Enhancements to FreeIPA Replication Topology Management

Jan Pazdziora
Sr. Principal Software Engineer
Identity Management Special Projects, Red Hat

LINUXCON
EUROPE

6th October 2015

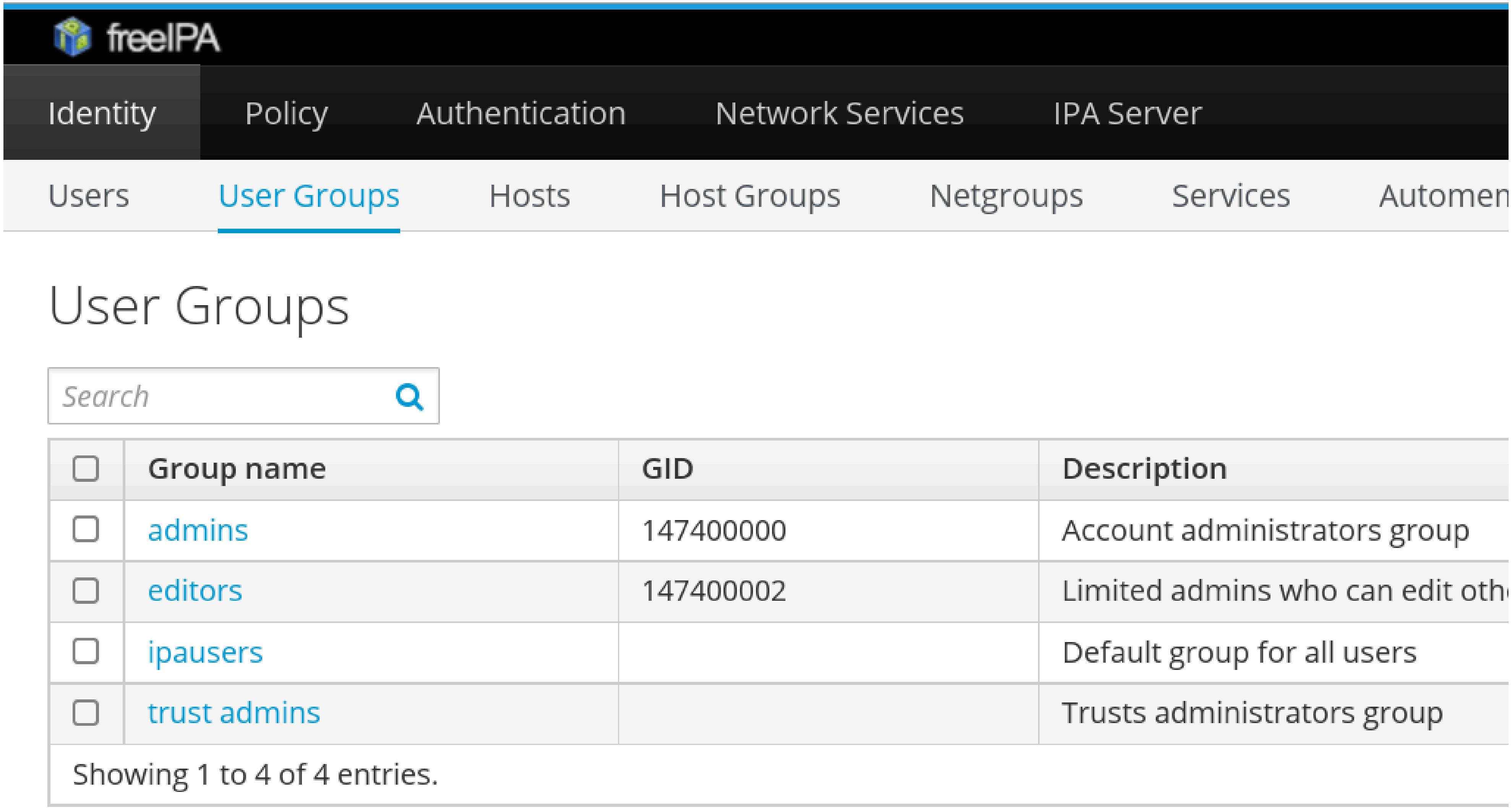
FreeIPA

- Integration of multiple identity-management tools.
    - directory server
    - Kerberos key distribution center
    - optionally DNS server, certification authority, vault
    - WebUI
    - command-line interface

Identities and policies

- Identities managed:
  - users, user groups, hosts, host groups, services, ...
  - with certificates, keytabs, ...
- Policies:
  - ACLs in server itself;
  - host-based access control for IPA-enrolled systems.

FreeIPA WebUI



User Groups

□	Group name	GID	Description
□	admins	147400000	Account administrators group
□	editors	147400002	Limited admins who can edit oth
□	ipausers		Default group for all users
□	trust admins		Trusts administrators group

Showing 1 to 4 of 4 entries.

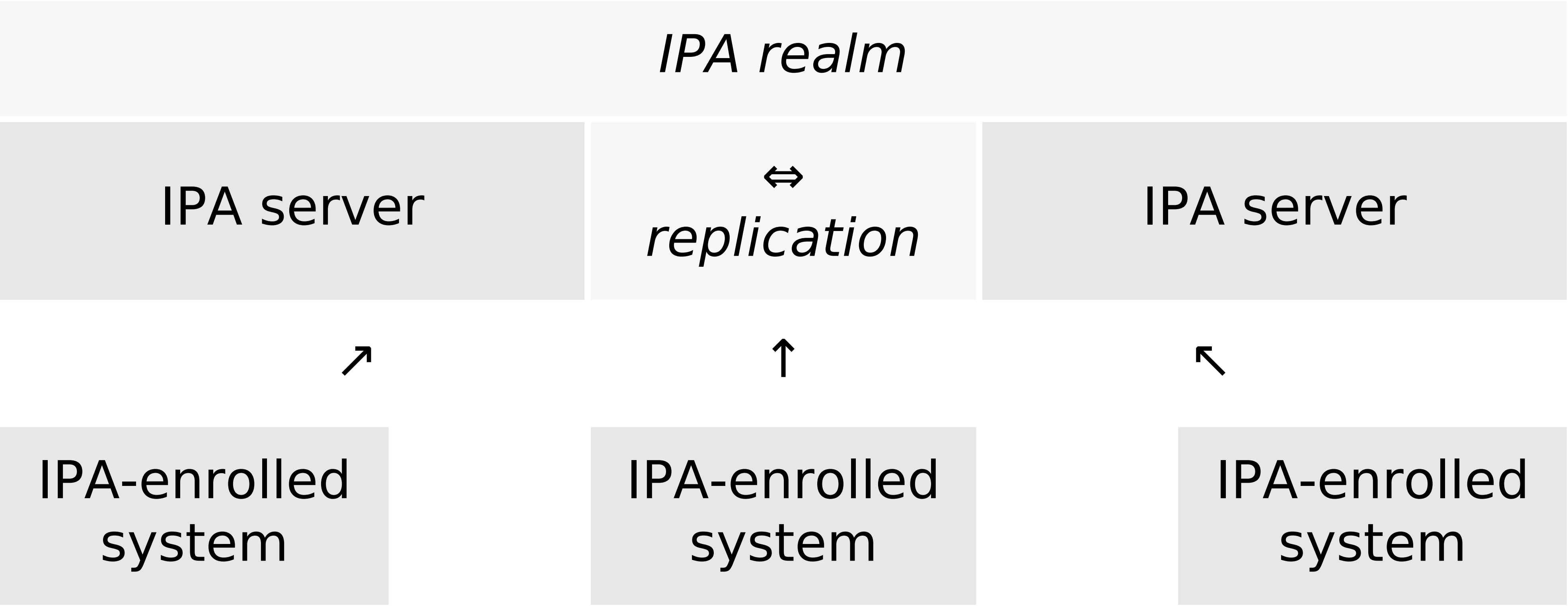
IPA-enrolled systems

- SSSD (System Security Services Daemon):
  - NSS (Name Service Switch) service;
  - PAM (Pluggable Authentication Module) service;
  - plugs to other subsystems — sudo, Kerberos, ...
  - DNS records can prioritize IPA servers used:

    ```
    # /etc/sssd/sssd.conf
    [domain/example.test]
    ipa_server = _srv_, ipa1.example.test
    ...
    ```

  - KDC's IP address cached in `/var/lib/sss/pubconf/kdcinfo.*`.

FreeIPA replication



IPA realm

IPA server

⇔ *replication*

IPA server

↗ ↑ ↖

IPA-enrolled system

IPA-enrolled system

IPA-enrolled system

- IPA servers get found via DNS or with their hostname hardcoded on clients.

FreeIPA 4.2 replication setup

- Multi-master replication.
- Setup of new replica:
  - Remember the Directory Manager password.
  - Create GPG-encrypted replica information file.

    ```
    ipa1# ipa-replica-prepare ipa2.example.com
    ```

  - Transfer the encrypted file to the replica machine.
  - Setup the replica:

    ```
    ipa2# ipa-replica-install \
                     replica-info-ipa2.example.com.gpg
    ```

FreeIPA 4.2 replication

- Replica setup is a two-step process.
  - Hard to automate.
- `ipa-replica-manage` tool
  - Has to connect to all replicas directly to run actions.
- No centralized overview of CAs and their replication.

Upcoming FreeIPA 4.3 release

Two areas of replication improvement:

- Replica promotion.
- Topology plugin.

