
The LDAP plugin for Fuel documentation

Release 3.0-3.0.2-1

Mirantis Inc.

March 15, 2017

CONTENTS

1	Plugin Guide	1
1.1	LDAP plugin for Fuel	1
1.2	Release notes / Changelog	1
1.3	LDAP plugin limitations	2
1.4	Installation Guide	2
1.5	Configuring LDAP plugin	2
1.6	User Guide	14
1.7	LDAP plugin validation	15
1.8	Troubleshooting	16
1.9	Appendix	16

PLUGIN GUIDE

1.1 LDAP plugin for Fuel

This plugin extends Mirantis OpenStack functionality by adding LDAP support. It allows to use an existing LDAP server as authentication backend for Keystone. Enabling this plugin means that all users except system users will be authenticated against the configured LDAP server.

Please note that Fuel will not validate the settings, e.g. by attempting to connect to the LDAP server.

1.1.1 Requirements

Requirement	Version/Comment
Fuel	9.0
Pre-configured LDAP server	

LDAP server should be pre-deployed and be accessible via Public network from Controller nodes.

1.2 Release notes / Changelog

3.0.2

- Security fix: ldap password is removed from puppet logs [LP #1658655]

3.0.1

- Tasks version 2.0.0 is set by default [LP #1638617]

3.0.0

- Support of ldap proxy
- Compatibility with MOS 9.0

2.0.0

- Support of multi-domains
- Compatibility with MOS 8.0

1.0.0

- This is the first release of the plugin

1.3 LDAP plugin limitations

1. LDAP plugin has the following limitations:

- Installation of LDAP plugin before deployment only;
- Fuel will not validate the settings, e.g., by attempting to connect to the LDAP server;
- In multidomain configuration the attributes of the first domain are filled in the web form, whereas the attributes of other domains are filled in one field;
- The settings of domains determined in “List of additional Domains” field will not be validated;
- The settings of proxy determined in “List of custom LDAP proxy configs” field will not be validated;

1.4 Installation Guide

1.4.1 Installing LDAP plugin

To install LDAP plugin, follow these steps:

1. Download the plugin from the [Fuel Plugins Catalog](#).
2. Copy the plugin on an already installed Fuel Master node (SSH can be used for that). If you do not have the Fuel Master node yet, see [Quick Start Guide](#):

```
# scp ldap-3.0-3.0.2-1.noarch.rpm root@<Fuel_Master_IP>:/tmp
```

3. Log into the Fuel Master node. Install the plugin:

```
# cd /tmp
# fuel plugins --install ldap-3.0-3.0.2-1.noarch.rpm
```

4. Check if the plugin was installed successfully

```
# fuel plugins
id | name | version | package_version | releases
---+-----+-----+-----+-----
1  | ldap | 3.0.2   | 3.0.0           | ubuntu (mitaka-9.0)
```

1.5 Configuring LDAP plugin

1. Create a new OpenStack environment to use an existing LDAP server as authentication backend for Keystone. For more information about environment creation, see [Mirantis OpenStack User Guide](#).
2. Open *Settings* tab of the Fuel Web UI, scroll the page down and select the *LDAP plugin for Keystone* checkbox:

Dashboard
Nodes
Networks
Settings
Logs
Health Check

OpenStack Settings

General
Security
Compute
Storage
Logging
OpenStack Services
Other

☐ LDAP plugin for Keystone

Versions
3.0.0

Domain name
Name of the Keystone domain

LDAP URL
URL for connecting to the LDAP server.

☐ LDAP proxy
Enable LDAP proxy.

☐ Use TLS
Enable TLS for communicating with the LDAP server.

CA Chain
CA trust chain in PEM format.

LDAP Suffix
cn=example,cn=com
LDAP server suffix.

LDAP User
cn=admin,dc=local
User BindDN to query the LDAP server.

LDAP User Password
Password for the BindDN to query the LDAP server.

