Red Hat Summit

Experiencing FreeIPA before RHEL Identity Management

Deployment migration case

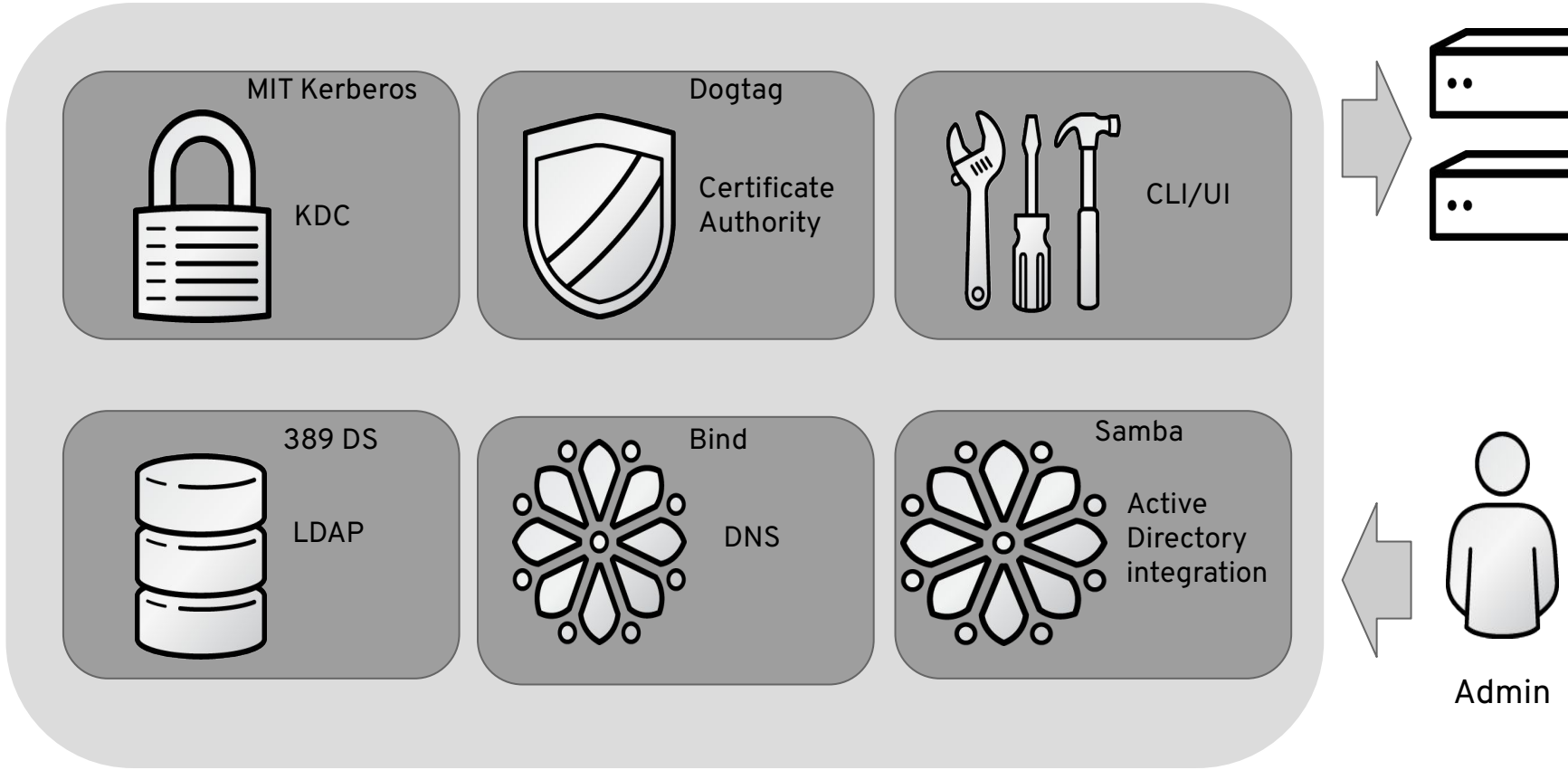
Alexander Bokovoy,
Senior Principal
Software Engineer

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 deployment migration

`ipa migrate-ds`: migration for remote LDAP servers since version 2.0.0

- **Only migrates users and groups**
- User-private groups are not maintained
- Executed as a server-side plugin within the context of a client connection
- There is no feedback during the migration beyond watching the logs
- There is no migration-specific journal
- Syntax errors can cause migration to fail with the only resolution being to skip broken entries or fix the remote LDAP server

FreeIPA deployment migration

- New migration tool: `ipa-migrate`
  - Migrates IPA deployment to IPA deployment
  - Upstream design document: https://freeipa.readthedocs.io/en/latest/designs/ipa_to_ipa_migration.html
  - Available in Fedora and RHEL 9 and 10 as a Tech Preview

