The LDAP plugin for Fuel documentation

Release 3.0-3.0.1-1

Mirantis Inc.

January 24, 2017

CHAPTER

ONE

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

3.0.1

- 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-3.0-3.0.1-1.noarch.rpm root@<Fuel_Master_IP>:/tmp
   ```

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

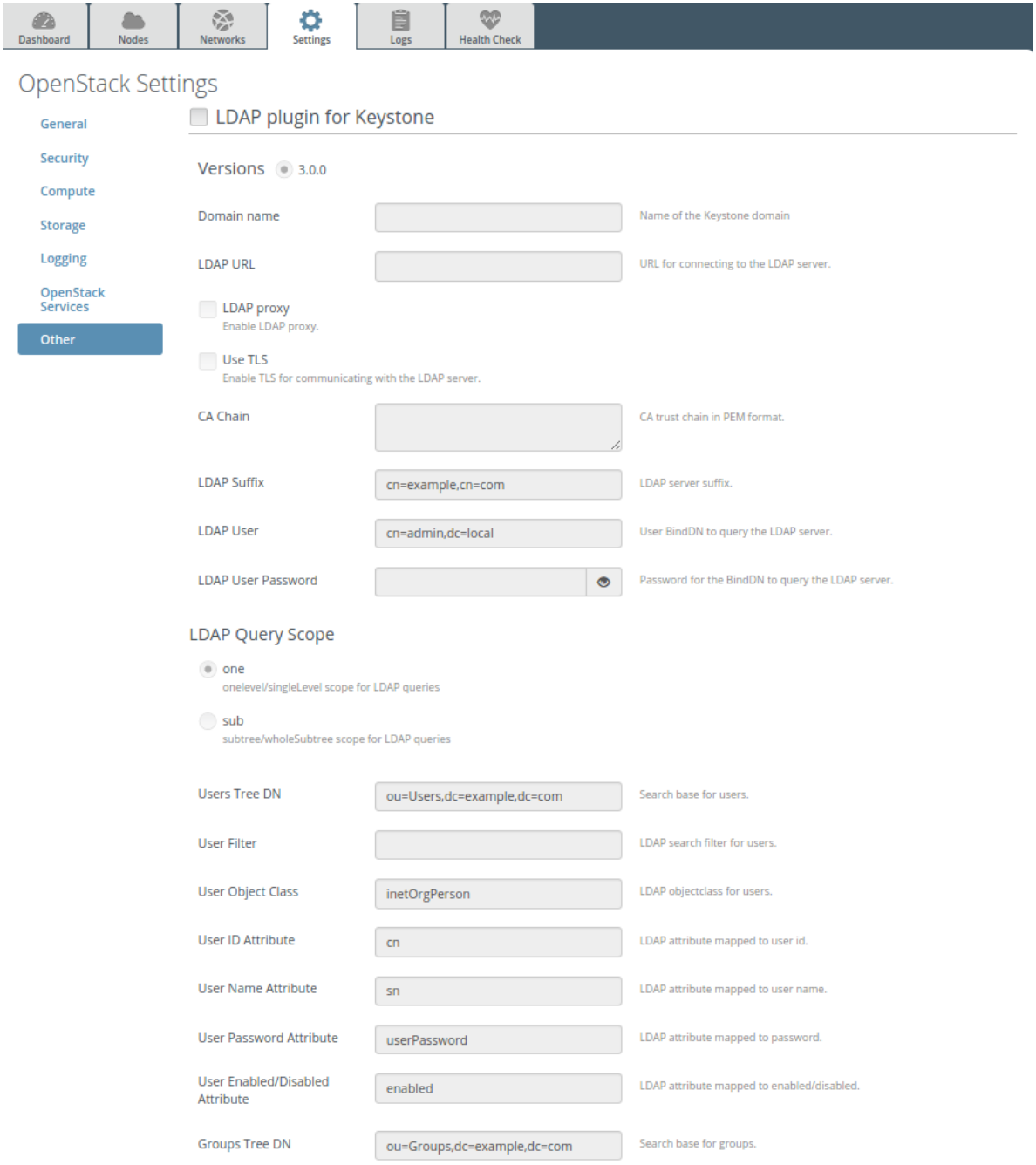
   ```
   # cd /tmp
   # fuel plugins --install ldap-3.0-3.0.1-1.noarch.rpm
   ```

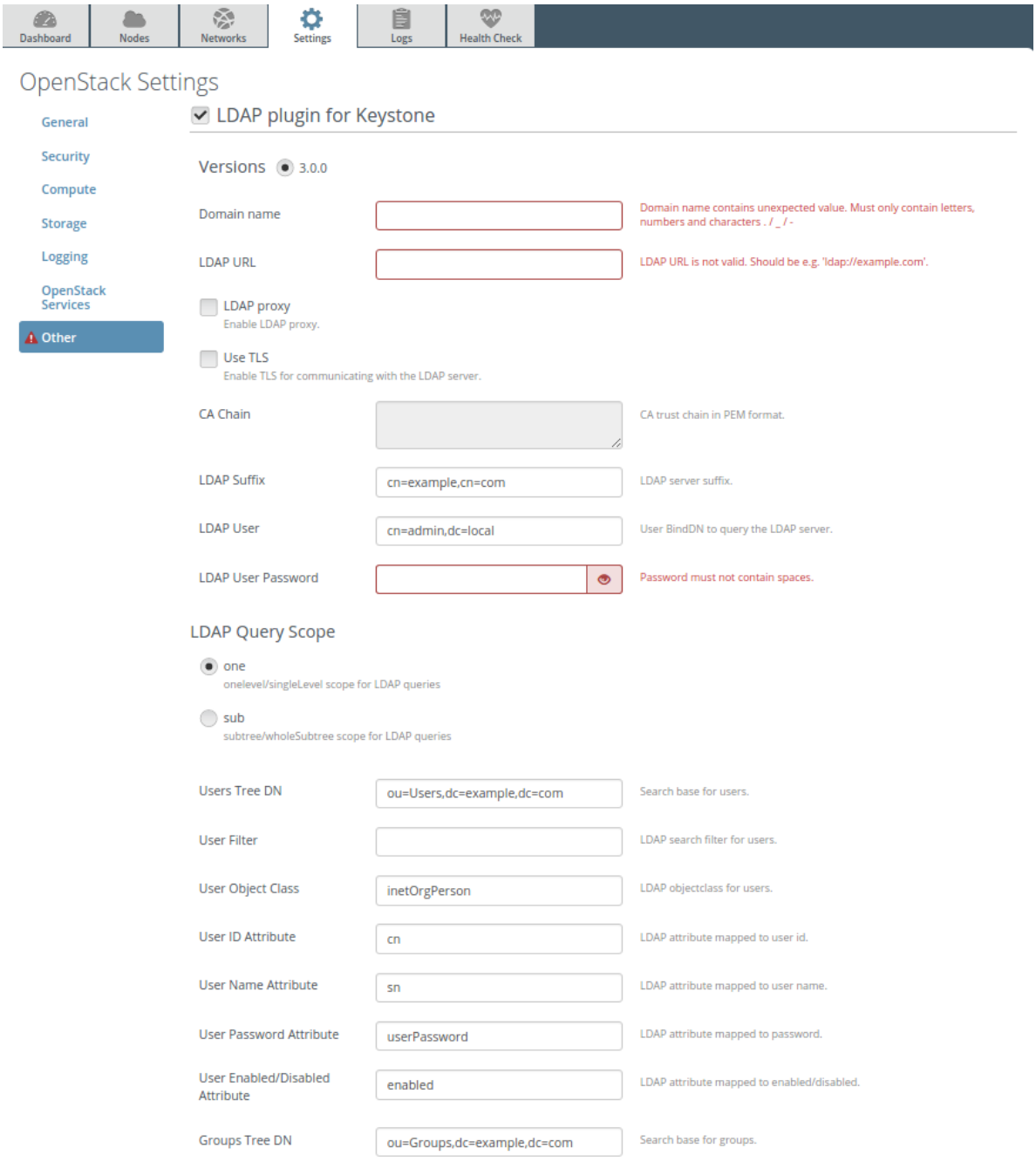
4. Check if the plugin was installed successfully

   ```
   # fuel plugins
   id | name | version | package_version | releases
   ---+------+---------+-----------------+--------------------
   1  | ldap | 3.0.1   | 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:

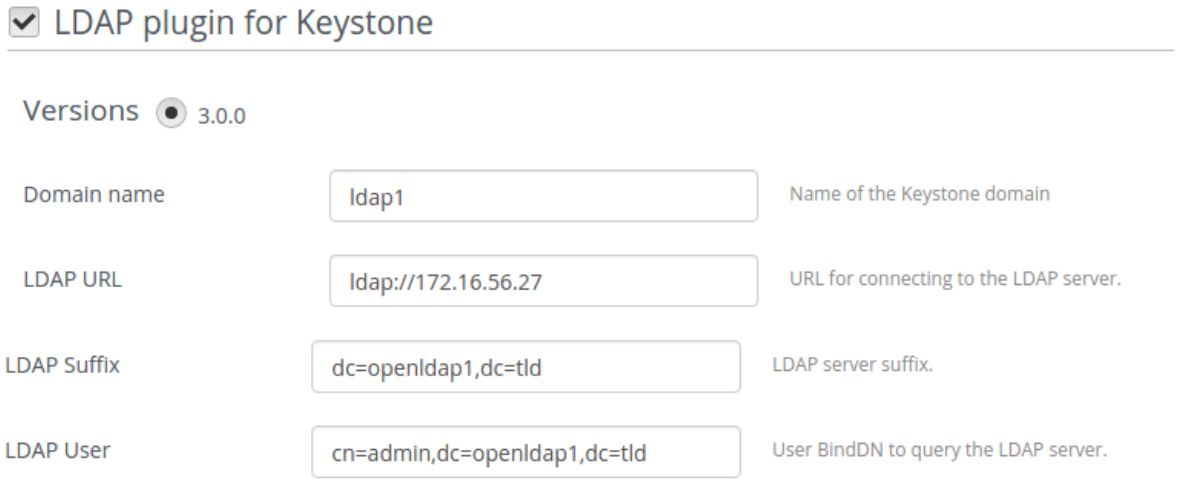

Dashboard
Nodes
Networks
Settings
Logs
Health Check
OpenStack Settings
General
Security
Compute
Storage
Logging
OpenStack Services
Other
LDAP plugin for Keystone
Versions
3.0.0
Domain name
Name of the Keystone domain
LDAP URL
URL for connecting to the LDAP server.
LDAP proxy
Enable LDAP proxy.
Use TLS
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.