LDAP Query Scope

☒ one
onelevel/singleLevel scope for LDAP queries

☐ sub
subtree/wholeSubtree scope for LDAP queries

Users Tree DN
ou=Users,dc=example,dc=com
Search base for users.

User Filter
LDAP search filter for users.

User Object Class
inetOrgPerson
LDAP objectclass for users.

User ID Attribute
cn
LDAP attribute mapped to user id.

User Name Attribute
sn
LDAP attribute mapped to user name.

User Password Attribute
userPassword
LDAP attribute mapped to password.

User Enabled/Disabled Attribute
enabled
LDAP attribute mapped to enabled/disabled.

Groups Tree DN
ou=Groups,dc=example,dc=com
Search base for groups.

Dashboard
Nodes
Networks
Settings
Logs
Health Check

OpenStack Settings

General
Security
Compute
Storage
Logging
OpenStack Services
Other

☒ LDAP plugin for Keystone

Versions
3.0.0

Domain name
Domain name contains unexpected value. Must only contain letters, numbers and characters . / _ / -

LDAP URL
LDAP URL is not valid. Should be e.g. 'ldap://example.com'.

☐ LDAP proxy
Enable LDAP proxy.

☐ Use TLS
Enable TLS for communicating with the LDAP server.

CA Chain
CA trust chain in PEM format.

LDAP Suffix
LDAP server suffix.

LDAP User
User BindDN to query the LDAP server.

LDAP User Password
Password must not contain spaces.

LDAP Query Scope

☒ one
onelevel/singleLevel scope for LDAP queries

☐ sub
subtree/wholeSubtree scope for LDAP queries

Users Tree DN
Search base for users.

User Filter
LDAP search filter for users.

User Object Class
LDAP objectclass for users.

User ID Attribute
LDAP attribute mapped to user id.

User Name Attribute
LDAP attribute mapped to user name.

User Password Attribute
LDAP attribute mapped to password.

User Enabled/Disabled Attribute
LDAP attribute mapped to enabled/disabled.

Groups Tree DN
Search base for groups.

3. Enter plugin settings into the text fields:

☒ LDAP plugin for KeystoneVersions ☒ 3.0.0

Domain name	ldap1	Name of the Keystone domain
LDAP URL	ldap://172.16.56.27	URL for connecting to the LDAP server.
☒ LDAP proxy	Enable LDAP proxy.	
☒ Use TLS	Enable TLS for communicating with the LDAP server.	
CA Chain	-----BEGIN CERTIFICATE----- MIIDNzCCA... -----END CERTIFICATE-----	CA trust chain in PEM format.
LDAP Suffix	dc=openldap1,dc=tld	LDAP server suffix.
LDAP User	cn=admin,dc=openldap1,dc=tld	User BindDN to query the LDAP server.
LDAP User Password	*****	Password for the BindDN to query the LDAP server.

LDAP Query Scope

- ☐ one
onelevel/singleLevel scope for LDAP queries
- ☒ sub
subtree/wholeSubtree scope for LDAP queries

Users Tree DN	dc=openldap1,dc=tld	Search base for users.
User Filter		LDAP search filter for users.
User Object Class	inetOrgPerson	LDAP objectclass for users.
User ID Attribute	cn	LDAP attribute mapped to user id.
User Name Attribute	sn	LDAP attribute mapped to user name.
User Password Attribute	userPassword	LDAP attribute mapped to password.
User Enabled/Disabled Attribute	enabled	LDAP attribute mapped to enabled/disabled.
Groups Tree DN	dc=openldap1,dc=tld	Search base for groups.
Group Filter		LDAP search filter for groups.
Group Object Class	groupOfNames	LDAP objectclass for groups.
Group ID Attribute	cn	LDAP attribute mapped to group id.

1.5. Configuring LDAP plugin

Group Name Attribute		LDAP attribute mapped to group name.
Group Member Attribute	member	LDAP attribute that maps user to group.

