FreeIPA-to-FreeIPA Migration: Current Capabilities and Use Cases

1-2 February 2025 | Brussels, Belgium

Francisco Triviño <ftrivino@redhat.com>
Rob Crittenden <rcritten@redhat.com>
Mark Reynolds <mareynol@redhat.com>

Slides available

Background

Key Migration Terminology

When managing an identity system, there are different approaches to keeping it up to date or moving it to a new environment:

- **Update** - minor release v4.12.2 → v4.12.3, (e.g. RHEL 9.1 → RHEL 9.2)

- **Upgrade** - moving to a new major version (e.g. RHEL8 → RHEL9)
  - in-place (keep data and config)
  - Upgrade procedure - add a replica (e.g. RHEL7 to RHEL8)

- **Migration**
  - Migration across major operating system versions (e.g. RHEL7 to RHEL9)

Source:

FreeIPA ipa-migrate design page

Background

Key Migration Terminology

When managing an identity system, there are different approaches to keeping it up to date or moving it to a new environment:

- **Update** - minor release v4.12.2 → v4.12.3, (e.g. RHEL 9.1 → RHEL 9.2)

- **Upgrade** - moving to a new major version (e.g. RHEL8 → RHEL9)
  - in-place (keep data and config)
  - Upgrade procedure - add a replica (e.g. RHEL7 to RHEL8)

- **Migration**
  - Migration across major operating system versions (e.g. RHEL7 to RHEL9)

Source:

FreeIPA ipa-migrate design page

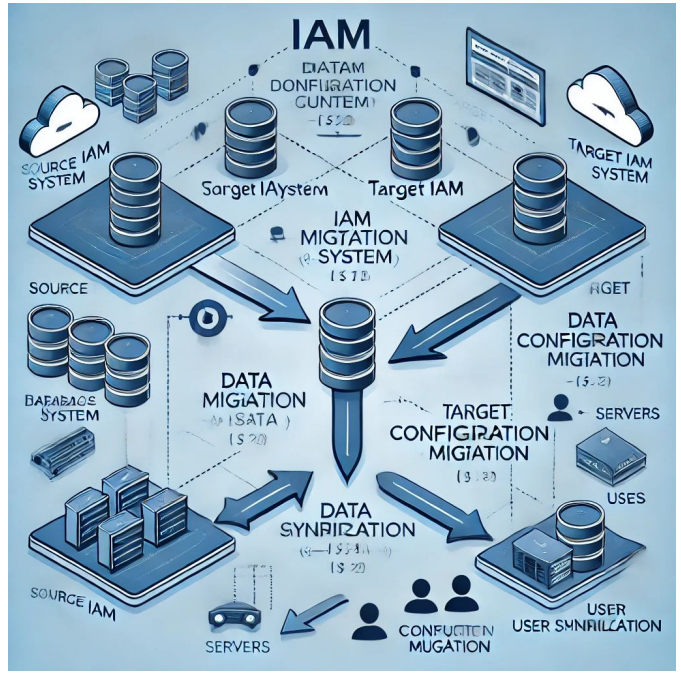
Background

Importance of Migration Mechanism in Identity Management Systems

In the context of FreeIPA, full migration means transferring:

- Users, Groups, Roles, ..., Host Groups, Services, ... from one deployment to another

- Why it matters?
  - Reduce admin burden and complexity
  - Minimizes end-user disruption
  - helps avoid downtime and service interruptions



... migrating without good tools is like moving a beehive bare-handed—you'll get it done, but expect pain ...

Source:

FreeIPA ipa-migrate design page

Red Hat

Background

Overview of the old FreeIPA plugin-based migration

IPA has had a plugin-based migration for remote LDAP servers since version 2.0.0. This is insufficient for the following reasons:

- **Only migrate users and groups**, It severely limits IPA-to-IPA migration as all other entry types are lost
- User-private groups are not maintained
- It is executed as a server-side plugin and if it runs long enough the client may disconnect
- There is no feedback during the migration beyond watching the logs
- There is no migration-specific log
- Syntax errors can cause migration to fail with the only resolution being to skip broken entries or fix the remote LDAP server

Source:

FreeIPA ipa-migrate design page

/usr/sbin/ipa-migrate

ipa-migrate

- Designed to facilitate robust IPA-to-IPA migrations while addressing the complexities of **LDAP schema**, **configuration**, and **database migration**
- New *AdminTool* standalone client tool: **/usr/sbin/ipa-migrate**
- Configurable migration methods: **production** for retaining critical IDs and staging for regenerating attributes, and options to mix and match **online** and **offline** methods for optimized performance.
- Advanced capabilities such as **dry-run** simulations, **selective content migration**, and non-IPA data handling further enhance the tool's adaptability
- Logging (**/var/lib/ipa-migrate.log**), Verbose logging (**--verbose, -v**)
- Summary Report

Source:

FreeIPA ipa-migrate design page

What is currently migrated ...

