



freeIPA
identity | policy | audit

FreeIPA Training Series

SSH Public Keys in FreeIPA

Jan Cholasta

01-15-2013



Introduction to SSH public key management (1)

- Public key cryptography in SSH:
 - Is used to authenticate hosts (by SSH client)
 - Can be used to authenticate users (by SSH server)
- Therefore:
 - Host public keys must be available to SSH clients
 - User public keys must be available to SSH servers
- How to manage these public keys?



Introduction to SSH public key management (2)

- Usually, public keys are stored in OpenSSH-style files
 - Host public keys are in `known_hosts` files (global or per-user)
 - User public keys are in `authorized_keys` file (per-user)
- Public keys are managed by manipulating these files on each system
 - Manually editing them by the administrator or user
 - Automatically generating them by some tool
 - Distributing them from a central location



Motivation

- Manipulating files
 - Might not scale well for a large set of systems
 - There might be issues when the server / central location is offline
- Store SSH public keys in FreeIPA and use SSSD to provide them to SSH client and server software
 - SSSD requests public keys of a host / user on demand
 - SSSD caches public keys for offline use



FreeIPA SSH LDAP schema

- Attribute `ipaSshPubKey`
 - Contains public keys in OpenSSH format
- Abstract object class `ipaSshGroupOfPubKeys`
 - Base object class of containers of public keys
- Auxiliary object class `ipaSshUser`
 - Container of user public keys
- Auxiliary object class `ipaSshHost`
 - Container of host public keys



FreeIPA installer

- Tools `ipa-server-install` and `ipa-client-install`:
 - Enable OpenSSH integration in SSSD
 - Configure OpenSSH (both `ssh` and `sshd`)
 - `--no-ssh` disables `ssh` configuration
 - `--no-sshd` disables `sshd` configuration
 - `--ssh-trust-dns` configures `ssh` to use DNS SSHFP records to authenticate hosts instead of SSSD (does not work without DNSSEC!)
 - Store host public keys from `/etc/ssh` in FreeIPA
 - `--no-dns-sshfp` disables automatic update of SSHFP DNS records



FreeIPA management tools

- Use `host` commands to manage host public keys
 - Option `--sshpubkey` of `host-add` and `host-mod`
 - Automatic update of SSHFP DNS records with `--updatedns` flag of `host-add`, `host-mod` and `host-del`
- Use `user` commands to manage user public keys
 - Option `--sshpubkey` of `user-add` and `user-mod`
- Public keys in FreeIPA use OpenSSH `authorized_keys` format



FreeIPA SSH public key management example

- Add a user with multiple SSH public keys:

```
$ ipa user-add user --sshpubkey='ssh-rsa AAAA...'  
--sshpubkey='ssh-dss AAAA...'
```

- Add new SSH public keys to a host and update DNS:

```
$ ipa host-mod host.example.com  
--addattr='ipasshpubkey=ssh-rsa AAAA...' --updatedns
```

(note that you have to use `--addattr` in order to add new keys without removing the old ones)



Debugging FreeIPA installer

- Check installer log files
 - `/var/log/ipaserver-install.log`
 - `/var/log/ipaclient-install.log`



Debugging FreeIPA management tools

- Check FreeIPA server log
 - `/var/log/httpd/error_log`

- Check LDAP

```
$ ldapsearch -H ldap://ipaserver.example.com  
-Y GSSAPI -b <basedn>
```

- For users, `<basedn>` is
`uid=<username>,cn=users,cn=accounts,dc=example,dc=com`
- For hosts, `<basedn>` is
`fqdn=<hostname>,cn=hosts,cn=accounts,dc=example,dc=com`



More information

- “SSSD and OpenSSH Integration” slides
- OpenSSH manual pages
 - `sshd(8)`
- FreeIPA management tool help
 - `ipa help host`, `ipa help user`
- FreeIPA manual pages
 - `ipa-server-install(1)`,
`ipa-client-install(1)`