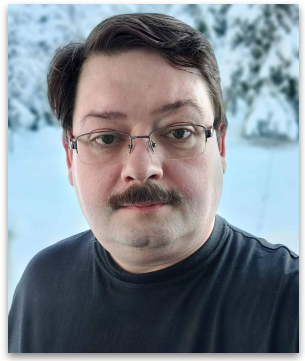
Red Hat Summit

Experiencing FreeIPA before RHEL Identity Management

Dynamic inventory in ansible-freeipa



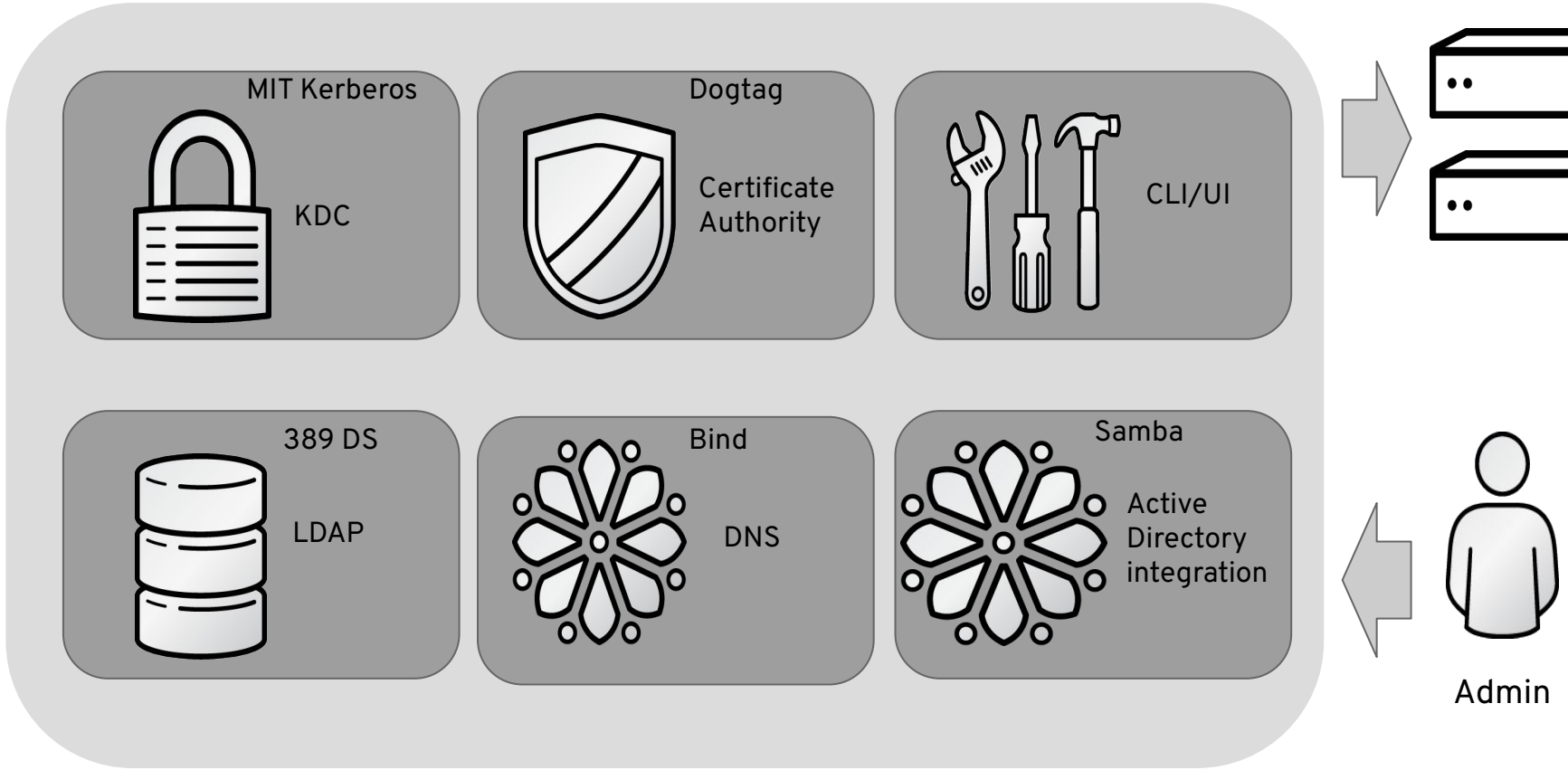
Alexander Bokovoy,
Senior Principal
Software Engineer

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

`ansible-freeipa` Ansible collection

- Roles and playbooks to install and manage IdM systems and resources
  - Server, replica and client deployment
  - Cluster deployments: server, replicas and clients in one playbook
  - One-time-password (OTP) support for client installation
  - Repair mode for clients
  - Backup and restore, also to and from controller
  - Smartcard setup for servers and clients
  - Inventory plugin
- Modules for almost every IdM resource

Inventory plugin

- Sources IdM servers from the deployment
  - Filters by role: “IPA master”, “CA server”, “KRA server”, “DNS server”, “AD trust controller”, “AD trust agent”
- Usage

<freeipa.yml>

```
---
plugin: freeipa.ansible_freeipa.freeipa
server: server.ipa.local
ipaadmin_password: some_value
```

```
$ ansible-inventory -v -i freeipa.yml --graph
```

Inventory plugin

Variable	Description	Required
`ipaadmin_principal`	The admin principal is a string and defaults to `admin`	no
`ipaadmin_password`	The admin password is a string and is required if there is no admin ticket available on the node	no
`server`	The FQDN of server to start the scan. (string)	yes
`verify`	The server TLS certificate file for verification (/etc/ipa/ca.crt). Turned off if not set. (string)	yes
`role`	The role(s) of the server. If several roles are given, only servers that have all the roles are returned. (list of strings) (choices: "IPA master", "CA server", "KRA server", "DNS server", "AD trust controller", "AD trust agent")	no
`inventory_group`	The inventory group to create. The default group name is "ipaservers".	no

Red Hat Summit

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat