

# Enhancements to FreeIPA Replication Topology Management

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



6<sup>th</sup> 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

freelPA

Identity Policy Authentication Network Services IPA Server

Users User Groups Hosts Host Groups Netgroups Services Automen

## User Groups

Search 

<input type="checkbox"/>	Group name	GID	Description
<input type="checkbox"/>	<a href="#">admins</a>	147400000	Account administrators group
<input type="checkbox"/>	<a href="#">editors</a>	147400002	Limited admins who can edit oth
<input type="checkbox"/>	<a href="#">ipausers</a>		Default group for all users
<input type="checkbox"/>	<a href="#">trust admins</a>		Trusts administrators group

Showing 1 to 4 of 4 entries.

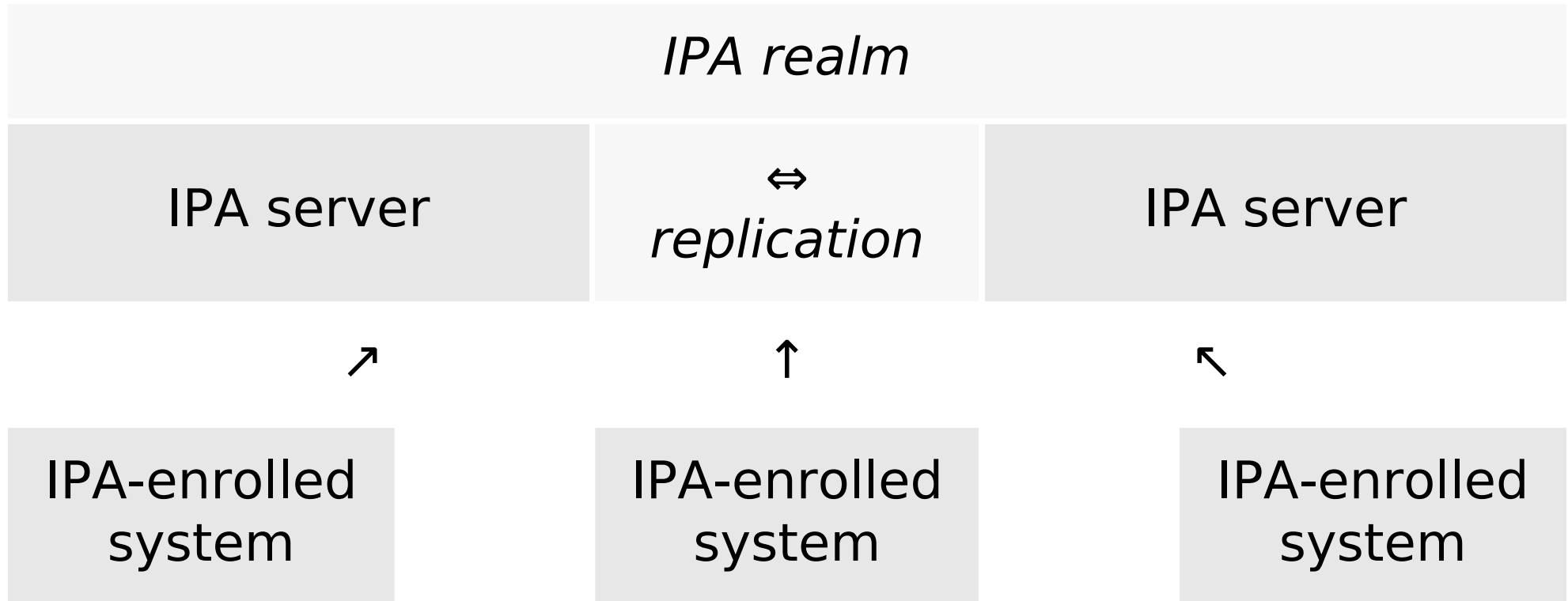
# IPA-enrolled systems

- 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/sss/sss.conf
[domain/example.test]
ipa_server = _srv_, ipa1.example.test
...
```

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

# FreeIPA replication



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

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

```
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.

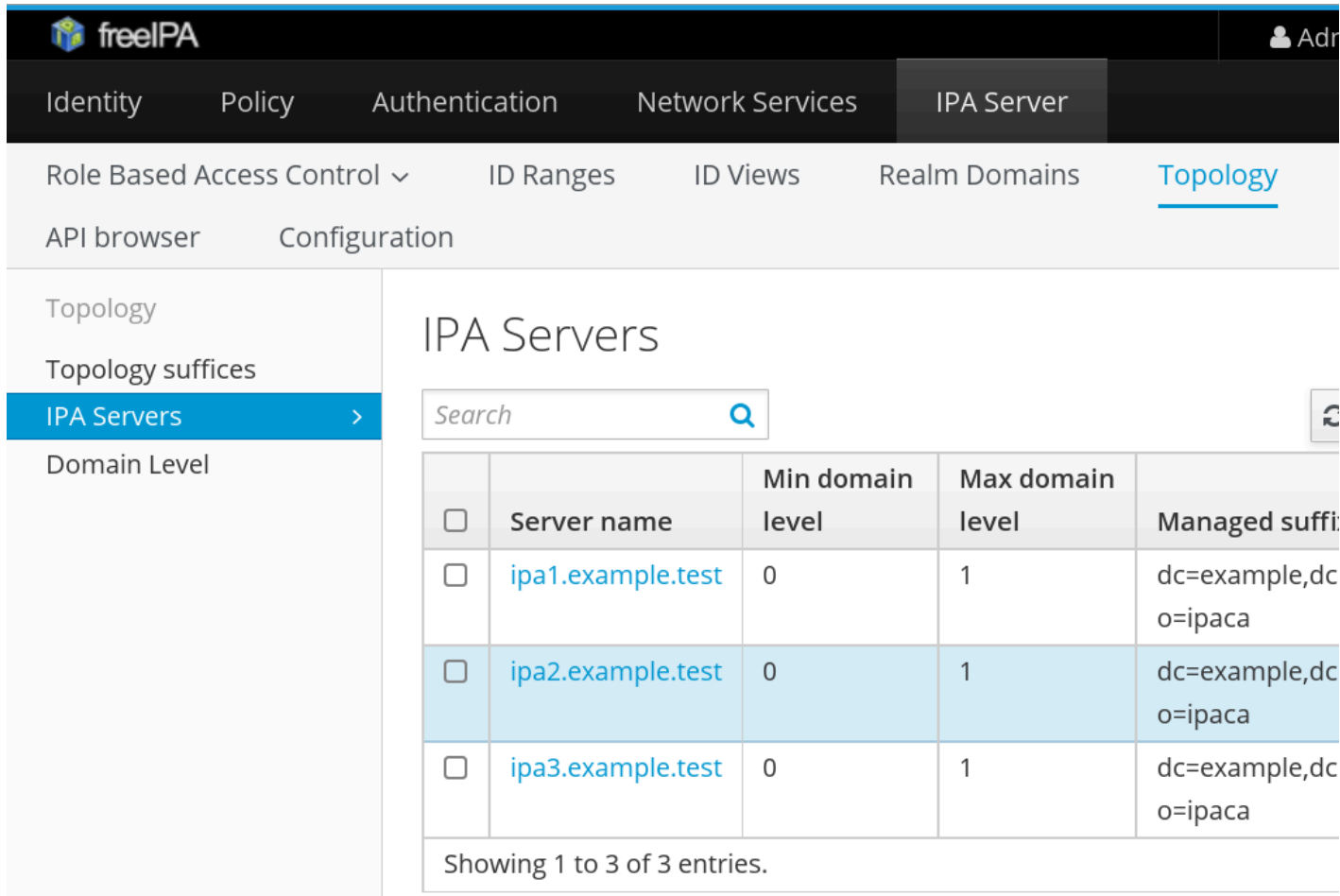
```
xmlrpc_uri = https://ipa2.example.test/ipa/xml
```

- 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.



The screenshot shows the FreeIPA web interface. The top navigation bar includes 'freelPA' and a user profile icon. Below this, a secondary navigation bar contains 'Identity', 'Policy', 'Authentication', 'Network Services', and 'IPA Server'. A third navigation bar includes 'Role Based Access Control', 'ID Ranges', 'ID Views', 'Realm Domains', and 'Topology' (which is underlined). Below this, there are links for 'API browser' and 'Configuration'. On the left side, a sidebar menu shows 'Topology', 'Topology suffices', 'IPA Servers' (highlighted with a blue bar and a right-pointing arrow), and 'Domain Level'. The main content area is titled 'IPA Servers' and features a search box with the placeholder text 'Search' and a magnifying glass icon. Below the search box is a table with the following data:

<input type="checkbox"/>	Server name	Min domain level	Max domain level	Managed suffi
<input type="checkbox"/>	<a href="#">ipa1.example.test</a>	0	1	dc=example,dc o=ipaca
<input type="checkbox"/>	<a href="#">ipa2.example.test</a>	0	1	dc=example,dc o=ipaca
<input type="checkbox"/>	<a href="#">ipa3.example.test</a>	0	1	dc=example,dc o=ipaca

Below the table, it says '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

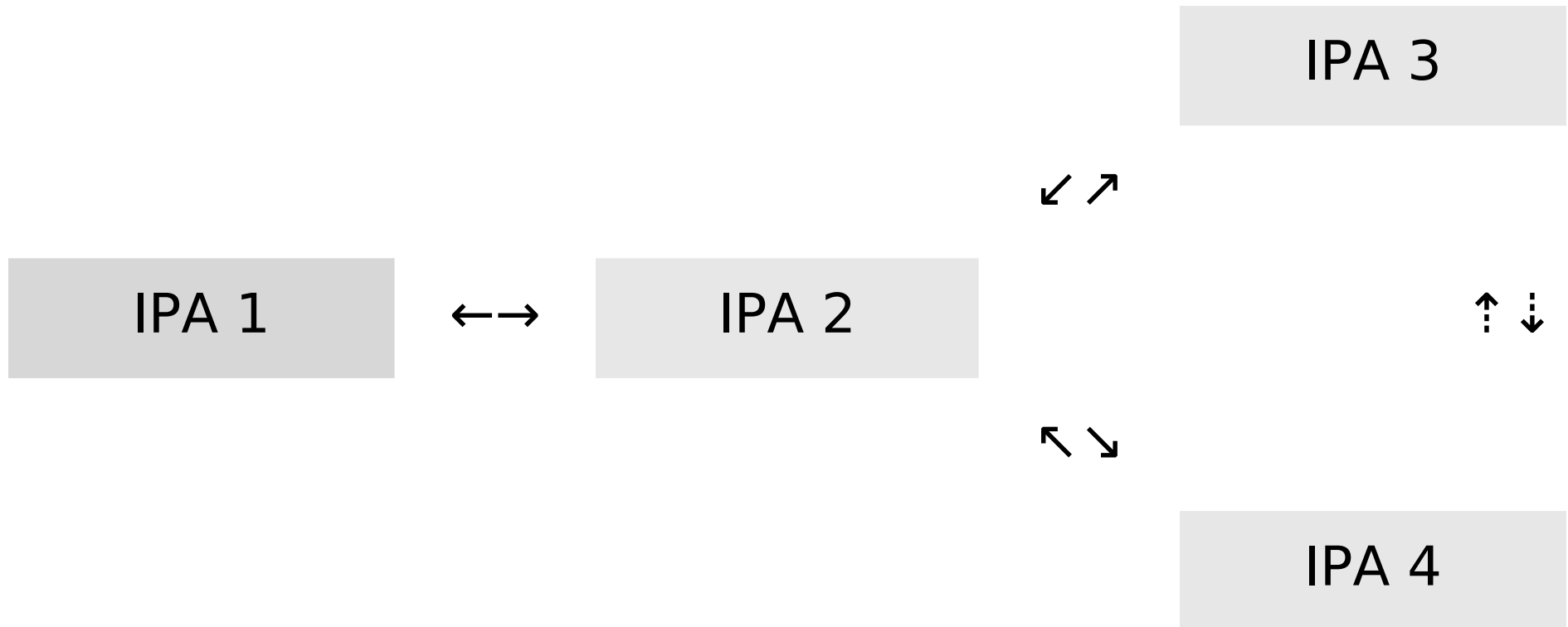
-----
Number of entries returned 2
-----
```

# 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.



- 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](http://www.freeipa.org/page/V4/Replica_Promotion)
- [www.freeipa.org/page/V4/Manage\\_replication\\_topology](http://www.freeipa.org/page/V4/Manage_replication_topology)