Replica promotion

- Promotion of any IPA-enrolled client to FreeIPA replica.
- The `ipa-replica-install` tool still used.
- GPG-encrypted file no longer needed.
- New API on IPA servers.
- Standard Kerberos authentication.
  - Note: keep credentials secure especially in case of automated setup.

Replica promotion

- Check `/etc/ipa/default.conf` points to the master.

```
[global]
server = ipa1.example.test
xmlrpc_uri = https://ipa1.example.test/ipa/xml
```

- After replica promotion, it gets updated to point to itself.

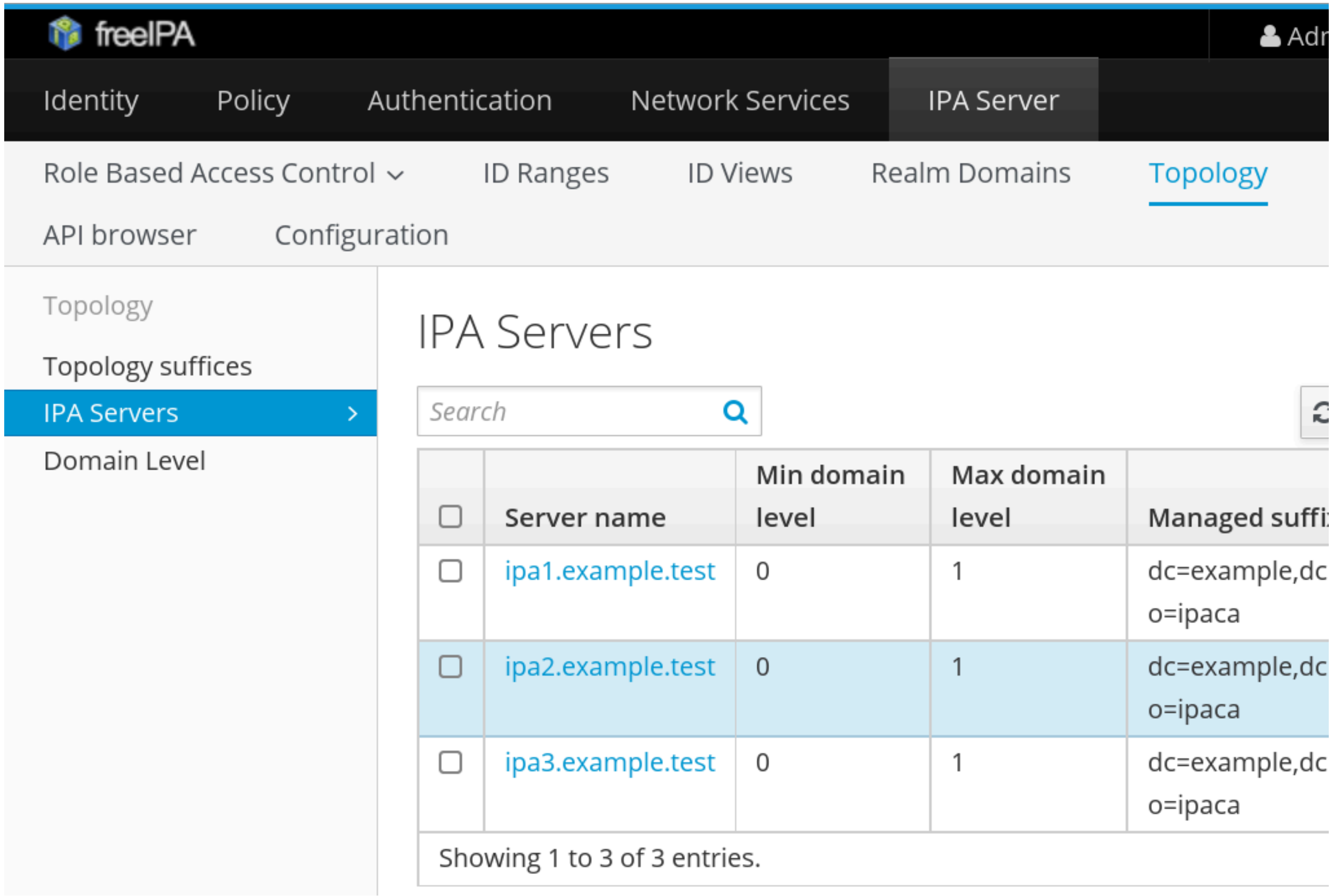
```
xmlrpc_uri = https://ipa2.example.test/ipa/xml
```

- Domain level at least 1 (important for upgrades).

```
ipa1# ipa domainlevel-get
-----------------------
Current domain level: 1
-----------------------
```

Topology information

- Topology info is now replicated across all replicas.



