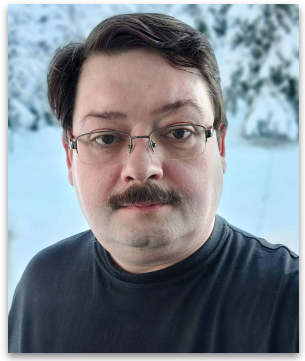
Red Hat Summit

Experiencing FreeIPA before RHEL Identity Management

Integration with Keycloak



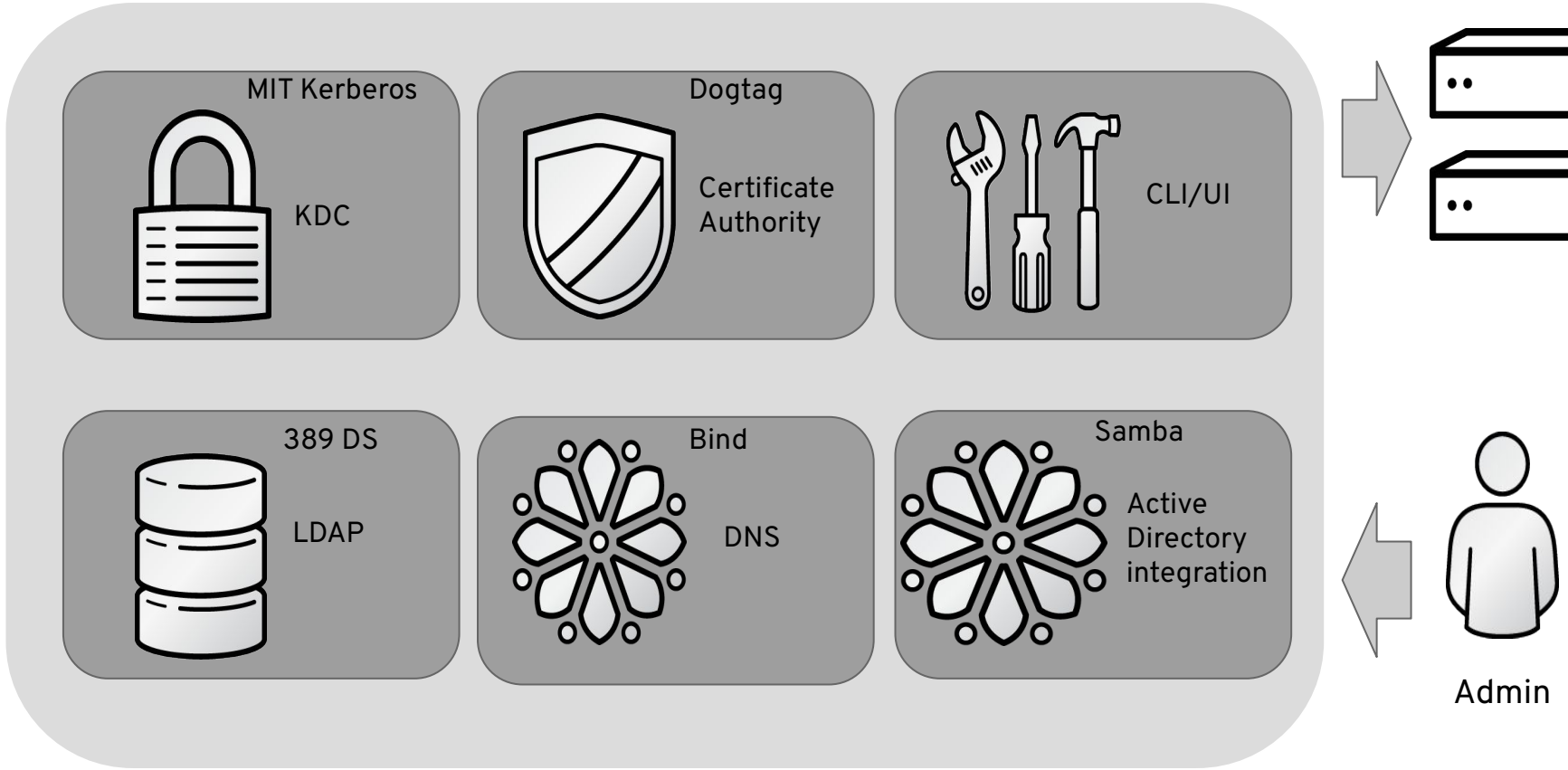
Alexander Bokovoy,
Senior Principal
Software Engineer

Red Hat

FreeIPA: upstream to RHEL Identity Management

FreeIPA (IdM) deployment	Organization domain + domain controllers + enrolled client systems
Organization domain	Kerberos realm: users + hosts + services
Domain controller	Kerberos KDC + LDAP server datastore + optional services + management tools
Optional services	Certificate Authority and its services, DNS server, Active Directory integration
LDAP datastore	users, groups, machines, Kerberos services, SUDO rules, HBAC rules, certificates, ...
Enrolled client system	Kerberos client + LDAP client (SSSD) + domain access control
Domain access control	groups, host-based access control (HBAC), SUDO rules, Kerberos ticket properties

FreeIPA domain controller

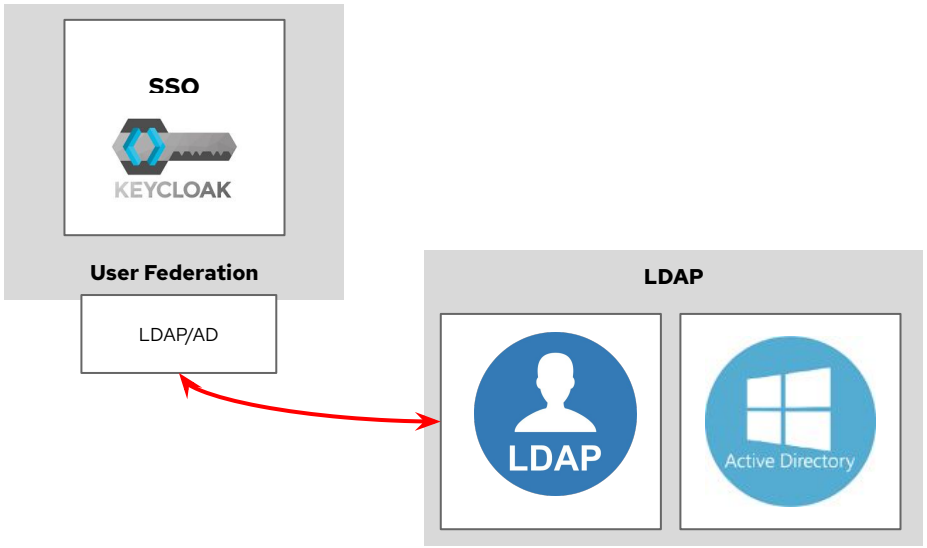


https://access.redhat.com/articles/1586893

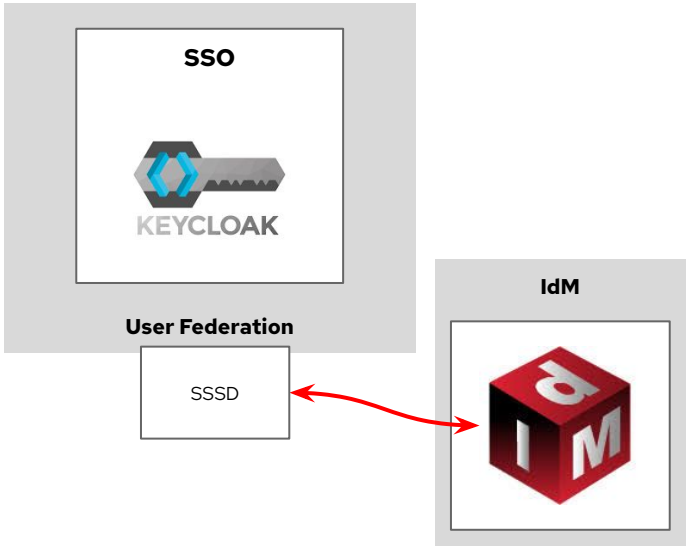
FreeIPA integration with Keycloak

Traditional Keycloak integration options

- Treat FreeIPA as an LDAP store for Keycloak identities
  - Allows to read and write users and groups



- Use SSSD Keycloak integration to lookup identities in IPA domain
  - Read-only access to users and groups
  - Support for complex AD integration options