Specify domain name, LDAP URL, LDAP suffix:

☒ LDAP plugin for Keystone

Versions ☒ 3.0.0

Domain name	ldap1	Name of the Keystone domain
LDAP URL	ldap://172.16.56.27	URL for connecting to the LDAP server.
LDAP Suffix	dc=openldap1,dc=tld	LDAP server suffix.
LDAP User	cn=admin,dc=openldap1,dc=tld	User BindDN to query the LDAP server.

Enable TLS use and put certificate if it is needed:

☒ Use TLS
Enable TLS for communicating with the LDAP server.

CA Chain

```
-----BEGIN CERTIFICATE-----
MIIDNzCCA+gAwIBAgIMV2wFCgCodNwbbGRwMA0GCSqGSIb3DQEBCwUAMBQx
EjAQ
BgNVBAMTCW9wZW5sZGFwMTAeFw0xNjA2MjMxNTQ5MzBaFw00MzExMDgxNTQ
5MzBa
MCsxFtATBgNVBAMTDDE3MI4xNI41Ni4yNzESMBAGA1UEChMjb3BlbmxxYXAxMI
Gf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDEikRtXY/fGinlvR001IQQFDENKtYh
zxzHdFxb/fUuU/UCns82jwj0Ra7XoJY2O/X2eQoEP5UDSqYXlrTQRDmq2MDswX
MsCB50JV2uWMFGonlIsWhX6lus+dM/JAjtXuPll+09em+6zocICssSBtiGBfwwZe
l+LaaCsO79t+ZwiDAQABO3YwdDAMBgNVHRMBAf8EAJAAMBGA1UdJQMMAoG
CCsG
AQUFBwMBMA8GA1UdDwEB/wQFAwMHAAAwHQYDVR0OBBYEFF7LYI8IMQXQJW
Zg1Wc7
Y/+tWsnCMB8GA1UdIwQYMBaAFGpx2fdW6TSYycKPIE/sGf3L3EN3MA0GCSqGSIb3
DQEBCwUAA4IBgQBo2lqcUOAUt2agGyrXZPAuwhy6xjhJdGrFgBQ2025mkuUR1LgS
t+0Rfd90D7JHE2VoeZD6lomTn6KailbgM1/dkgwZQ0IdKrapQ4QbPzvuNJD8bnHYj
ou5l7PK6cwAOAPzOcmjrHLZuZHlBQw1XnmHjkZ4lc3ElXPWWu8KlUck5/JPWAqW
vn9QrIFol5p+wsTBWAmtdrIplvPX/fjy6l3Mfz6P53w3Y3+DWZJ24wualQwer6j
il/UGNgu66/OFd8lRmzAs19CHhfQTPY4xCZ0sBjCxoJ5efGbt/Aldg1A0Tb9UyCT
Z8no8/dk700n+vEXvtgtGj/+mfSSj9nOOZ4QoOHVZycTRUX0yBG/UllHchWYhEc9
pz+Fz7QyurmHVNg7zSt/5V1bITISTwoXIWFxfHQ+2fDT0oKewfbBiYhhppqfNMRkj
8zcBLEvlgDqUYroLLDP7UI5bBjb6JonoLorFjNwjQute9WPZn+h4yrXNqqVNL7a
mUWq4Agp+ylyt/0=
-----END CERTIFICATE-----
```

CA trust chain in PEM format.

Enable LDAP proxy and put custom config if it is needed:

☒ LDAP plugin for Keystone

Versions ☒ 3.0.0

Domain name

Name of the Keystone domain

LDAP URL

URL for connecting to the LDAP server.

☒ LDAP proxy
Enable LDAP proxy.

☒ Use TLS
Enable TLS for communicating with the LDAP server.

List of custom LDAP proxy
configs

```
config_for=base_config
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/nis.schema
modulepath /usr/lib/ldap
moduleload back_ldap
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
loglevel -1

config_for=ldap2
database ldap
suffix "dc=mirantis,dc=tld"
readonly yes
protocol-version 3
uri "ldap://172.18.196.224"
rootdn "dc=mirantis,dc=tld"
tls start tls_reqcert=demand tls_cacert=/etc/ssl/certs/
idassert-bind bindmethod=simple
        binddn="cn=admin,dc=mirantis,dc=tld"
        credentials="1111"
        mode=self
idassert-authzFrom "*"

```

List of custom LDAP proxy configs.

