Red Hat Summit

Experiencing FreeIPA before RHEL Identity Management

Trust between IdM deployments

Alexander Bokovoy,

Senior Principal

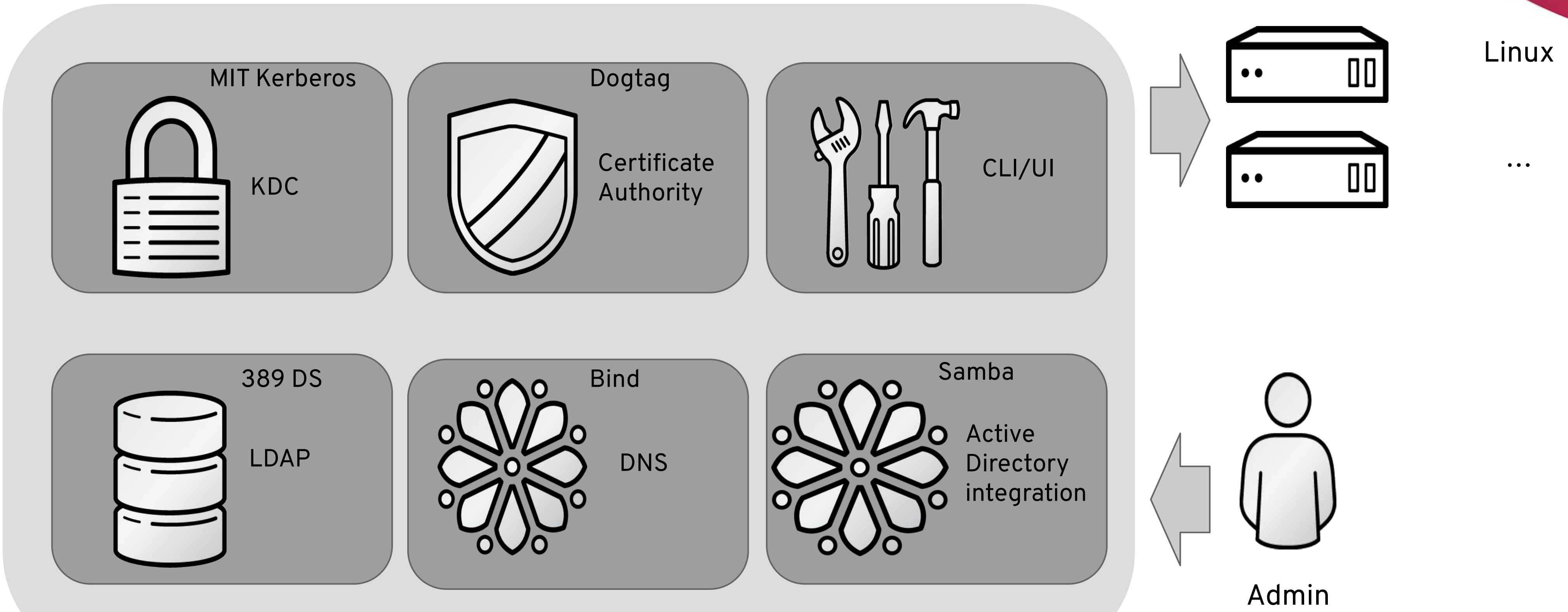
Software Engineer

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

Demo setup

Fedora 42+ VM as the main host with sufficient RAM

https://github.com/freeipa/freeipa-local-tests/tree/main/ipalab-config/ipa-trust

To access a shell in the container(s), find IP address, browser:

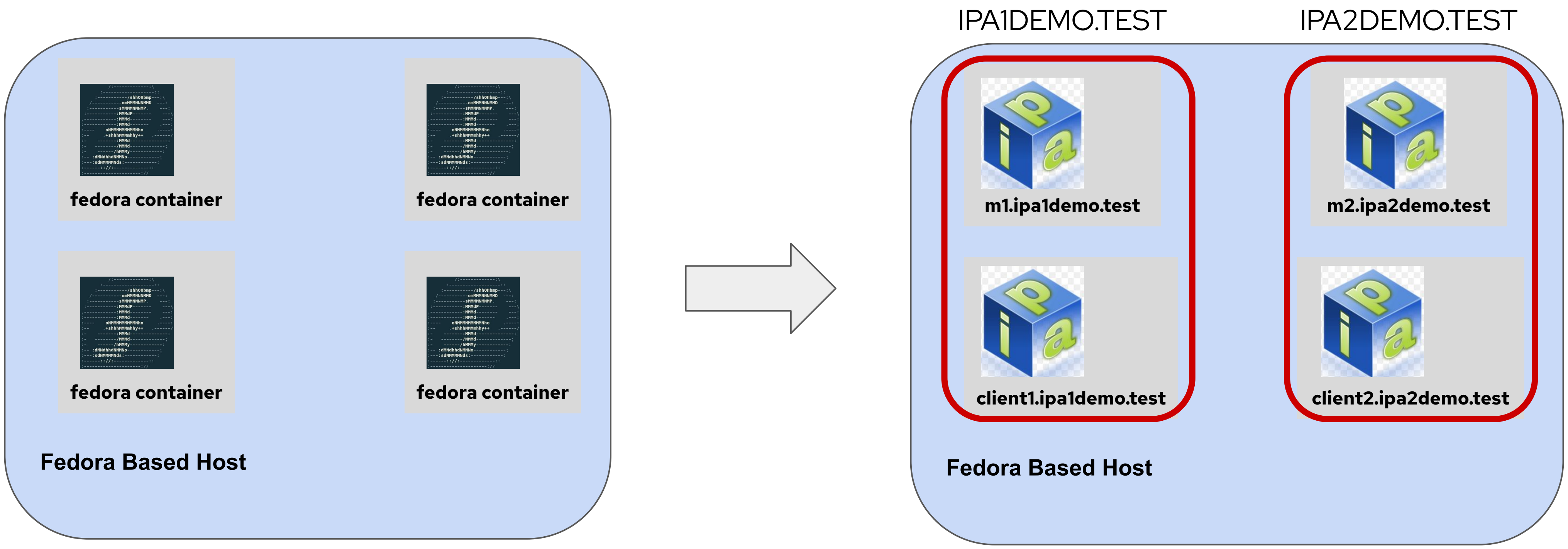
```
$ podman exec -ti <hostname> bash

$ podman exec -ti m1.ipa1demo.test hostname -i

$ podman unshare --rootless-netns firefox --new-instance --new-window $url
```

Trust between IdM deployments

- Test Environment
  - Fedora-based host running multiple containers or virtual machines
  - Simulates two independent IPA deployments: *IPA1DEMO.TEST* and *IPA2DEMO.TEST*
- Provisioning Tool:
  - ipalab-config to generate podman compose files + podman-compose to produce the test setup
- Deployment Automation:
  - ansible-freeipa to deploy IPA configurations
- Sample Containerfile uses IPA-IPA trust COPR repository
-

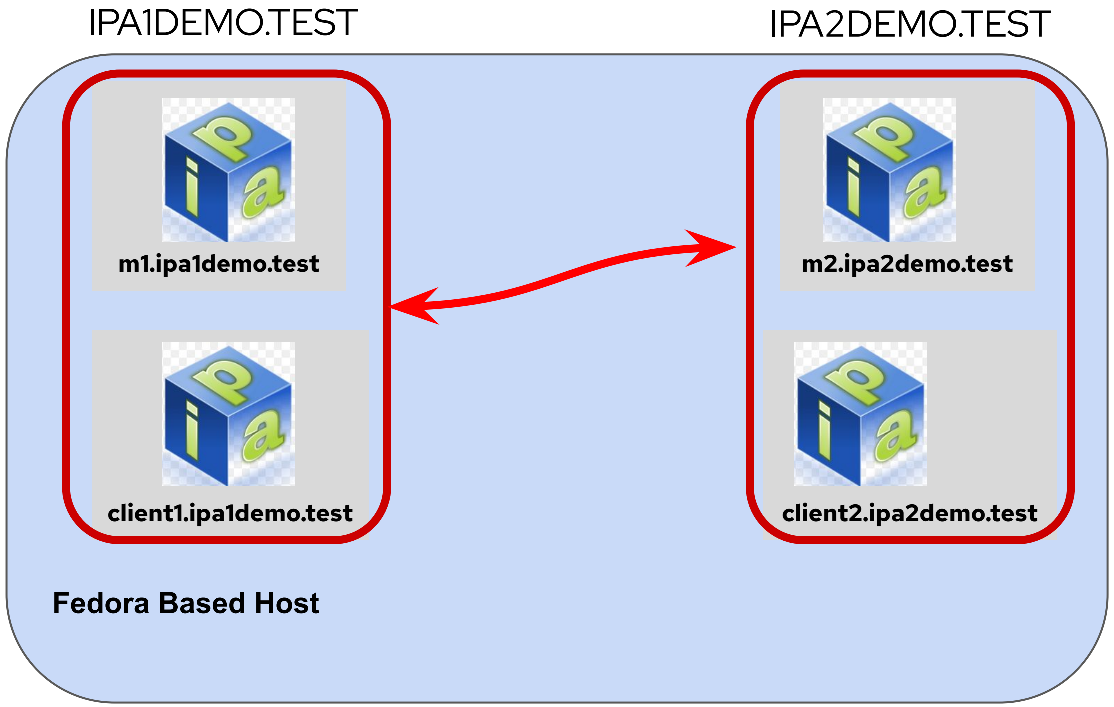
Trust between IdM deployments

- Use the Ansible playbooks to automate the deployment of two separate FreeIPA servers and their respective clients, mimicking two independent IPA domains



Trust between IdM deployments

- Use the Ansible playbooks to automate the deployment of two separate FreeIPA servers and their respective clients, mimicking two independent IPA domains



Trust between IdM deployments

- The automation process includes several key steps to manage and establish trust between two IdM environments
  - Clean up old data
  - Collect information about the FreeIPA deployments
  - Establish Bidirectional Trust
  - Add ID range for IPA1DEMO.TEST on IPA2DEMO.TEST deployment
- **NB!** The process to establish trust will change.

Trust between IdM deployments

- Once Trust is established:
  - Both IPA environments ready to resolve users and groups from the trusted domains
  - All operations available for trust with Active Directory can also be performed for trust with IPA
- Usual administrative operations:
  - grant any access you need:
    - create HBAC and SUDO rules
  - redefine POSIX attributes for trusted domain users
    - create ID Overrides
  - Allow administrative operations for trusted domain users, including enrolling new machines

Trust between IdM deployments

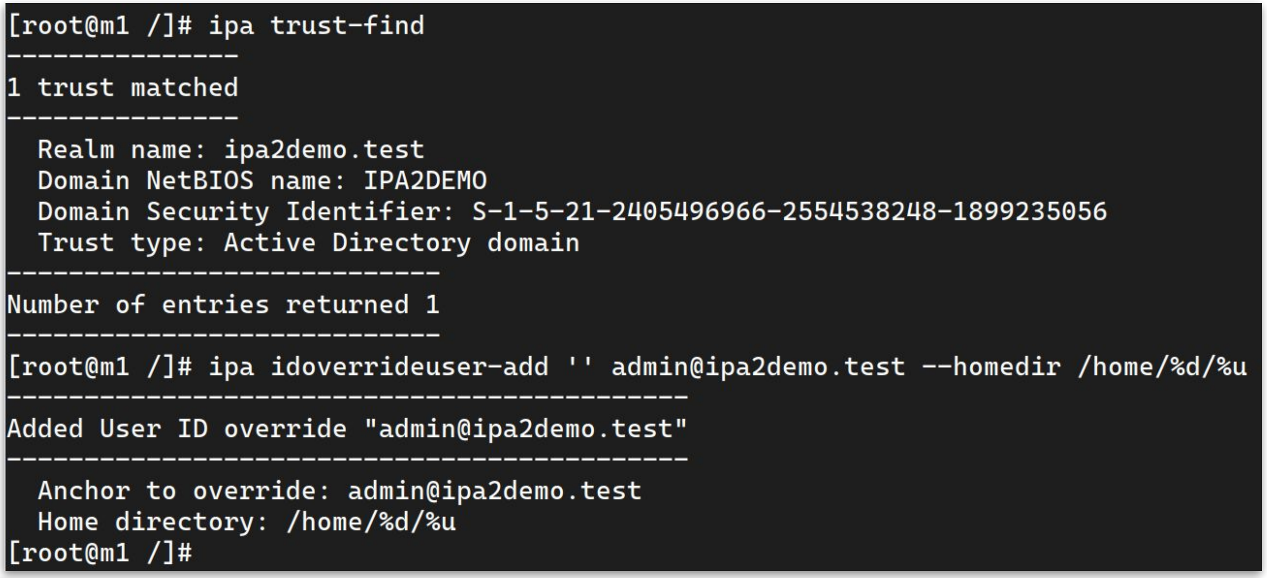
What is already supported?

- Trusted IPA users and groups can be
  - added as external members of external (non-POSIX) groups
  - added to ID overrides in 'Default Trust View' to allow login to Web UI

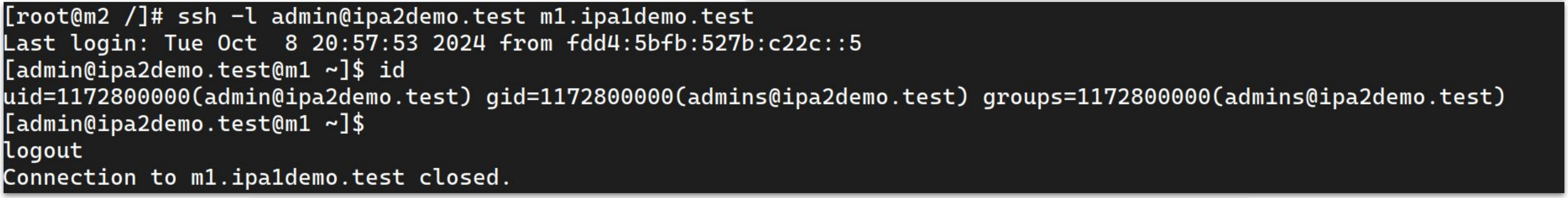
- ID overrides in ‘Default Trust View’
  - can be added as members of IPA groups to allow permissions/roles to apply
  - can be templated for the whole trusted domain
- External groups can be added as members of POSIX groups
- SUDO rules and HBAC rules can be applied via external group membership
- SSSD recognizes trust IPA domains as subdomains of the primary IPA domain