Red Hat

FreeIPA integration with Keycloak

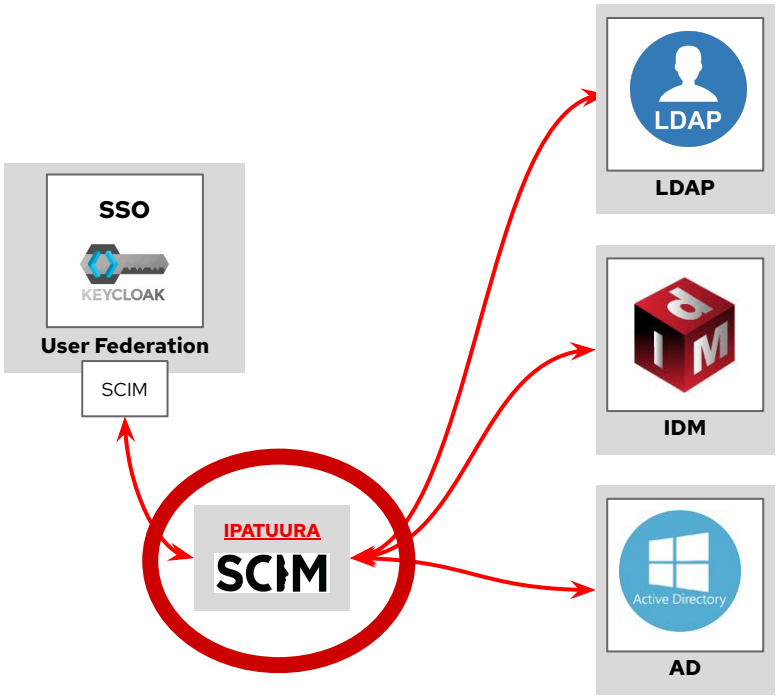
Gaps

- SSSD/IdM and LDAP/AD integrations offer different features - missing feature parity
- Existing SSSD federation plugin is read-only, requires java dbus libraries and UNIX sockets
- Limitations for deployment in containers
- Complicated setup steps required

FreeIPA integration with Keycloak

New approach: SCIM v2-based ipa-tuura
https://github.com/freeipa/ipa-tuura/

- Keycloak plugin
  - Accesses `ipa-tuura` (Bridge service) over HTTPS to /scim/v2 specification endpoints
  - No direct communication with the backend servers (FreeIPA, AD, LDAP).
  - Pass-through authentication to `ipa-tuura`
- `ipa-tuura`
  - Translates SCIMv2 endpoint requests into identity provider operations on the backend.
    - Uses SSSD and direct IPA API calls
  - Custom REST API for authentication needs
    - Supports password- and Kerberos authentication



Red Hat

FreeIPA integration with Keycloak

Keycloak plugin

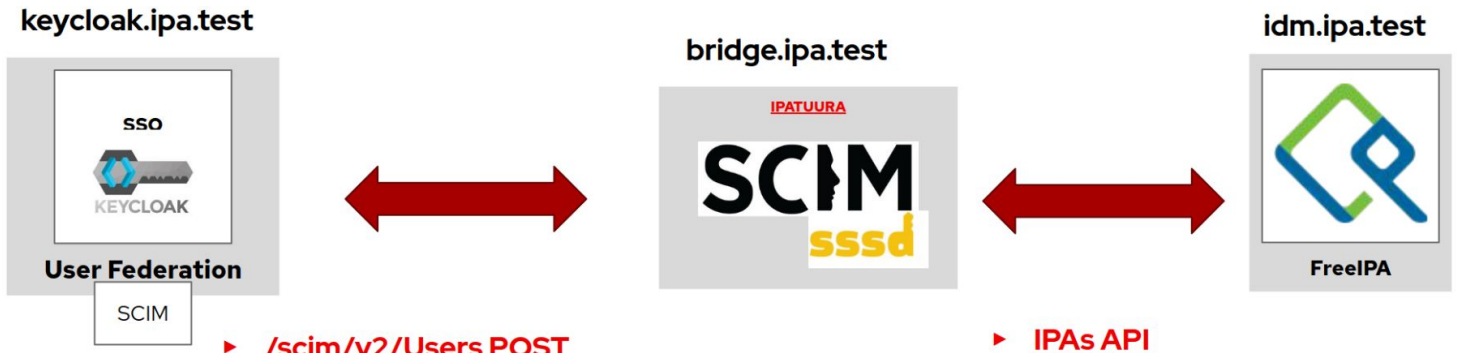
- Merged upstream in Keycloak 26.2.0
  - https://github.com/keycloak/keycloak/tree/main/federation/ipatuura
    - Quick-start guide is provided above
  - Available in quay.io/keycloak/keycloak:latest image as experimental feature
    - `kc.sh [build|start] --features=ipa-tuura-federation …`