Specify LDAP user, password and other settings:

LDAP Suffix	dc=openldap1,dc=tld	LDAP server suffix.
LDAP User	cn=admin,dc=openldap1,dc=tld	User BindDN to query the LDAP server.
LDAP User Password	qwerty123! 	Password for the BindDN to query the LDAP server.

LDAP Query Scope

- ☐ one
 onelevel/singleLevel scope for LDAP queries
- ☒ sub
 subtree/wholeSubtree scope for LDAP queries

Users Tree DN	dc=openldap1,dc=tld	Search base for users.
User Filter		LDAP search filter for users.
User Object Class	inetOrgPerson	LDAP objectclass for users.
User ID Attribute	cn	LDAP attribute mapped to user id.
User Name Attribute	sn	LDAP attribute mapped to user name.
User Password Attribute	userPassword	LDAP attribute mapped to password.
User Enabled/Disabled Attribute	enabled	LDAP attribute mapped to enabled/disabled.

To use LDAP groups provide settings for it:

Groups Tree DN	dc=openldap1,dc=tld	Search base for groups.
Group Filter		LDAP search filter for groups.
Group Object Class	groupOfNames	LDAP objectclass for groups.
Group ID Attribute	cn	LDAP attribute mapped to group id.
Group Name Attribute	cn	LDAP attribute mapped to group name.
Group Member Attribute	member	LDAP attribute that maps user to group.
Group description Attribute	description	LDAP attribute mapped to description.

Fields description:

Field	Comment
Domain name	Name of the Keystone domain.
LDAP URL	URL for connecting to the LDAP server.
LDAP proxy	Enable LDAP proxy.
Use TLS	Enable TLS for communicating with the LDAP server.
CA Chain	CA trust chain in PEM format.
LDAP Suffix	LDAP server suffix.
LDAP User	User BindDN to query the LDAP server.
LDAP User Password	Password for the BindDN to query the LDAP server.
LDAP Query Scope	The LDAP scope for queries, this can be either “one” (onelevel/singleLevel) or “sub” (subtree/wholeSubtree).
Users Tree DN	Search base for users.
User Filter	LDAP search filter for users.
User Object Class	LDAP objectclass for users.
User ID Attribute	LDAP attribute mapped to user id.
User Name Attribute	LDAP attribute mapped to user name.
User Password Attribute	LDAP attribute mapped to password.
User Enabled/Disabled Attribute	LDAP attribute mapped to enabled/disabled.
Groups Tree DN	Search base for groups.
Group Filter	LDAP search filter for groups.
Group Object Class	LDAP objectclass for groups.
Group ID Attribute	LDAP attribute mapped to group id.
Group Name Attribute	LDAP attribute mapped to group name.
Group Member Attribute	LDAP attribute that maps user to group.
Group description Attribute	LDAP attribute mapped to description.
Page Size Attribute	Maximum results per page.
Chase referrals Attribute	Referral chasing behavior for queries.
List of additional Domains	Blocks of additional domains/parameters that should be created.
List of custom LDAP proxy configs	List of custom LDAP proxy configs.

- To deploy an environment with support of multiple domains ‘List of additional Domains’ text area should be used. All needed parameters that describes a domain should be copied there, all parameters form a block of parameters.

List of additional Domains

```

domain=ldap2
url=ldap://172.18.196.224
suffix=dc=mirantis,dc=tld
user=cn=admin,dc=mirantis,dc=tld
password=1111
query_scope=sub
user_tree_dn=dc=mirantis,dc=tld
user_objectclass=inetOrgPerson
user_id_attribute=cn
user_name_attribute=sn
user_pass_attribute=userPassword
user_enabled_attribute=enabled
user_allow_create=False
user_allow_update=False
user_allow_delete=False
user_filter=
group_tree_dn=dc=mirantis,dc=tld
group_objectclass=groupOfNames
group_id_attribute=cn
group_name_attribute=cn
group_desc_attribute=description
group_member_attribute=member
group_allow_create=False
group_allow_update=False
group_allow_delete=False
group_filter=
use_tls=True
ldap_proxy=true
ca_chain=-----BEGIN CERTIFICATE-----
MIIDRzCCAf+gAwIBAgIEVukIzDANBgkqhkiG9w0BAQsFADATMREwDwYDVQQDEwh
t
aXJhbnRpczAeFw0xNjAzMTYwOTIyMjBaFw0yNjAzMTQwOTIyMjBaBMBxETAPBgN
V
BAMTCG1pcmFudGlzMIIBUjANBgkqhkiG9w0BAQEFAAOCAT8AMIIBOgKCAATEAtvHJ
m7jqoTp8XtUNYin1sQK12bUTCKGo2Qdq8KCVFodnX8trAW7YNpMyyZ/eaKmkA
J
1Ta/SJl5j6KDjh2v2JwmwVZLYz6hXZraaNEZvaSe/N0a71s6C3io2oVyKPxSePgO
Agmv5DOYQLyGV8ccVHVQj0s//Q3Q88+KuMykGQO0I2LBo2z6cBrjDEkds+W34YeP
2ZQ2iFwT1GBcuog4CysFHdi0CYO40JUDNim+UP5EXOP+4f0T1JKbNGP7YnXyxm9d
/RPbiN8PDcgl0a3F4mFKW3kkWmtbfcggM8HkPcNHbLerXYQ3vqUmlKC0PH27x7K9
Bn0THo8hTalDhMfpjgFfruyvtn0yXMwfAaxXxtvCjz8AiF5dLZIF/QFr/+j81PM6
R6IKmQpIn/UDWG1SAQIDAQABo0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1U
dDwEB
/wQFAwMHBAawHQYDVR00OBByEFH5Q4yw2+u170/e1+IZ5cOZ4WPajMA0GCSqGS
lb3
DQEBcWUAA4IBMQCRPexLKa5nQV02VbGEr5iRik9WMD9yj7ygbKZvKH8QM2d48tn
f
1/1tgqIPwP5Hbl1zCLXdVwQgFjaz+fluGINZ5sqz+AB+av9KXoxVwTp1b7vo34u
bfKP42ECzAAmBlqs/RW2F2697oQlgy8koeFsMxFL/DHHm/pEK7AZrJUI5ANCgQ
rpQ5ngdk6UYCcRAet5ccc6pkzewnxixVy4JHcmdHc0CpBGdCzD++QbTlrz8sSq0
Q7A4gCbJNx/FAPqhrCeDS6tRiV81qONwy4GsPzo/6QuDHdKzUBsz19yRmJMiXCBU
KivmZtsndZ5Ce/1KV9OCfjZ6MpDE+OCegAsiD1MGeiBU9nKt3g2PpZBMHBP95EK
smMYTjyC1AGUSMThafp9nllfnRNurZSeU5GK
-----END CERTIFICATE-----

```

Blocks of additional domains/parameters that should be created.

To add multiple domains such block of parameters should be added to ‘List of additional Domains’ text area and these blocks should be separated by empty line.

5. To set up an environment with activated LDAP proxy ‘LDAP proxy’ checkbox should be selected. When only ‘LDAP proxy’ checkbox is selected: it activates LDAP proxy for base domain and activates LDAP proxy for

additional domains if they have 'ldap_proxy=true' parameter in their configurations.

☒ LDAP plugin for Keystone

Versions ☒ 3.0.0

Domain name

Name of the Keystone domain

LDAP URL

URL for connecting to the LDAP server.

☒ LDAP proxy
Enable LDAP proxy.

☒ Use TLS
Enable TLS for communicating with the LDAP server.