Trust between IdM deployments

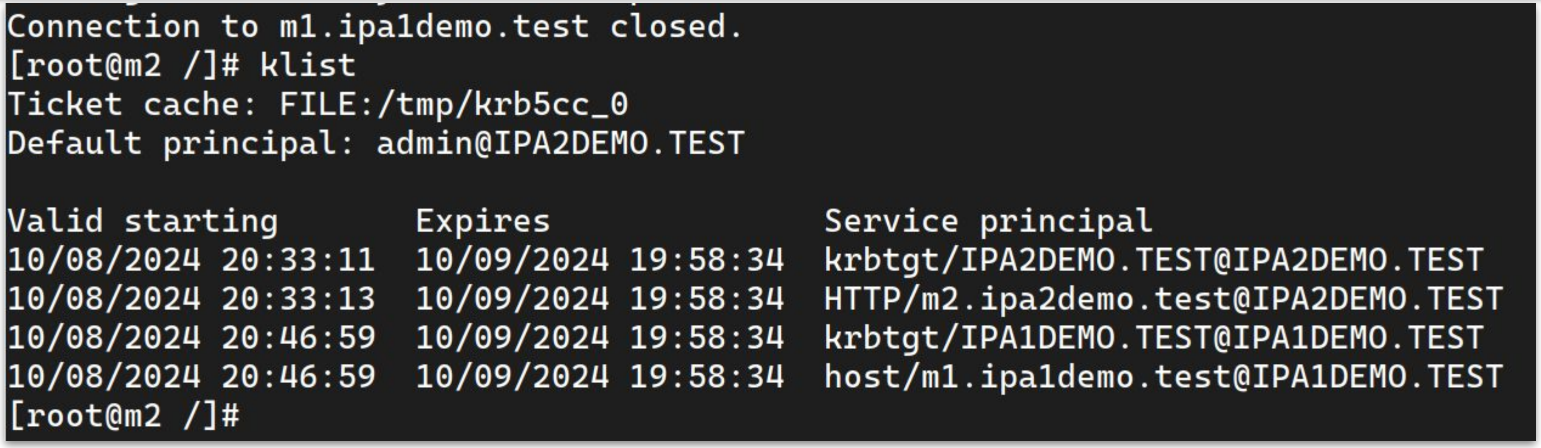
Demo



```
[root@m1 /]# ipa trust-find
---------------
1 trust matched
---------------
  Realm name: ipa2demo.test
  Domain NetBIOS name: IPA2DEMO
  Domain Security Identifier: S-1-5-21-2405496966-2554538248-1899235056
  Trust type: Active Directory domain
----------------------------
Number of entries returned 1
----------------------------
[root@m1 /]# ipa idoverrideuser-add '' admin@ipa2demo.test --homedir /home/%d/%u
--------------------------------------------
Added User ID override "admin@ipa2demo.test"
--------------------------------------------
  Anchor to override: admin@ipa2demo.test
  Home directory: /home/%d/%u
[root@m1 /]#
```



```
[root@m2 /]# ssh -l admin@ipa2demo.test m1.ipa1demo.test
Last login: Tue Oct  8 20:57:53 2024 from fdd4:5bfb:527b:c22c::5
[admin@ipa2demo.test@m1 ~]$ id
uid=1172800000(admin@ipa2demo.test) gid=1172800000(admins@ipa2demo.test) groups=1172800000(admins@ipa2demo.test)
[admin@ipa2demo.test@m1 ~]$
logout
Connection to m1.ipa1demo.test closed.
```



```
Connection to m1.ipa1demo.test closed.
[root@m2 /]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@IPA2DEMO.TEST

Valid starting       Expires              Service principal
10/08/2024 20:33:11  10/09/2024 19:58:34  krbtgt/IPA2DEMO.TEST@IPA2DEMO.TEST
10/08/2024 20:33:13  10/09/2024 19:58:34  HTTP/m2.ipa2demo.test@IPA2DEMO.TEST
10/08/2024 20:46:59  10/09/2024 19:58:34  krbtgt/IPA1DEMO.TEST@IPA1DEMO.TEST
10/08/2024 20:46:59  10/09/2024 19:58:34  host/m1.ipa1demo.test@IPA1DEMO.TEST
[root@m2 /]#
```

What is next?

- Change how tust is established
  - OAuth2 end-point
- Support for modern authn workflows, e.g. passwordless methods
  - GSSAPI Authentication indicators across the trust boundary
- Federated authorization
  - Web UI login as trusted user with passwordless methods

Red Hat Summit

Thank you

in linkedin.com/company/red-hat

f facebook.com/redhatinc

▶ youtube.com/user/RedHatVideos

twitter.com/RedHat