`ipa-tuura` container image

- Available in quay.io/freeipa/ipa-tuura:latest

FreeIPA integration with Keycloak

- `ipa-tuura` handles both directions
  - Pull users and groups from FreeIPA and AD via SSSD
  - Add/modify users in FreeIPA via IPA API
  - Add/modify users in Active Directory via LDAP



▸ /scim/v2/Users POST

```
{
  "userName": "testuser",
  "emails": [
    {
      "primary": true,
      "type": "work",
      "value": "testuser@ipa.test"
    }
  ],
  "name": {
    "formatted": "testuser",
    "familyName": "user",
    "givenName": "test"
  },
  "externalId": "testuser",
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:User"
  ],
  "meta": {
    "resourceType": "User"
  }
}
```

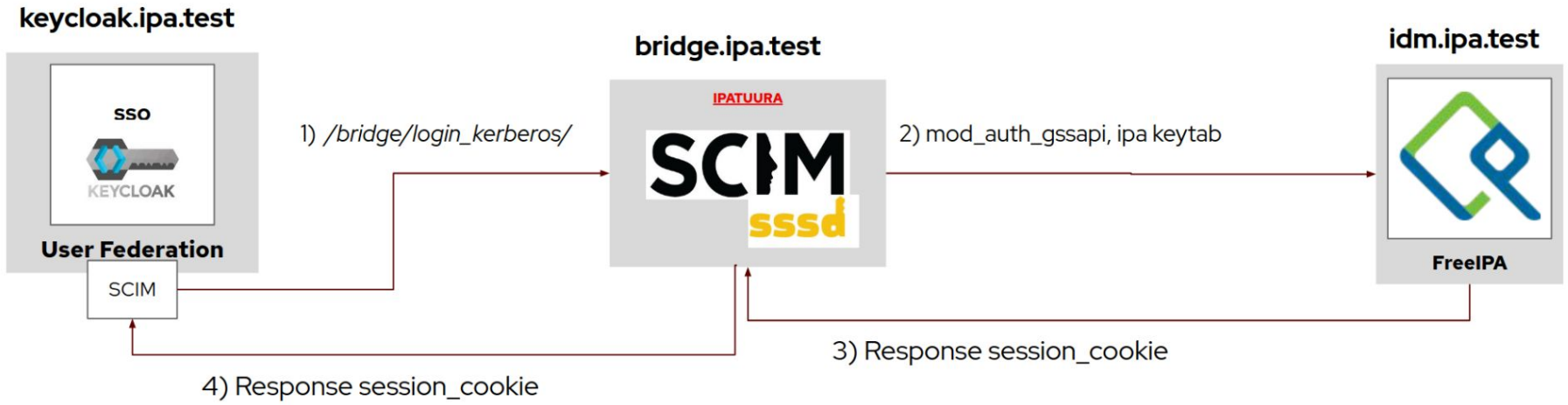
▸ IPAs API

```
api.Command.user_add("ipauser", givenname="ipa", sn="user")
"result": {
    "displayname": ["ipa user"],
    "cn": ["ipa user"],
    "gidnumber": ["1445000004"],
    "mail": ["ipauser@ipa.test"],
    "krbprincipalname": [ipapython.kerberos.Principal("test@IPA.TEST")],
    "loginshell": ["/bin/sh"],
    "initials": ["iu"],
    "uid": ["ipauser"],
    "uidnumber": ["1445000004"],
    ...
    ...
    "dn": ipapython.dn.DN("uid=test,cn=users,cn=accounts,dc=ipa,dc=test"),
```

FreeIPA integration with Keycloak

Authentication support is bridged through the `ipa-tuura`

- password-based authentication via PAM stack and `pam_sss`
  - Works for FreeIPA 2FA OTP authentication as well
- Kerberos authentication
  - Bridge owns the Kerberos service for Keycloak
  - Keycloak passes through the request
  - Bridge authenticates against IPA or AD
  - Keycloak passes back the response



Red Hat

FreeIPA integration with Keycloak

- Demo labs for Keycloak integration
  - FreeIPA local tests Keycloak/ipa-tuura
    - Work in progress
    - Creates new IPA deployment
    - Provisions Keycloak instance
    - Provisions `ipa-tuura` bridge
  - FreeIPA local tests for Keycloak as external IdP
    - Creates new IPA deployment
    - Provisions Keycloak instance
    - Configures Keycloak as an external Identity Provider for IPA users
    - Demonstrates how to obtain Kerberos ticket in IPA using Keycloak

Red Hat Summit

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat