

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

Bright OpenStack 7.3 uses a backend driver to communicate with AD using LDAP.

This keystone backend driver allows the administrator to use both the LDAP and the old SQL driver for the current users.

Integrate and activate driver

In order to integrate and activate this driver the following needs to be done:

```
#cmsh
```

```
#openstack
```

```
#settings
```

```
%authentication
```

```
%authbackends
```

```
%remove sql
```

```
%add ldap ad
```

```
show
```

```
Parameter
```

```
Value
```

```
-----  
Assignment driver
```

```
keystone.assignment.backends.sql.Assignment
```

```
Identity driver
```

```
keystone.identity.backends.Ldap.Identity
```

```
Revision
```

```
Type
```

```
OpenStackAuthBackendLDAP
```

```
Alias dereferencing
```

```
Default
```

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

Allow subtree delete	no
Chase referrals	no
Name	ad
Password	*****
Query scope	Subtree
Suffix	DC=lab,DC=local
TLS	no
URL	ldap://lab.local
Use dumb member	no
Username	bright
Group settings	<submode>
User settings	<submode>
Use SQL backend for assignments	yes
SQL Backend	<submode>
Use connection pool	no

Multiple variables can be set, based on the need. A run through with the simplest configuration is shown here:

```
%set url
```

```
%set username
```

```
%set password
```

```
%set chasereferrals no
```

```
%set suffix
```

Configure settings and filters

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

The usersettings submode and groupsettings submode need to be accessed to configure settings and filters :

```
%usersettings
```

```
%show
```

```
show
```

Parameter	Value
-----------	-------

Additional attribute mappings

Allow create	no
--------------	----

Allow delete	no
--------------	----

Allow update	no
--------------	----

Default project ID attribute

Enabled default	True
-----------------	------

Enabled emulation	no
-------------------	----

Ignored attributes	default_project_id,tenants
--------------------	----------------------------

Revision

Enabled attribute	enabled
-------------------	---------

Enabled attribute inverted	no
----------------------------	----

Enabled bit	0
-------------	---

Filter

Group member mapped attribute	uid
-------------------------------	-----

ID attribute	sAMAccountName
--------------	----------------

Mail attribute	mail
----------------	------

Name attribute	sAMAccountName
----------------	----------------

Page 3 / 7

(c) 2020 Bright Computing <kb@brightcomputing.com> | 2020-10-30 00:01

URL: <http://oldkb.brightcomputing.com/faq/index.php?action=artikel&cat=24&id=366&artlang=en>

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

Object class	person
Password attribute	userPassword
Tree DN	DC=lab,DC=local

Any of the following variables can be used to match the setup. The following are used as an example:

```
%set idattribute sAMAccountName;  
  
%set nameattribute sAMAccountName;  
  
%set objectclass person;  
  
%set treedn "yourdn"
```

The filter can be set too:

```
%set filter ""  
  
%..
```

Groupsettings submode can then be accessed one level up:

```
%groupsettings  
  
%show
```

Parameter	Value

Additional attribute mappings

Allow create	no
Allow delete	no
Allow update	no

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

Ignored attributes

Revision

Description attribute description

Filter

ID attribute sAMAccountName

Member attribute member

Name attribute cn

Object class group

Tree DN DC=lab,DC=local

The following values are used here:

```
%set idattribute sAMAccountName;
```

```
%set memberattribute member;
```

```
%set objectclass group;
```

```
%set threedn <SEARCH TREE>;
```

```
%..
```

The configuration can now be committed:

```
%commit
```

create ldap domain and project

cmsh can be exited now. From the head node, the following can be executed:

```
#openstack domain create ldap
```

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

openstack-keystone must be restarted on all of the controllers

```
#csh
```

```
%device
```

```
%foreach -n controller1..controller3 (services; restart openstack-keystone)
```

csh can be exited now. Users must now be listed for the first time so that OpenStack can create mappings

From the head node, the following is run:

```
#openstack user list --domain ldap
```

After, an ldap project must be created, and users must be assigned as members for this project. It is also an option to set up one of the users as admin.

```
#openstack project create ldap --domain $(openstack domain list -f value | grep ldap | awk '{print $1}')
```

The following example script can be used to assign all users to the ldap project as members :

```
for i in $(openstack user list -f value --domain ldap -c Name ); do openstack role add --user $i --project <ldap project id > --user-domain < ldap domain id> member ; done
```

It is also possible to login using horizon , navigate to the OpenStack dashboard and use the following as input :

domain -> ldap

user -> your AD user

password -> Your AD password

Unique solution ID: #1366

Author: Frank Furter

OpenStack: How can I integrate Bright OpenStack 7.3 Keystone with LDAP/AD?

Last update: 2017-07-11 12:56