Adding IPA-to-IPA Migration Including All Entry Types.

1. The LDAP Schema:

- objectclasses
- attributes

2. The config:

- LDAP configuration under cn=config (dse.ldif)
- Performance tuning
- Security settings
- Log rotation settings
- ...

3. Database - the main LDAP database content:

- **Accounts**: Users, Groups, Roles, ..., Host Groups, Services, 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

Source:

FreeIPA ipa-migrate design page

What is currently not migrated ...

Supported Migration Scenarios

Few points to consider:

Replicas: replicas are not migrated, ipa-replica-install can be used to add them after migrating the server.

Source:

FreeIPA ipa-migrate design page

What is currently not migrated ...

Supported Migration Scenarios

Few points to consider:

Replicas: replicas are not migrated, ipa-replica-install can be used to add them after migrating the server.

Certificates: the existing CA is abandoned in favor of a CA on the new installation. All certificates will need to be re-issued.

Source:

FreeIPA ipa-migrate design page

What is currently not migrated ...

Supported Migration Scenarios

Few points to consider:

Replicas: replicas are not migrated, ipa-replica-install can be used to add them after migrating the server.

Kerberos: the kerberos master key is not migrated. Kerberos principals are retained but the keys are not.

Certificates: the existing CA is abandoned in favor of a CA on the new installation. All certificates will need to be re-issued.

Source:

FreeIPA ipa-migrate design page

Migration Methods

Online, Offline, Mixing Online and Offline

Online Migration

- Contacting the remote server over the network and pulling in all the info.

Offline Migration

- Using LDIF files from the remote server
  - /etc/dirsrv/slapd-<your-ldap-instance>/**dse.ldif**
  - schema - all files found under /etc/dirsrv/schema/* and /etc/dirsrv/slapd-<your-ldap-instance>/schema/*
  - database - export of the **userroot database** into an ldif file
- Copy all LDIF files to the new local server.

Mixing online and offline methods

- Mix and Match - e.g. config & schema online, then use a database LDIF from the remote.

Source:

FreeIPA ipa-migrate design page

Migration Modes

Production mode, Staging mode, ...

Production Mode

- Assuming that the remote server is fully functional, **everything is brought over** !!
- DNA ranges, IDs, SIDs, ... migrated as is.

Staging Mode

- Assuming that the remote server is in a staging environment..
- DNA ranges, IDs, SIDs, ... **should not be migrated as is.**
- DNA entry attrs will be reset to the magic *regen* value.

Dry-run Migration Mode

- just to see what would be migrated to the new local server...

Source:

FreeIPA ipa-migrate design page

Red Hat

Migration Scenarios

Supported Migration Scenarios

Scenario 1: Production to new Production

- There is a new IPA server installation with the **same realm and domain**
- The realm and domain may be changed, the migrated data will accommodate these changes but requires a reconfiguration of all the clients.

Scenario 2: Production to new Staging

- There is a new IPA server installation with a **different realm and domain** (e.g. staging.example.test)

Scenario 3: Staging to new Production

- There is a new IPA server installation with a **different realm and domain** (e.g. production.example.test)

Scenario 4: From IPA backup

- There is a new IPA server installation with the **same realm and domain**

Source:

FreeIPA ipa-migrate design page

Logging

/var/log/ipa-migrate.log

By default, content will be appended to and not overwritten. Example:

```
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, --verbose, -v CLI option.

```
...
...
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
```


Source:

FreeIPA ipa-migrate design page

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
```


Source:

FreeIPA ipa-migrate design page

DEMO

Examples

Examples

```
# ipa-migrate prod-mode remote.server.com

# ipa-migrate prod-mode remote.server.com --dryrun

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

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

# ipa-migrate prod-mode remote.server.com --skip-config --skip-schema

# ipa-migrate stage-mode remote.server.com --dryrun-record=/tmp/dryrun-ops.ldif

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

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


Source:

FreeIPA ipa-migrate design page

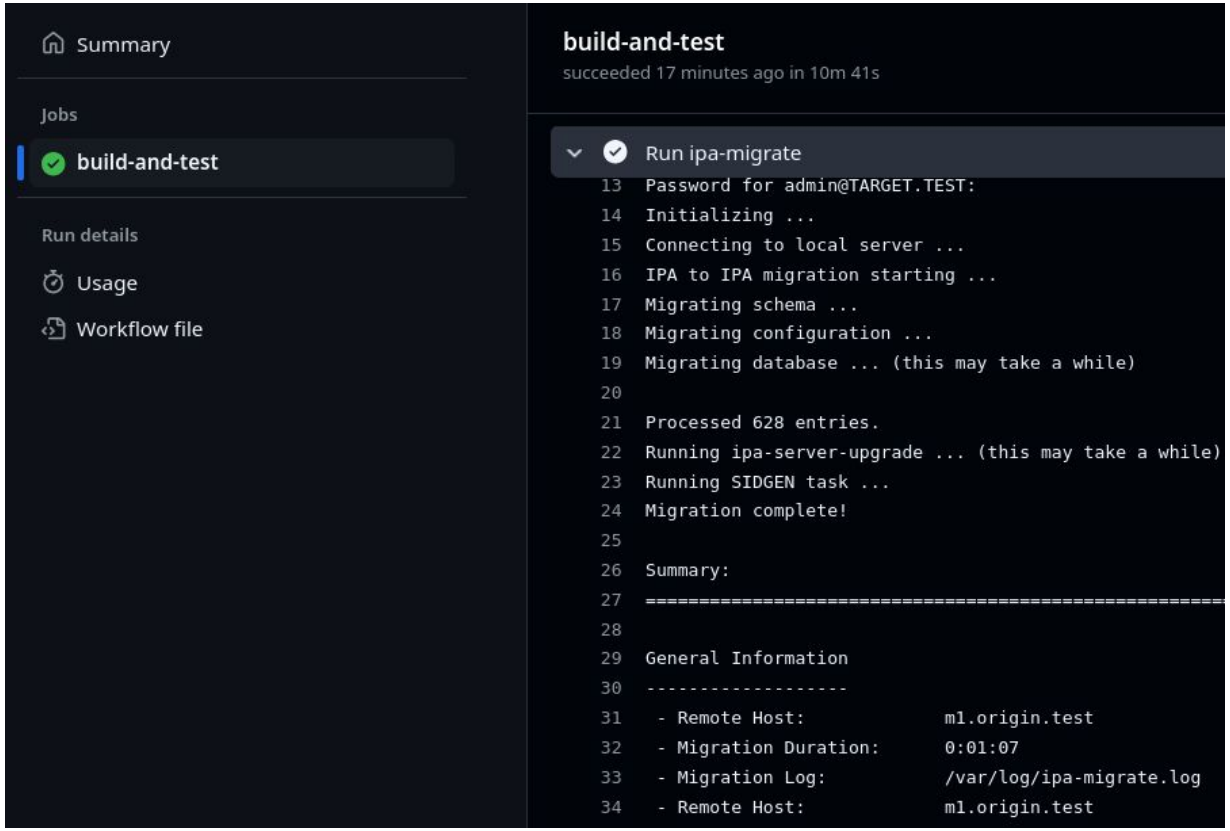
DEMO

Source:

FreeIPA ipa-migrate design page

Tutorial Demo Available

[ipalab-config/ipa-migrate]



Source:

FreeIPA ipa-migrate design page

Streamlined IPA Migration

New IPA to IPA migration tool

- ipa-migrate available in the freeipa project
- If you find issues, please file a ticket https://pagure.io/freeipa/issues
- The tool is available in Fedora and RHEL 9 (as Tech Preview)
- Fedora Test Day

Source:

FreeIPA ipa-migrate design page

Red Hat

Q&A

Slides available

FreeIPA-to-FreeIPA Migration: Current Capabilities and Use Cases

1-2 February 2025 | Brussels, Belgium

Francisco Triviño <ftrivino@redhat.com>
Rob Crittenden <rcritten@redhat.com>
Mark Reynolds <mareynol@redhat.com>

Slides available