

oVirt 3.6 aaa-jdbc provider

Manage your users/groups using database

Martin Peřina

Software Engineer at Red Hat

- Introduction
- Managing user/groups/passwords
- Configuration of additional domains

Introduction

- **'internal' domain**
 - provided by legacy internal provider
 - only one user and no groups
 - ability to change password
 - admin user cannot be disabled (locked)
- **LDAP domains**
 - provided by kerbldap and aaa-ldap providers
 - unlimited numbers of users and groups
 - user/group management is done by LDAP tools

- **LDAP domains**
 - same as in previous version
- **Database domains**
 - provided by new aaa-jdbc provider
 - unlimited number of users and groups
 - user/group management is done by command line tool
 - **'internal'** domain is also provided by aaa-jdbc and it's configured during installation/upgrade

- Complete user/group/password management using provided command line tool
- Plugged into engine using engine AAA extension API
- Users/groups/passwords are stored in PostgreSQL database
- Ability to provide multiple domains (stored in one or multiple PostgreSQL databases)
- More information at http://www.ovirt.org/Features/AAA_JDBC

Managing user/groups/passwords

ovirt-aaa-jdbc-tool **user** <COMMAND> <...>

- <COMMAND>
 - add
 - edit
 - delete
 - show
 - unlock

`ovirt-aaa-jdbc-tool user password-reset <...>`

- Password can be specified in one of the following formats:
 - interactive
 - on command line
 - using environment variable
 - using a file
 - setting empty password
- By default new password expires at the same moment as it's set

ovirt-aaa-jdbc-tool **group** <COMMAND> <...>

- <COMMAND>
 - add
 - edit
 - delete
 - show

ovirt-aaa-jdbc-tool **group-manage** <COMMAND> <...>

- <COMMAND>
 - useradd
 - userdel
 - groupadd
 - groupdel
 - show

```
ovirt-aaa-jdbc-tool query --what=<ENTITY> <...>
```

- <ENTITY>
 - user
 - group

ovirt-aaa-jdbc-tool **settings** <COMMAND> <...>

- <COMMAND>
 - set
 - show

Configuration of additional domains

- 'internal' domain configured during setup (using engine database)
- additional domains can be configured manually
- each domain can be installed
 - local or remote database
 - unique user per domain or shared user with unique schema name per domain

- Profile is oVirt AAA extension API term for domain
- Configuration files
 - **/etc/ovirt-engine/extensions.d**
 - <PROFILE>-authn.properties
 - <PROFILE>-authz.properties
 - **/etc/ovirt-engine/aaa**
 - <PROFILE>.properties
- Documentation provided in **/usr/share/doc/ovirt-engine-extension-aaa-jdbc-1.0.0/README.admin**
- Templates provided in **/usr/share/ovirt-engine-extension-aaa-jdbc/examples**

THANK YOU!

<http://www.ovirt.org>
mperina@redhat.com
mperina at #ovirt (irc.oftc.net)