectClass: inetorgperson
  objectClass: inetuser
  objectClass: posixaccount
  objectClass: krbprincipalaux
  objectClass: krbticketpolicyaux
  objectClass: ipaobject
  objectClass: ipasshuser
  objectClass: ipaSshGroupOfPubKeys
  objectClass: mepOriginEntry
------------------------------
Number of entries returned 283
------------------------------
[egarrido@dev-app-eg3 ~]$
```

Summary

Core web services and identity management components were validated across the environment. Apache HTTP Server installation and version consistency were confirmed using both binary inspection and package verification to ensure alignment with the operating system.

Centralized authentication was tested through Kerberos ticket acquisition and validation, confirming successful integration with the identity provider. Directory queries were used to inspect user accounts, group memberships, and policy attributes, providing visibility into access controls and authentication behavior.

These steps demonstrate routine enterprise Linux administration practices, including service verification, identity troubleshooting, and directory inspection, helping ensure system reliability, secure access, and operational consistency.