IPA Servers

	Server name	Min domain level	Max domain level	Managed suffi

□	ipa1.example.test	0	1	dc=example,dc
				o=ipaca

□	ipa2.example.test	0	1	dc=example,dc
				o=ipaca

□	ipa3.example.test	0	1	dc=example,dc
				o=ipaca

Showing 1 to 3 of 3 entries.

Topology information

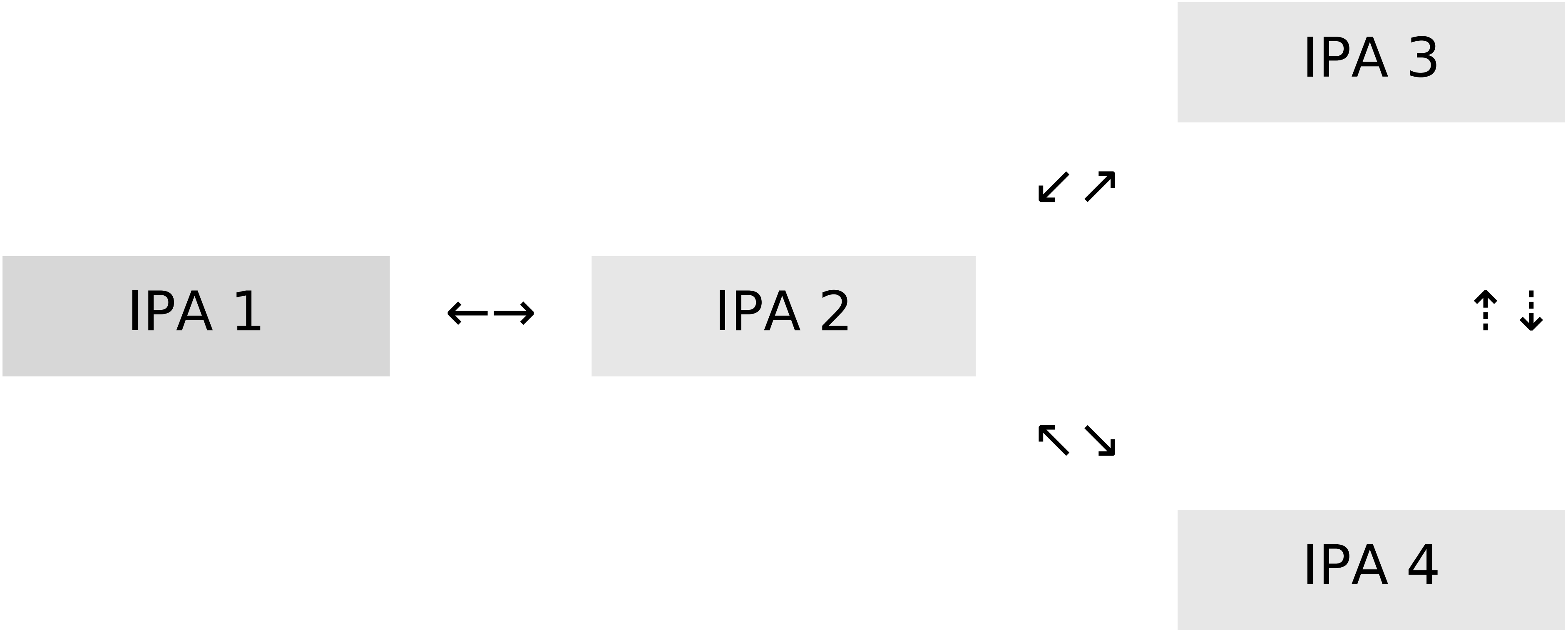
```
ipa1# ipa topologysegment-find realm
------------------
2 segments matched
------------------
  Segment name: ipa1.example.test-to-ipa2.example.test
  Left node: ipa1.example.test
  Right node: ipa2.example.test
  Connectivity: both

  Segment name: ipa2.example.test-to-ipa3.example.test
  Left node: ipa2.example.test
  Right node: ipa3.example.test
  Connectivity: both
----------------------------
Number of entries returned 2
----------------------------
```

Topology plugin

- Segment is added by creating it in directory server.
  - Information gets replicated to the target nodes.
  - New replication agreement is established.
- CA and Password Vault information is included.
  - Not all nodes need to have CA and Vault installed.

Topology management

- Drive topology from one place.



IPA 3

↙ ↗

IPA 1 ←→ IPA 2 ⇡ ⇣

↖ ↘

IPA 4

- From IPA 1, segment between IPA 3 and IPA 4 can be added.

```
ipa1# ipa topologysegment-add realm ...
```

Conclusion

- Replica promotion — directly from IPA-enrolled client.
- Client can be created, enrolled, and promoted without manual action on master.
- Replication topology is now in shared data.
- Management from one node possible.
- Coming in FreeIPA 4.3 release.

References

- www.freeipa.org/page/V4/Replica_Promotion
- www.freeipa.org/page/V4/Manage_replication_topology