- The tool assumes that the target IPA deployment is already created
  - New deployment:
    - own CA unless it is a CA-less configuration
    - own Kerberos infrastructure
  - No topology changes: new replicas should be added in the new deployment

- Advanced capabilities:
  - dry-run simulations
  - selective content migration
  - non-IPA data handling

FreeIPA deployment migration

- Migration areas
  - LDAP schema (replicated)
  - LDAP server configuration (server-specific)
  - The main LDAP database content

- What is migrated
  - Accounts: Users, Groups, Roles, ..., Host Groups, Services, ID Views, ..., Sub IDs
  - HBAC & PBAC: Services, Privileges, Permissions...
  - Sudo: Rules, Commands, ...
  - DNS: Records, Servers
  - Kerberos: Realm, Policy, Passwd Policy, ...
  - Etc entries: CA, Topology, Passkey, ...
  - Plugins: Automember, DNA, MEP Templates, ...
  - Misc: Trusts, Provisioning, SELinux, ...
  - REALM/Domain: suffixes, ...
  - ID ranges: automatic migration

FreeIPA LDAP data store structure

- Single LDAP tree
  - All objects of a single type in a flat structure
    - Users: `uid=name,cn=users,cn=accounts,..`
    - Groups: `cn=name,cn=groups,cn=accounts,..`
    - Hosts: `fqdn=name,cn=computers,cn=accounts,..`
    - Kerberos services: `krbPrincipalName=name,cn=services,cn=accounts,..`
    - ...
  - `ipa env` will return all containers relative to the base DN:
    - `ipa env | egrep '(basedn|container_(user|group|host|service)+)'`

```
basedn: dc=example,dc=test
container_group: cn=groups,cn=accounts
container_host: cn=computers,cn=accounts
container_hostgroup: cn=hostgroups,cn=accounts
container_service: cn=services,cn=accounts
container_user: cn=users,cn=accounts
```

FreeIPA LDAP data store structure

- LDAP objects have a lot of attributes
  - Set of attributes is defined by the objectclasses associated with the entry
- Deployment-specific attributes
  - Kerberos attributes
  - Unique object identifiers
  - ...

```
objectClass: ipaobject
objectClass: person
objectClass: top
objectClass: ipasshuser
objectClass: inetorgperson
objectClass: organizationalperson
objectClass: krbticketpolicyaux
objectClass: krbprincipalaux
objectClass: inetuser
objectClass: posixaccount
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
objectClass: ipauserauthtypeclass
objectClass: ipantuserattrs
objectClass: ipapasskeyuser
```

```
dn: uid=abokovoy,cn=users,cn=accounts,dc=example,dc=test
uid: abokovoy
givenname: Alexander
sn: Bokovoy
cn: abokovoy
initials: AB
homedirectory: /home/abokovoy
gecos: Alexander Bokovoy
loginshell: /bin/bash
krbcanonicalname: abokovoy@EXAMPLE.TEST
krbprincipalname: abokovoy@EXAMPLE.TEST
mail: ab@example.test
uidnumber: 1000
gidnumber: 1000
manager: uid=admin,cn=users,cn=accounts,dc=example,dc=test
sshpubkeyfp: <encoded value>
sshpubkeyfp: <encoded value>
ipauserauthtype: password
ipauserauthtype: passkey
usercertificate <encoded value>
usercertificate <encoded value>
ipapasskey: <encoded value>
ipapasskey: <encoded value>
ipapasskey: <encoded value>
nsaccountlock: FALSE
has_password: TRUE
has_keytab: TRUE
displayName: Alexander Bokovoy
ipaNTSecurityIdentifier: S-1-5-21-245462123-1556963680-2572160461-1000000
ipaSshPubKey: <encoded value>
ipaUniqueID: 5a58979c-1aa9-11e5-a8f7-001a4a418612
krbExtraData: <encoded value>
krbLastFailedAuth: 20250504085845Z
krbLastPwdChange: 20250421075321Z
krbLastSuccessfulAuth: 20250514090854Z
```

FreeIPA deployment migration

- Migration scenarios
  - Production mode
    - Target deployment is fully functional
      - DNA ranges migrated intact
      - ID ranges migrated intact
      - SIDs migrated intact
  - Staging mode
    - Target deployment does not need exact IDs and will have them regenerated
      - DNA ranges will not be updated
      - ID ranges will not be updated
      - UID/GID values and SIDs will be automatically generated
- Dry-run support

FreeIPA deployment migration

- Migration approaches
  - Online
    - Use `ipa-migrate` on the new server
      - Connect to the old server
      - Retrieve data
      - Transform and apply to the new server
  - Offline
    - Take a backup of the original server data
      - `/etc/dirsrv/slapd-INSTANCE/dse.ldif`
      - `/etc/dirsrv/schema/*` and `/etc/dirsrv/slapd-INSTANCE/schema/*`
      - Export of the userRoot database as ldif file
    - Copy manually to the new server
    - Run `ipa-migrate` on the new server
  - Mixed use
    - Steps from online and offline approaches can be mixed together

FreeIPA deployment migration

- Migration logs in `/var/log/ipa-migrate.log`

```
024-02-27T17:10:03Z DEBUG ================================================================================
2024-02-27T17:10:03Z INFO IPA to IPA migration starting ...
2024-02-27T17:10:03Z DEBUG Migration options:
2024-02-27T17:10:03Z DEBUG --mode=prod-mode
2024-02-27T17:10:03Z DEBUG --hostname=hpe-dl385gen8-01.hpe2.lab.eng.bos.redhat.com
2024-02-27T17:10:03Z DEBUG --verbose=False
2024-02-27T17:10:03Z DEBUG --bind-dn=cn=directory manager
2024-02-27T17:10:03Z DEBUG --bind-pw-file=None
2024-02-27T17:10:03Z DEBUG --cacertfile=None
2024-02-27T17:10:03Z DEBUG --subtree=[]
2024-02-27T17:10:03Z DEBUG --log-file=/var/log/ipa-migrate.log
2024-02-27T17:10:03Z DEBUG --skip-schema=False
2024-02-27T17:10:03Z DEBUG --skip-config=False
```

- Verbose logging

```
...
...
2024-02-28T15:30:53Z INFO Migrating database ... (this make take a while)
2024-02-28T15:30:53Z INFO Entry is different and will be updated: 'uid=admin,cn=users,cn=accounts,dc=hpe2,dc=lab,dc=
2024-02-28T15:30:53Z INFO Add db entry 'uid=mark,cn=users,cn=accounts,dc=hpe2,dc=lab,dc=eng,dc=bos,dc=redhat,dc=com
2024-02-28T15:30:53Z INFO Entry is different and will be updated: 'cn=HPE2.LAB.ENG.BOS.REDHAT.COM_id_range,cn=ranges
2024-02-28T15:30:53Z INFO Entry is different and will be updated: 'cn=HPE2.LAB.ENG.BOS.REDHAT.COM_subid_range,cn=ran
```

FreeIPA deployment migration

- Summary report
  - At the end of the migration a summary report is displayed
  - Tracks/counts all entry types that were migrated
  - Uses the “map” objects to dynamically generate this report
  - By default only displays the entry types that were updated
  - Verbose option shows all the entry types that could be migrated

```
General Information
------------------
 - Remote Host:             m1.origin.test
 - Migration Duration:      0:01:05
 - Migration Log:           /var/log/ipa-migrate.log
 - Remote Host:             m1.origin.test
 - Remote Domain:           origin.test
 - Local Host:              m2.target.test
 - Local Domain:            target.test
 - Remote Suffix:           dc=origin,dc=test
 - Local Suffix:            dc=target,dc=test
 - Remote Realm:            ORIGIN.TEST
 - Local Realm:             TARGET.TEST
 - Schema Analyzed:         1882 definitions
 - Config Analyzed:         1 entries
 - Database Anaylzed:       628 entries
Schema Migration (migrated 0 definitions)
-----------------------------------------
 - Attributes:              0
 - Objectclasses:           0
DS Configuration Migration (migrated 1 entries)
-----------------------------------------------
 - DNA Plugin:              1
Database Migration (migrated 70 entries)
----------------------------------------
 - DNA Ranges:              2
 - Sysaccounts:             2
 - Admin:                   1
 - Users:                   50
 - Groups:                  14
 - AD:                      1
```

FreeIPA deployment migration

- Examples

```
# ipa-migrate prod-mode server.origin.test

# ipa-migrate prod-mode server.origin.test --dryrun

# ipa-migrate prod-mode server.origin.test -D "cn=directory manager" -j ./passwd.txt

# ipa-migrate prod-mode server.origin.test --db-ldif=/tmp/remote-userroot.ldif

# ipa-migrate prod-mode server.origin.test --skip-config --skip-schema

# ipa-migrate stage-mode server.origin.test --dryrun-record=/tmp/dryrun-ops.ldif

# ipa-migrate stage-mode server.origin.test --config-ldif=/tmp/dse.ldif \
                    --schema-ldif=/tmp/schema.ldif --db-ldif=/tmp/remote-userroot.ldif

# ipa-migrate stage-mode server.origin.test --subtree="ou=my own data,dc=origin,dc=test"
```

FreeIPA deployment migration

- Demo lab
  - FreeIPA local tests migration demo
    - Provision an original deployment
    - Add some objects
    - Create new deployment
    - Migrate original deployment to new one
- Demo can also be run as a Github action

Red Hat

Red Hat Summit

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat