Building cross-domain trust between FreeIPA deployments

FOSDEM 2025

Alexander Bokovoy, Sr. Principal Software Engineer, Red Hat

Francisco Triviño García, Principal Software Engineer, Red Hat

Advancements in Trusted relationships between FreeIPA deployments

Key Updates

Continuous testing using Fedora

- We are able to establish trust between two separate FreeIPA deployments
  - Looks similar to “trust between FreeIPA and Active Directory” from user’s point of view
    - Kerberos authentication works
    - SSSD resolves users and groups
    - ID overrides do work
- We have prepared infrastructure to test the trust
  - Upstream CIs in FreeIPA and SSSD allow test of multiple separate IPA environments
  - Multiple IPA environments can be created locally for developer convenience as well
  - SSSD and FreeIPA development branches automatically built in COPR as packages for Fedora

Demo setup

And some help for those less familiar with podman

Fedora 40+ VM as the main host with sufficient RAM

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

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

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

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

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

Automation

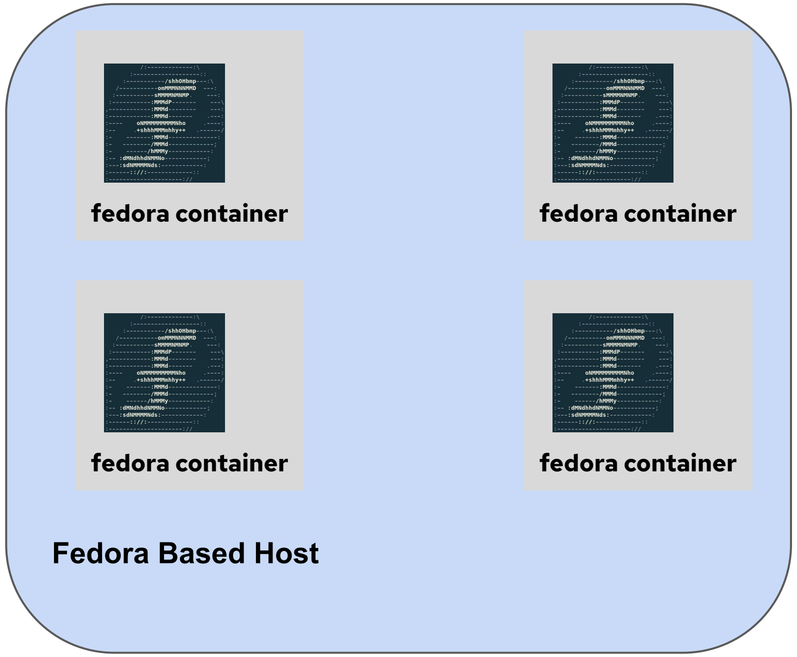
Testing in Fedora using Podman Containers

Environment Setup

- FreeIPA and SSSD upstream development at this point
- 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

Testing in Fedora using Podman Containers

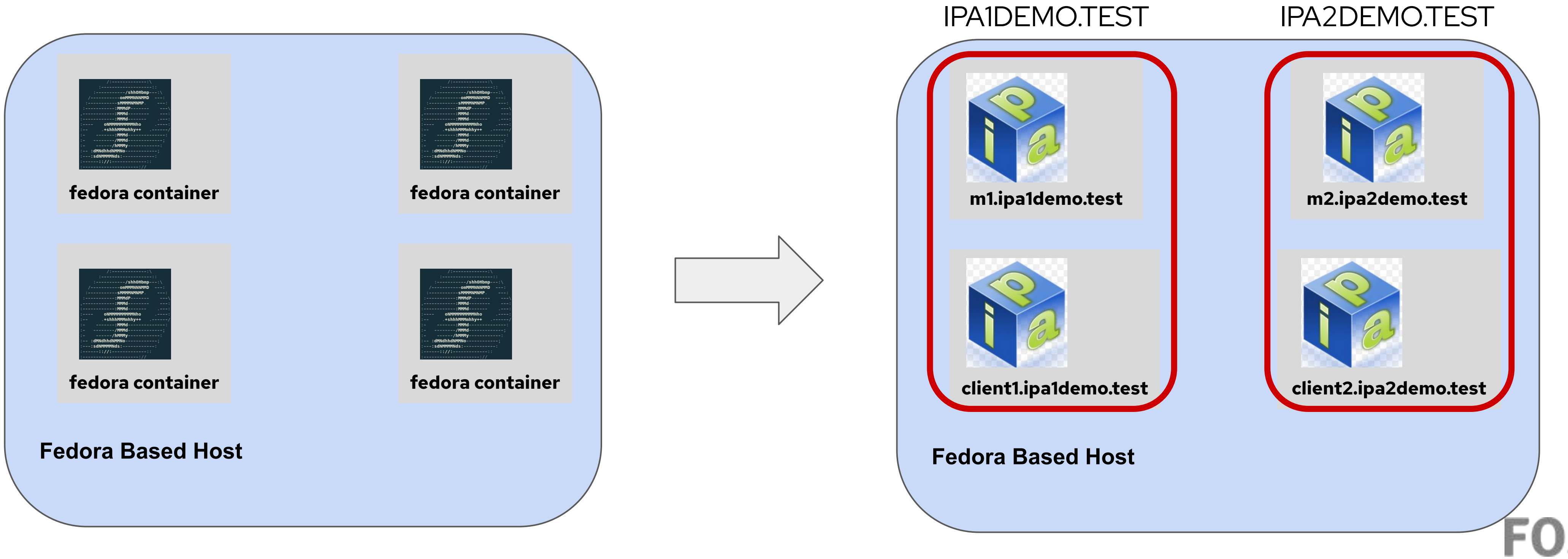
Environment Setup - Provisioning



Testing in Fedora using Podman Containers

Environment Setup – FreeIPA deployment

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

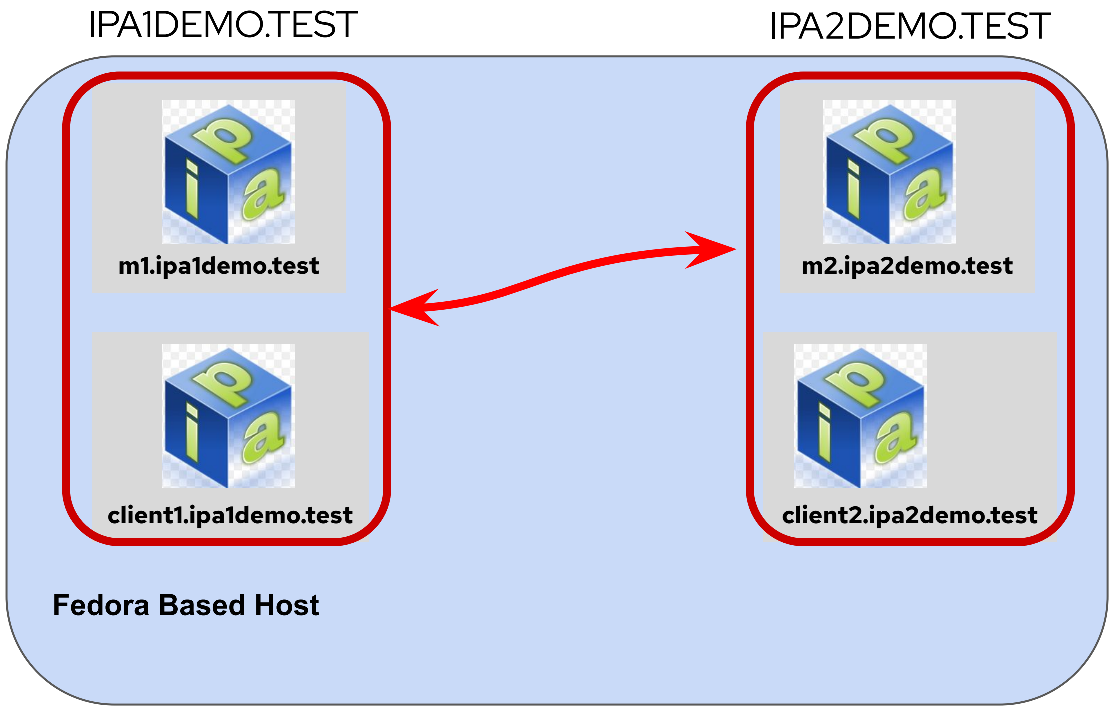


FOSDEM'25

Testing in Fedora using Podman Containers

Establish Trust

- Use the Ansible playbooks to establish trust



Establishing trust between multiple domains

Establish Trust

- 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. Current approach utilizes the same logic FreeIPA has for trust to Active Directory. In future, a process to establish trust will look similarly but will not rely on existence of Samba DC.

Perform Administrator Operations

Manage Trusted Domain

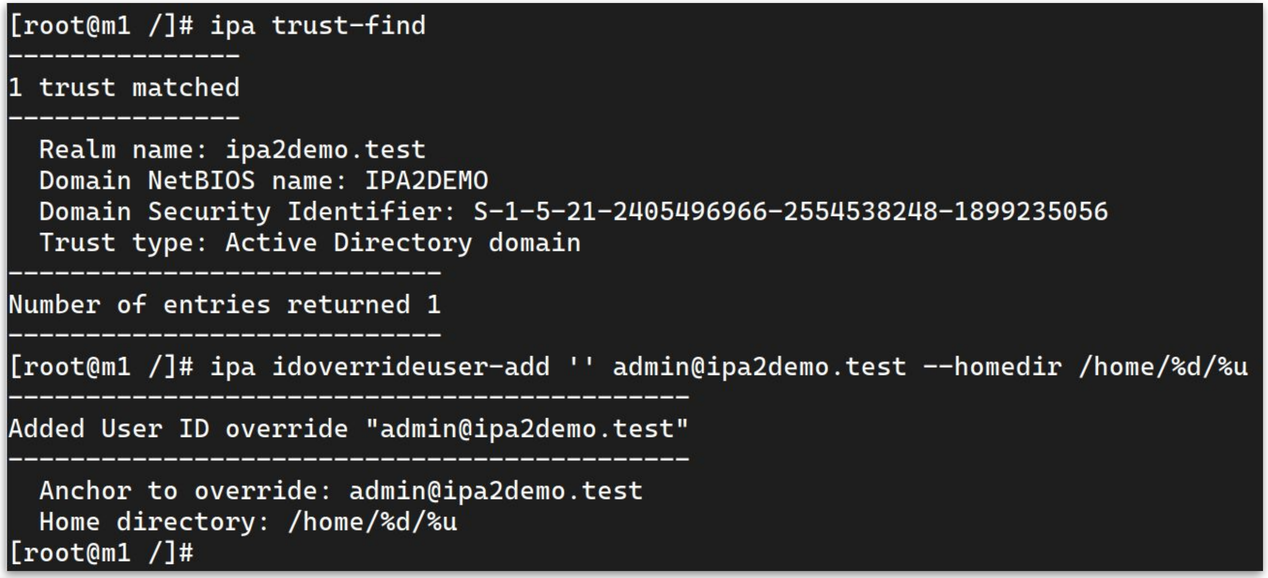
- After Trust Establishment completion:
  - Both IPA environments ready to resolve users and groups from the trusted domains
  - All operations available for trust with Active Directory can also be performed for trust with IPA
- Usual administrative operations:
  - block any access we don’t want to:
    - 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

Managing Trusted Domains

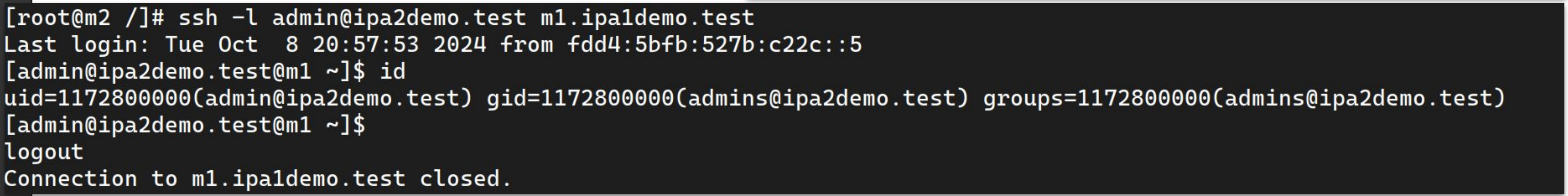
Features to test

- Trusted IPA users and groups can be added as external members of external (non-POSIX) groups
- External groups can be added as members of POSIX groups
- SUDO rules and HBAC rules can be applied via external group membership
- Trusted IPA users and groups can be handled in ID overrides
- Trusted IPA user can be 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

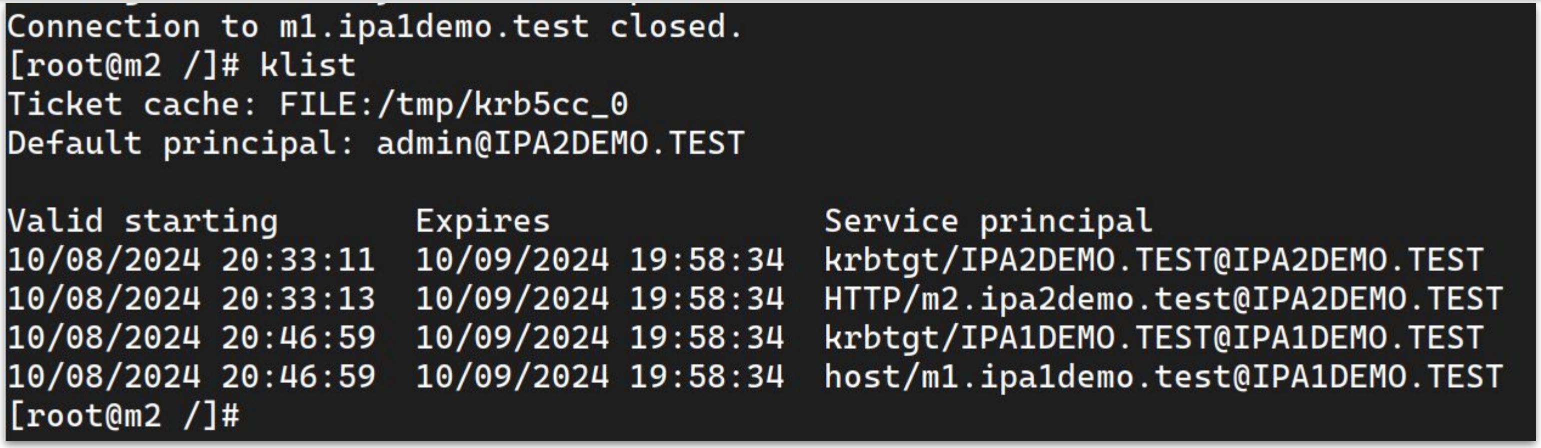
Live Demo



```
[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.
```



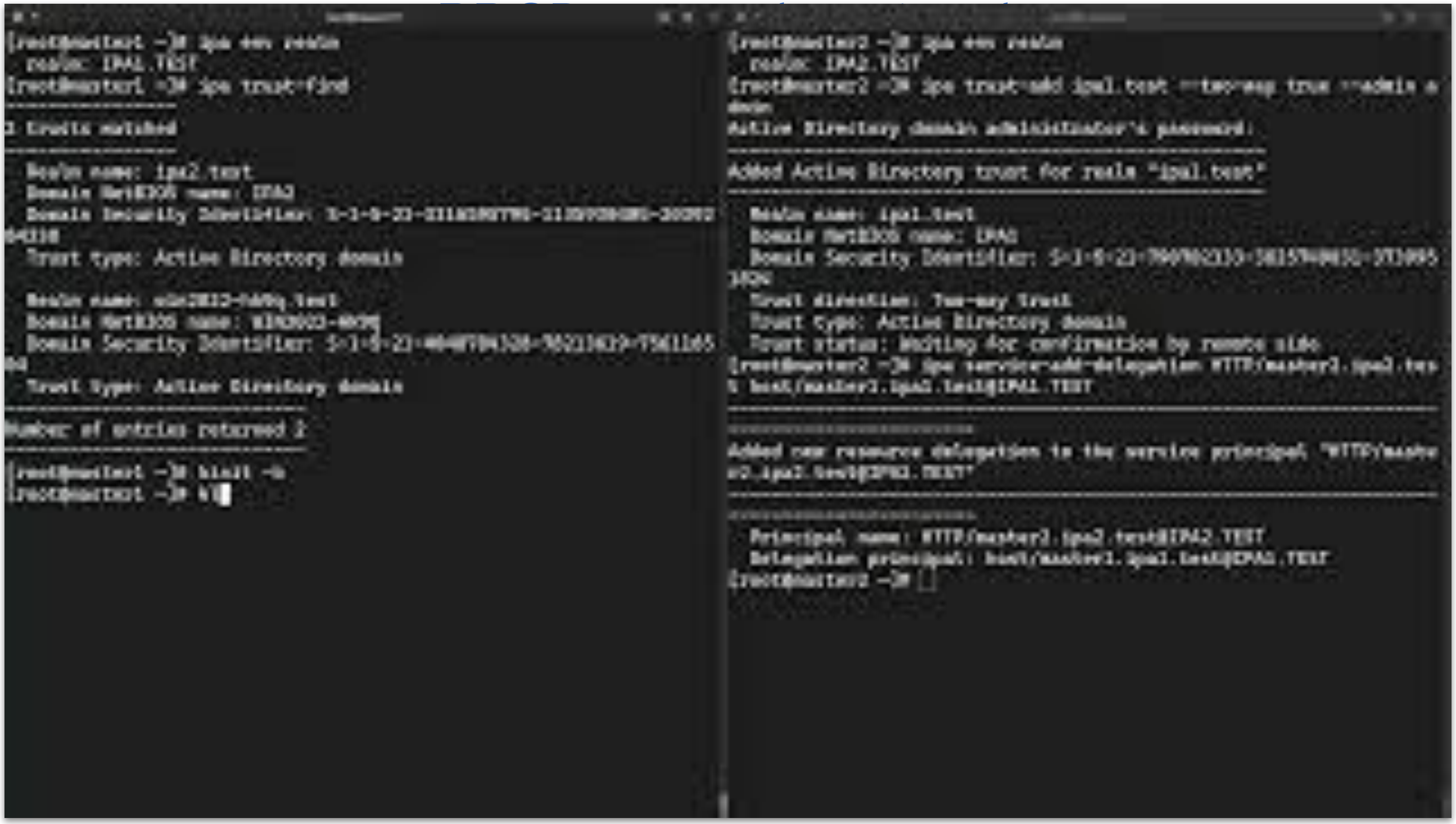
```
Connection to m1.ipa1demo.test closed.
[root@m2 /]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin@IPA2DEMO.TEST

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 /]#
```

Live Demo

Steps

- Provision a Fedora Base Host
- Build the container image using COPR
- Install provisioning system
- Deploy Servers and Clients
- Establish Bidirectional Trust, then
  - Show POSIX ID range for IPA1DEMO.TEST trust on IPA2DEMO.TEST
  - Show resolution of trusted users on IPA1DEMO
  - Show resolution of trusted users on IPA2DEMO

RBCD cross-domain rules



```
[root@master1 ~]# ipa env realm
  realm: IPA1.TEST
[root@master1 ~]# ipa trust-find
----------------
2 trusts matched
----------------
  Realm name: ipa2.test
  Domain NetBIOS name: IPA2
  Domain Security Identifier: S-1-5-21-[illegible]
[illegible]
  Trust type: Active Directory domain

  Realm name: win2022-[illegible].test
  Domain NetBIOS name: WIN2022-[illegible]
  Domain Security Identifier: S-1-5-21-[illegible]
[illegible]
  Trust type: Active Directory domain
----------------------------
Number of entries returned 2
----------------------------
[root@master1 ~]# kinit -k
[root@master1 ~]# kl
```

```
[root@master2 ~]# ipa env realm
  realm: IPA2.TEST
[root@master2 ~]# ipa trust-add ipa1.test --two-way true --admin a
dmin
Active Directory domain administrator's password:
--------------------------------------------------
Added Active Directory trust for realm "ipa1.test"
--------------------------------------------------
  Realm name: ipa1.test
  Domain NetBIOS name: IPA1
  Domain Security Identifier: S-1-5-21-[illegible]
[illegible]
  Trust direction: Two-way trust
  Trust type: Active Directory domain
  Trust status: Waiting for confirmation by remote side
[root@master2 ~]# ipa service-add-delegation HTTP/master2.ipa2.tes
t host/master1.ipa1.test@IPA1.TEST
-------------------------------------------------------------------
-------------------------------
Added new resource delegation to the service principal "HTTP/maste
r2.ipa2.test@IPA2.TEST"
-------------------------------------------------------------------
-------------------------------
  Principal name: HTTP/master2.ipa2.test@IPA2.TEST
  Delegation principal: host/master1.ipa1.test@IPA1.TEST
[root@master2 ~]#
```

Next steps

Next steps

- ID Overrides template resolving in sssd
  - Set default POSIX shell/home directory for trusted domain users per domain
- Changes in the process to establish trust
  - 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

Questions / Discussion