List of additional Domains

```
domain=ldap2
url=ldap://172.18.196.224
suffix=dc=mirantis,dc=tld
user=cn=admin,dc=mirantis,dc=tld
password=1111
query_scope=sub
user_tree_dn=dc=mirantis,dc=tld
user_objectclass=inetOrgPerson
user_id_attribute=cn
user_name_attribute=sn
user_pass_attribute=userPassword
user_enabled_attribute=enabled
user_allow_create=False
user_allow_update=False
user_allow_delete=False
user_filter=
group_tree_dn=dc=mirantis,dc=tld
group_objectclass=groupOfNames
group_id_attribute=cn
group_name_attribute=cn
group_desc_attribute=description
group_member_attribute=member
group_allow_create=False
group_allow_update=False
group_allow_delete=False
group_filter=
use_tls=True
ldap_proxy=true
ca_chain=-----BEGIN CERTIFICATE-----
```

In this case LDAP proxy configurations for LDAP domains are taken from templates located in the plugin. Configurations from the templates have minimal functionality and they are intended for testing needs.

To specify custom settings for LDAP proxy 'List of custom LDAP proxy configs' text area should be used. There can be specified base settings for a proxy service: 'includes', loglevel and etc. can be added to a proxy configuration file. For this 'config_for' parameter with 'base_config' value should be specified and after that needed settings should be added.

List of custom LDAP proxy
configs

```
config_for=base_config
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/nis.schema
modulepath /usr/lib/ldap
moduleload back_ldap
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
loglevel -1
```

List of custom LDAP proxy configs.

To specify custom settings for LDAP domain 'config_for' parameter with <domain_name> value should be added and after that custom settings can be specified.

List of custom LDAP proxy
configs

```
config_for=ldap2
database ldap
suffix "dc=mirantis,dc=tld"
readonly yes
protocol-version 3
uri "ldap://172.18.196.224"
rootdn "dc=mirantis,dc=tld"
tls start tls_reqcert=demand tls_cacert=/etc/ssl/certs/
ldassert-bind bindmethod=simple
binddn="cn=admin,dc=mirantis,dc=tld"
credentials="1111"
mode=self
ldassert-authzFrom ""
```

List of custom LDAP proxy configs.

Blocks of custom settings should be separated by empty line.

#.Continue with environment configuration and deploy it; for instructions, see [Fuel User Guide](#).

1. After successful environment deployment log into dashboard in default domain:



Domain

default

User Name

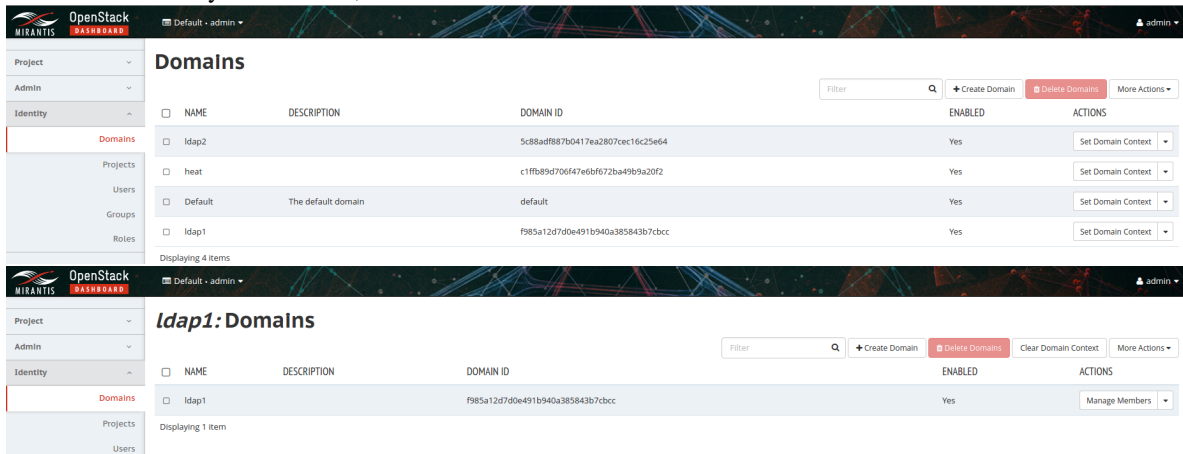
admin

Password

.....

Connect

2. Go to Identity -> Domains, select needed domain and 'Set Domain Context' for the domain:



Domains

NAME	DESCRIPTION	DOMAIN ID	ENABLED	ACTIONS
Idap2		5c88ad987b0417ea2807cec16c25e64	Yes	Set Domain Context
heat		c1fb89d706f47e6bf672ba49b9a20f2	Yes	Set Domain Context
Default	The default domain	default	Yes	Set Domain Context
Idap1		f985a12d7d0e491b940a385843b7cbcc	Yes	Set Domain Context

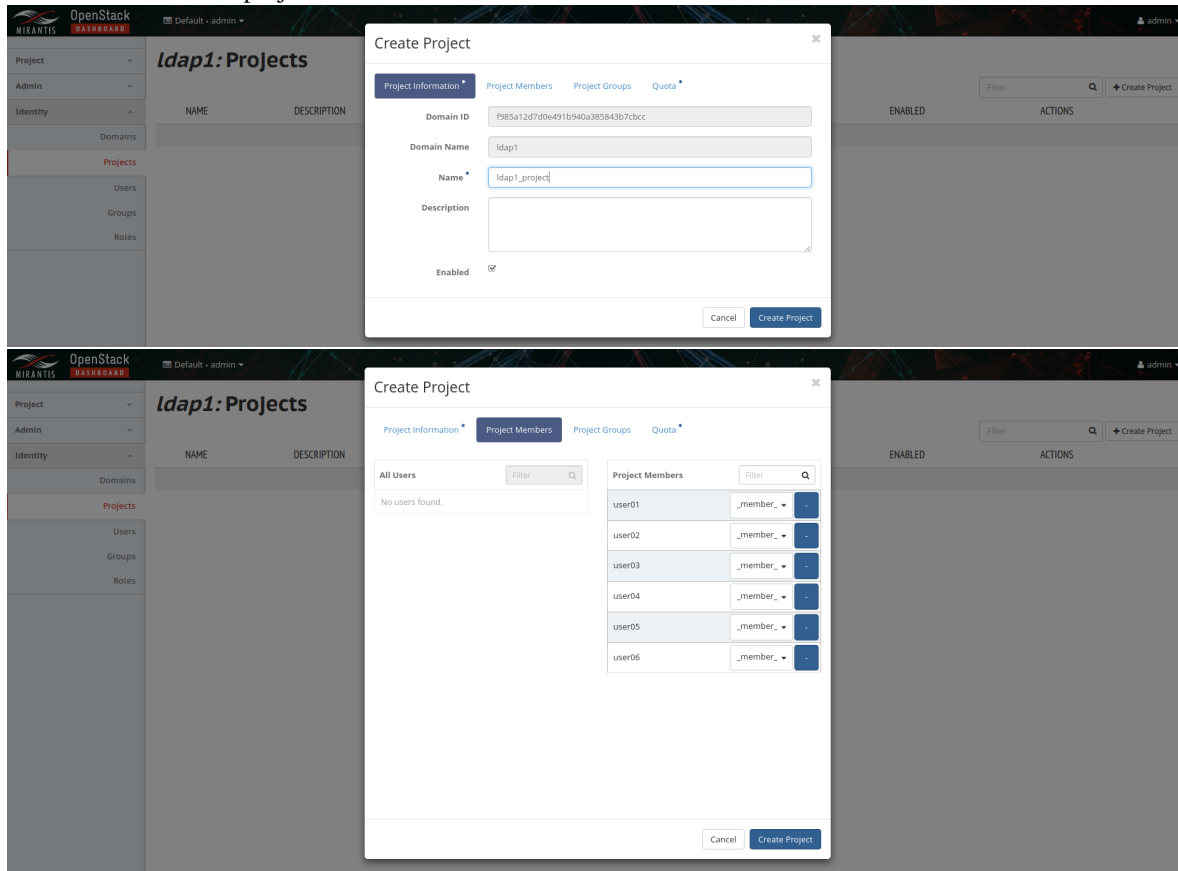
Displaying 4 items

Idap1: Domains

NAME	DESCRIPTION	DOMAIN ID	ENABLED	ACTIONS
Idap1		f985a12d7d0e491b940a385843b7cbcc	Yes	Manage Members

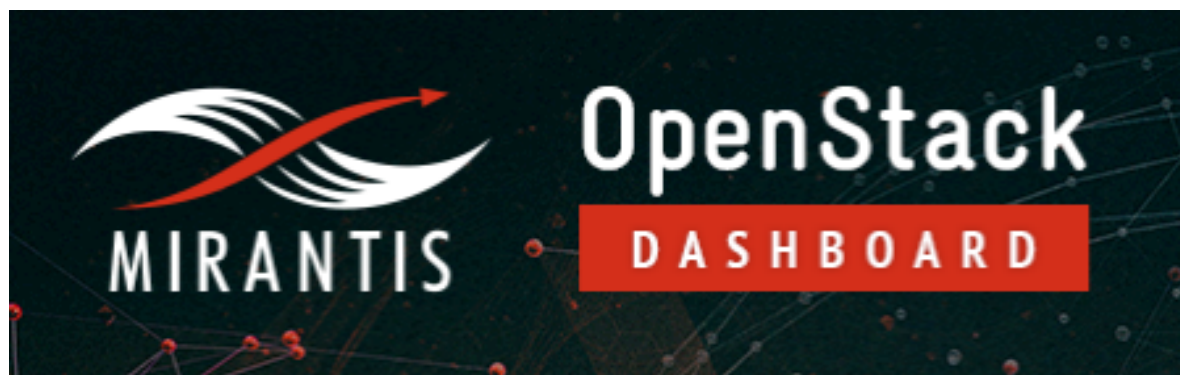
Displaying 1 item

3. Go to Identity -> Projects and select 'Create Project' to create a new project for the domain and add user members to the project:



1.6 User Guide

1. After successful deployment, all users from the LDAP directory matching the configured filter criteria can authenticate against Keystone. To validate the configuration, log into the Horizon dashboard using LDAP credentials:



Domain

ldap1

User Name

user01

Password

....|



Connect

1.7 LDAP plugin validation

1. To validate that LDAP plugin is successfully applied after deployment:
 - Log into Horizon using domain/user credentials from LDAP server;
 - Create an instance;

Expecting results:

- All LDAP users can authenticate via Keystone;
- An instance is successfully created;

1.8 Troubleshooting

1.8.1 Checking presence of LDAP domain/users

To get a list of domains in keystone run the following command on Controller node:

```
OS_IDENTITY_API_VERSION=3 openstack domain list
```

To get a list of users in a domain run the following command on Controller node:

```
OS_IDENTITY_API_VERSION=3 openstack user list --quiet --long --domain <domain_name>
```

1.8.2 Checking LDAP server availability

To check LDAP server availability run the following command on Controller node:

```
ldapsearch -H ldap://<url/ip_address> -x -b dc=<ldap>,dc=<suffix>
```

1.8.3 LDAP plugin log files

As LDAP plugin only updates keystone configuration files to check keystone service, these files keep logs:

/var/log/apache2/keystone_wsgi_admin_access.log

/var/log/apache2/keystone_wsgi_admin_error.log

/var/log/apache2/keystone_wsgi_main_access.log

/var/log/apache2/keystone_wsgi_main_error.log

1.9 Appendix

1.9.1 Links

- [Mirantis OpenStack Documentation Center](#)
- [Fuel Plugins Catalog](#)