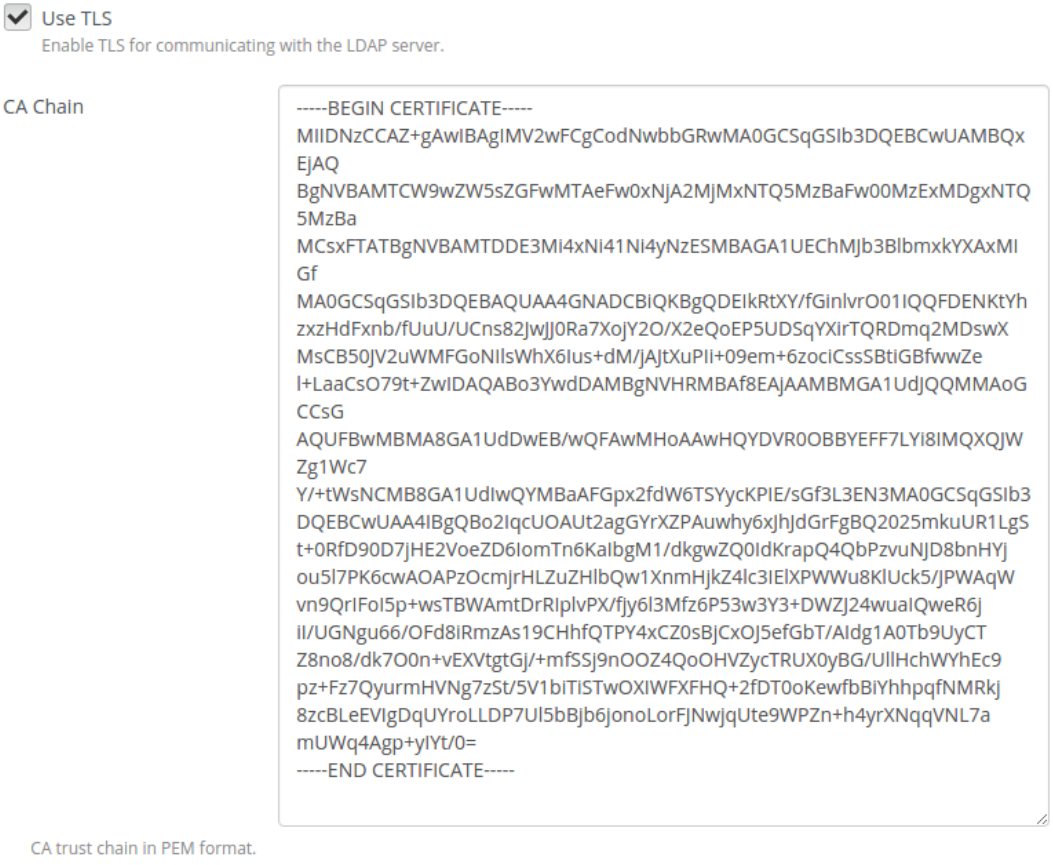
3. Enter plugin settings into the text fields:


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 proxy
Enable LDAP proxy.
Use TLS
Enable TLS for communicating with the LDAP server.
CA Chain
-----BEGIN CERTIFICATE-----
MIIDNzCCAZ+gAwIBAgIMV2wFCg
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.
LDAP attribute mapped to group name.
Group Member Attribute
member
LDAP attribute that maps user to group.

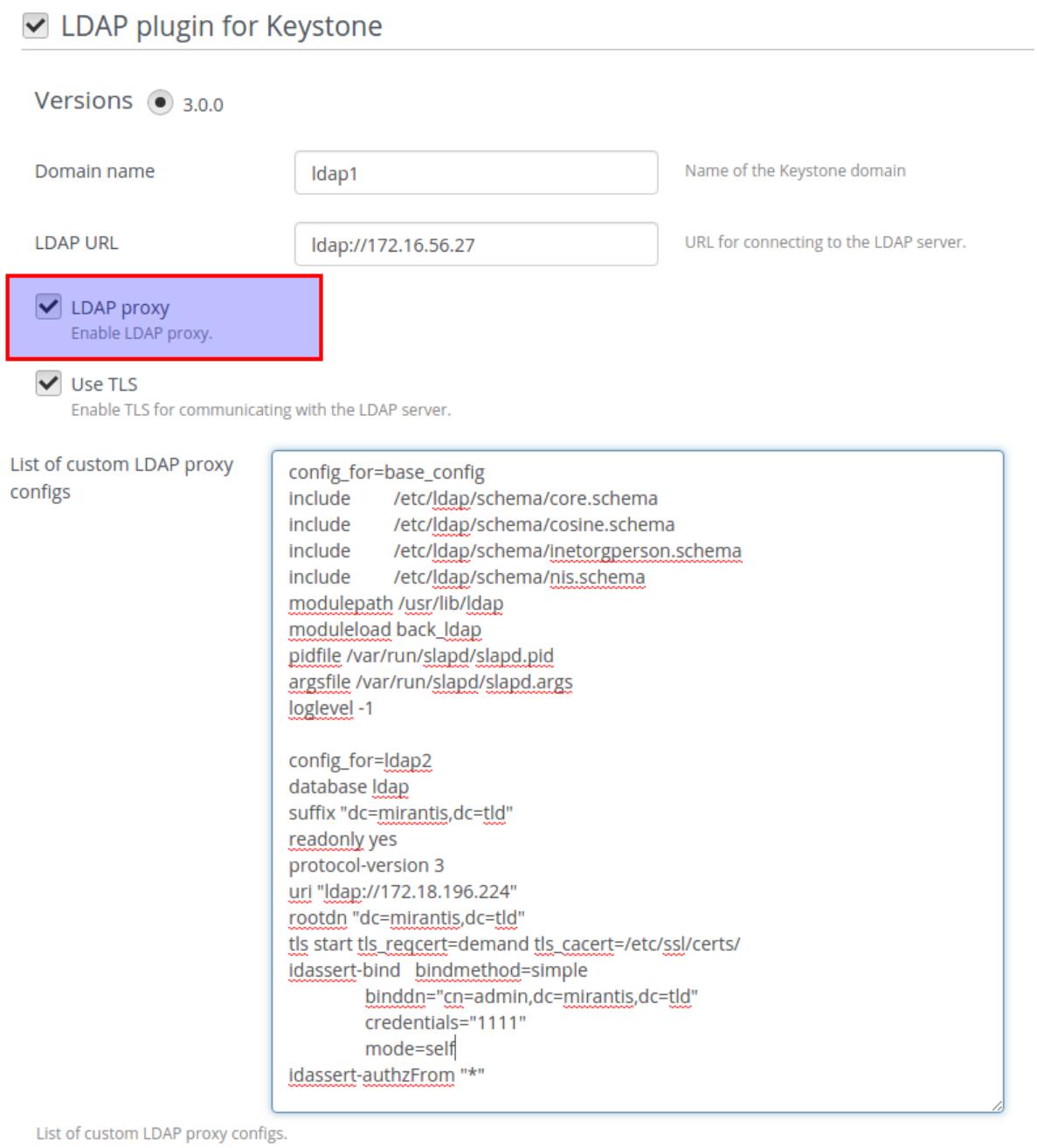
Specify domain name, LDAP URL, LDAP suffix:



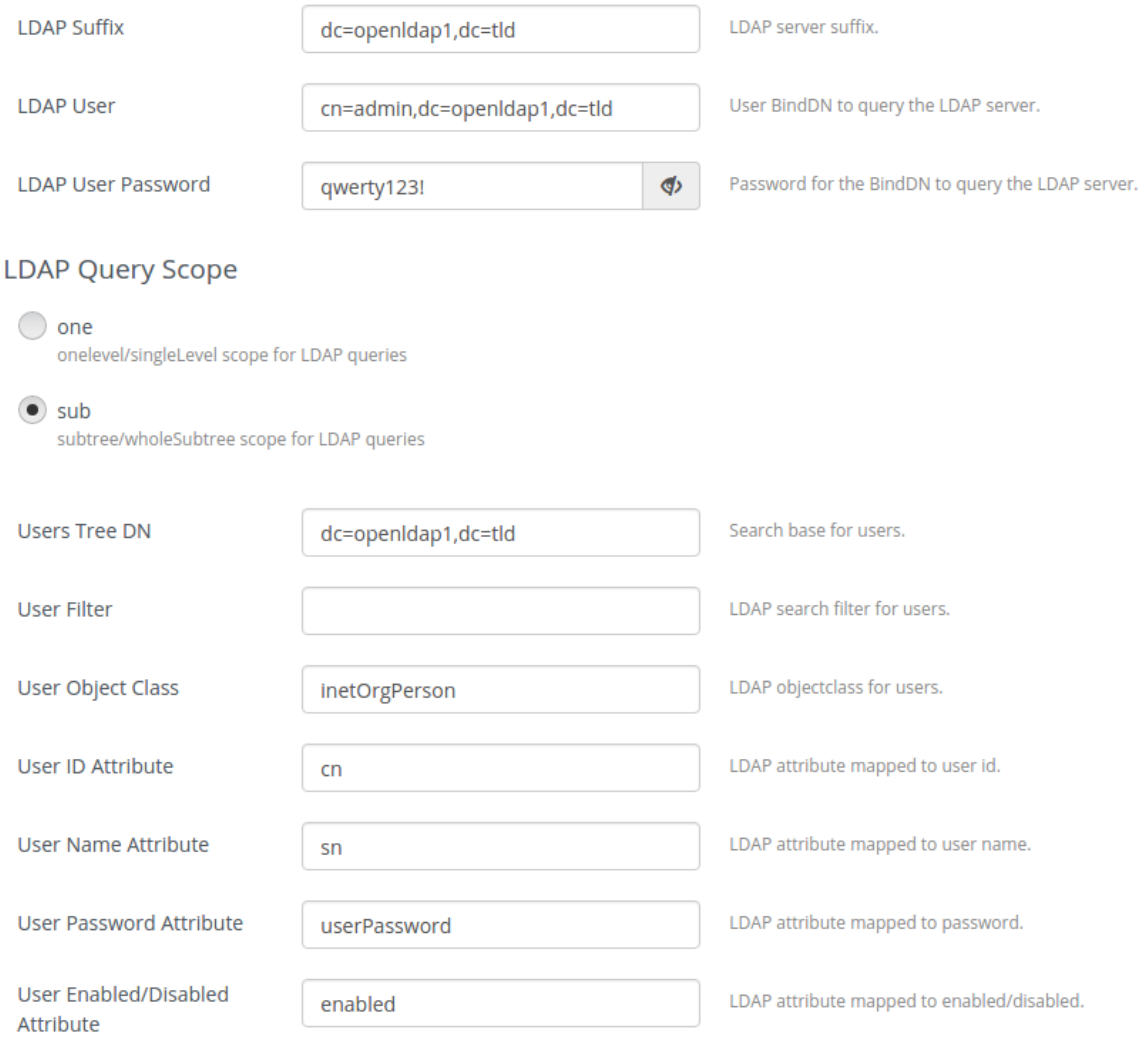
Enable TLS use and put certificate if it is needed:



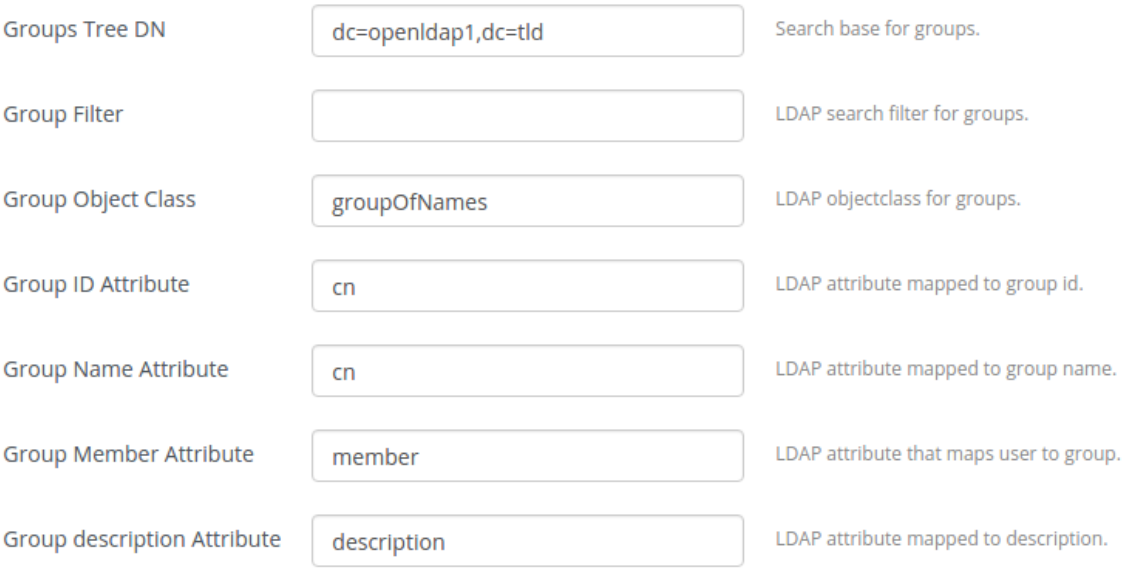
Enable LDAP proxy and put custom config if it is needed:



Specify LDAP user, password and other settings:



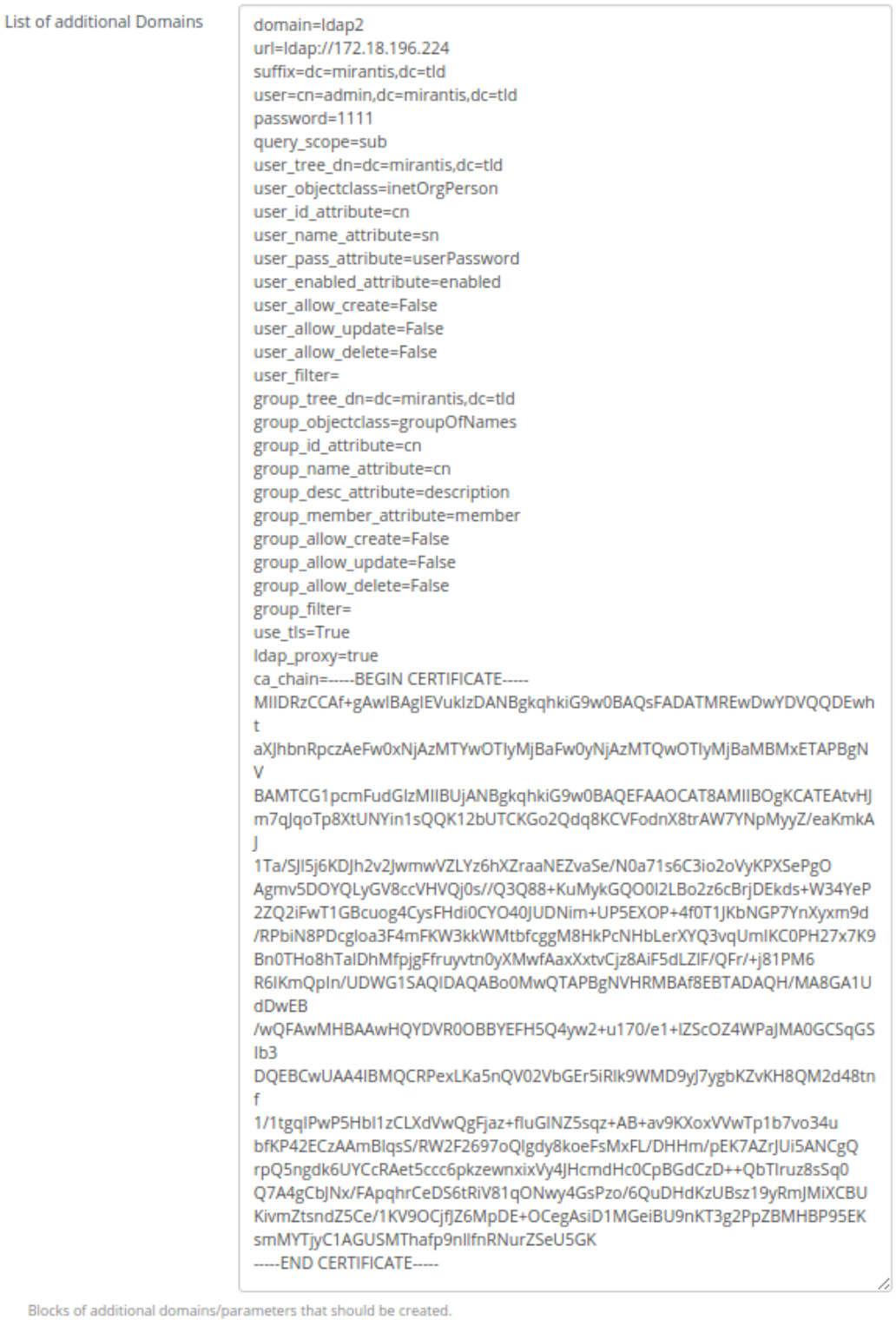
To use LDAP groups provide settings for it:



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.

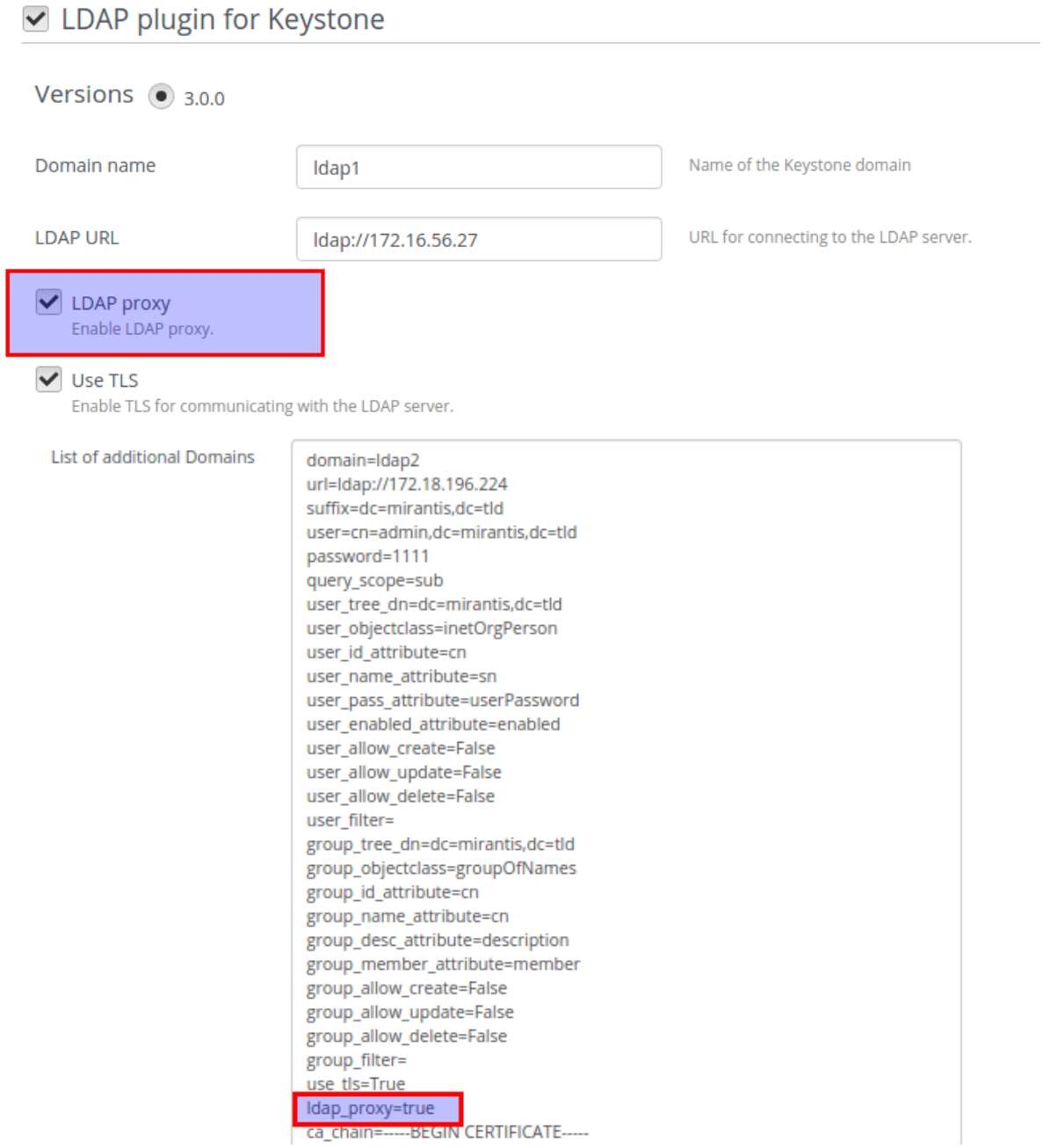
4. To deploy an environment with support of multiple domains 'List of additional Domains' text area should be used. All needed parameters that describes a domain should be copied there, all parameters form a block of parameters.



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.

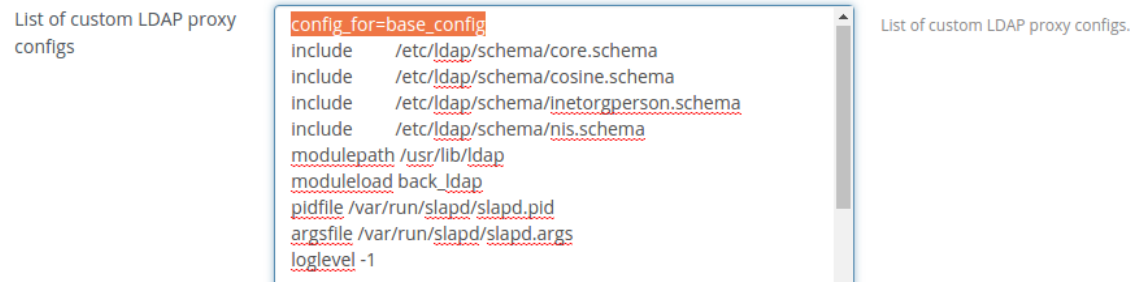
5. To set up an environment with activated LDAP proxy 'LDAP proxy' checkbox should be selected. When only 'LDAP proxy' checkbox is selected: it activates LDAP proxy for base domain and activates LDAP proxy for

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

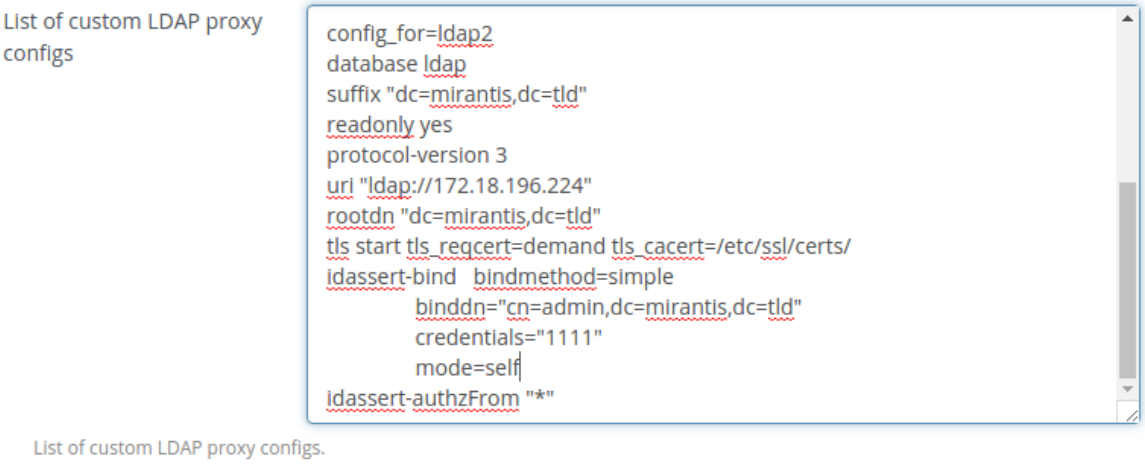


In this case LDAP proxy configurations for LDAP domains are taken from templates located in the plugin. Configurations from the templates have minimal functionality and they are intended for testing needs.

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.



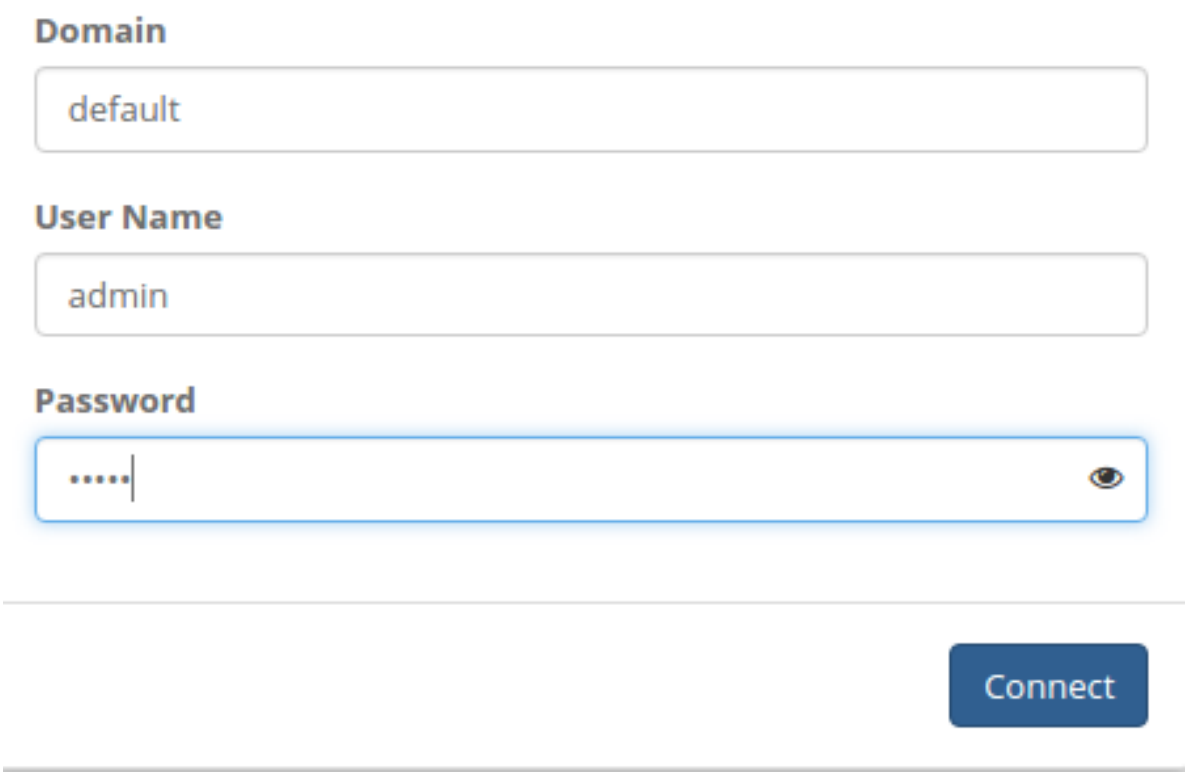
To specify custom settings for LDAP domain 'config_for' parameter with <domain_name> value should be added and after that custom settings can be specified.



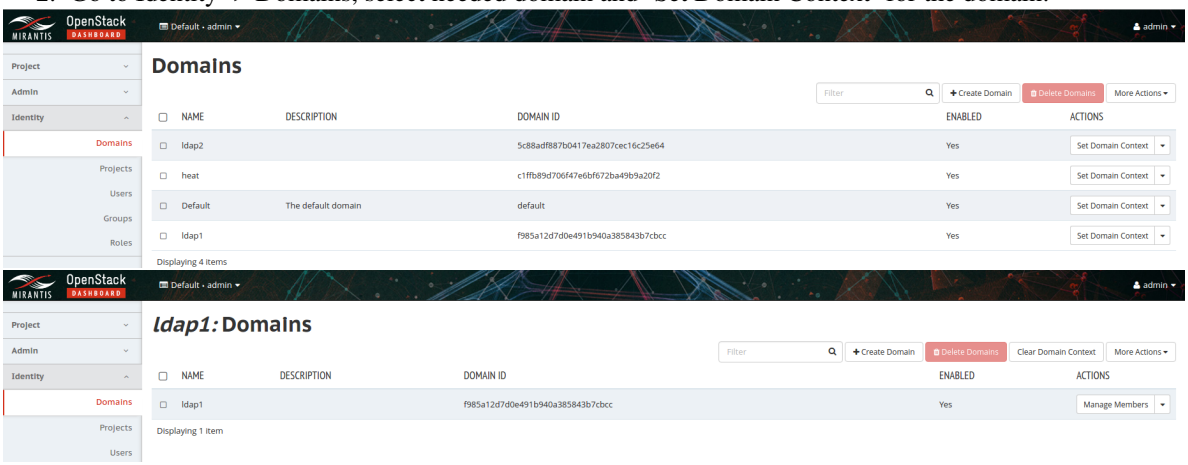
Blocks of custom settings should be separated by empty line.

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

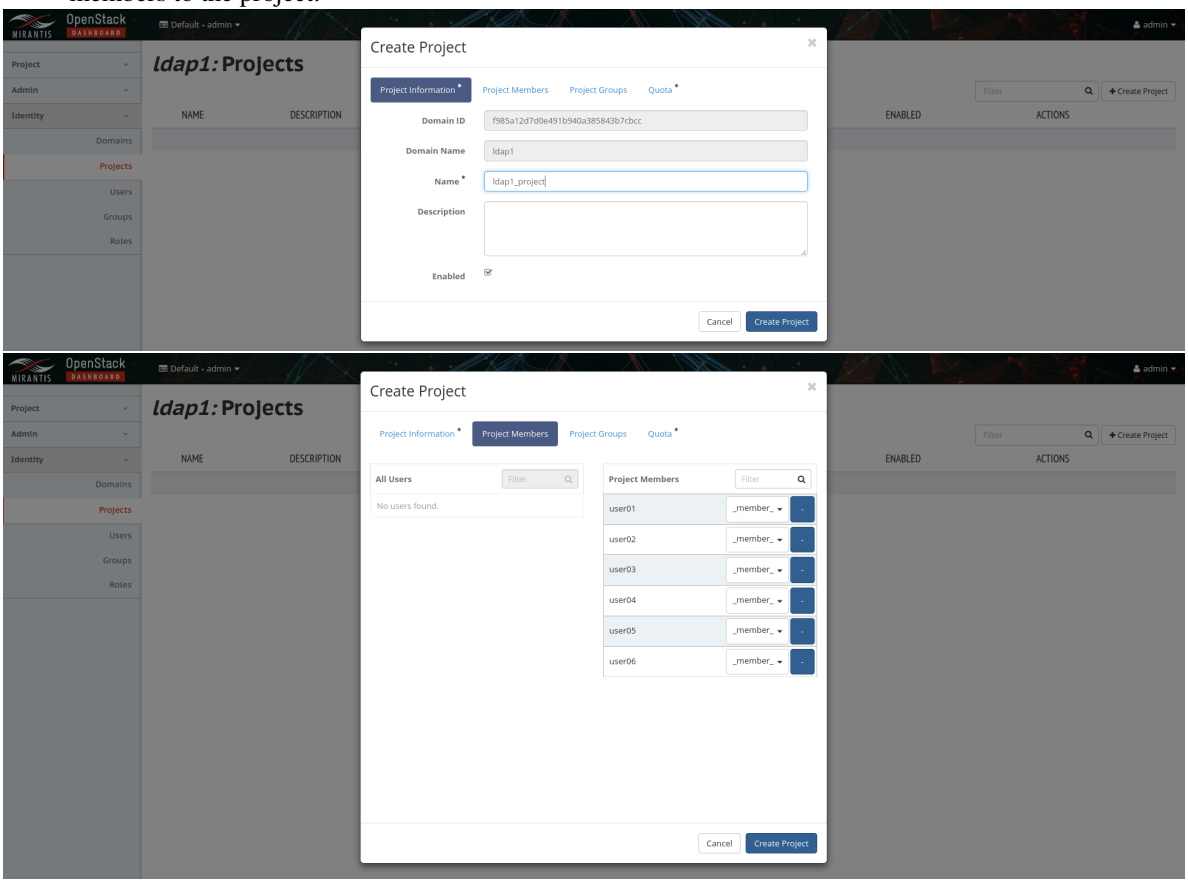
1. After successful environment deployment log into dashboard in default domain:



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

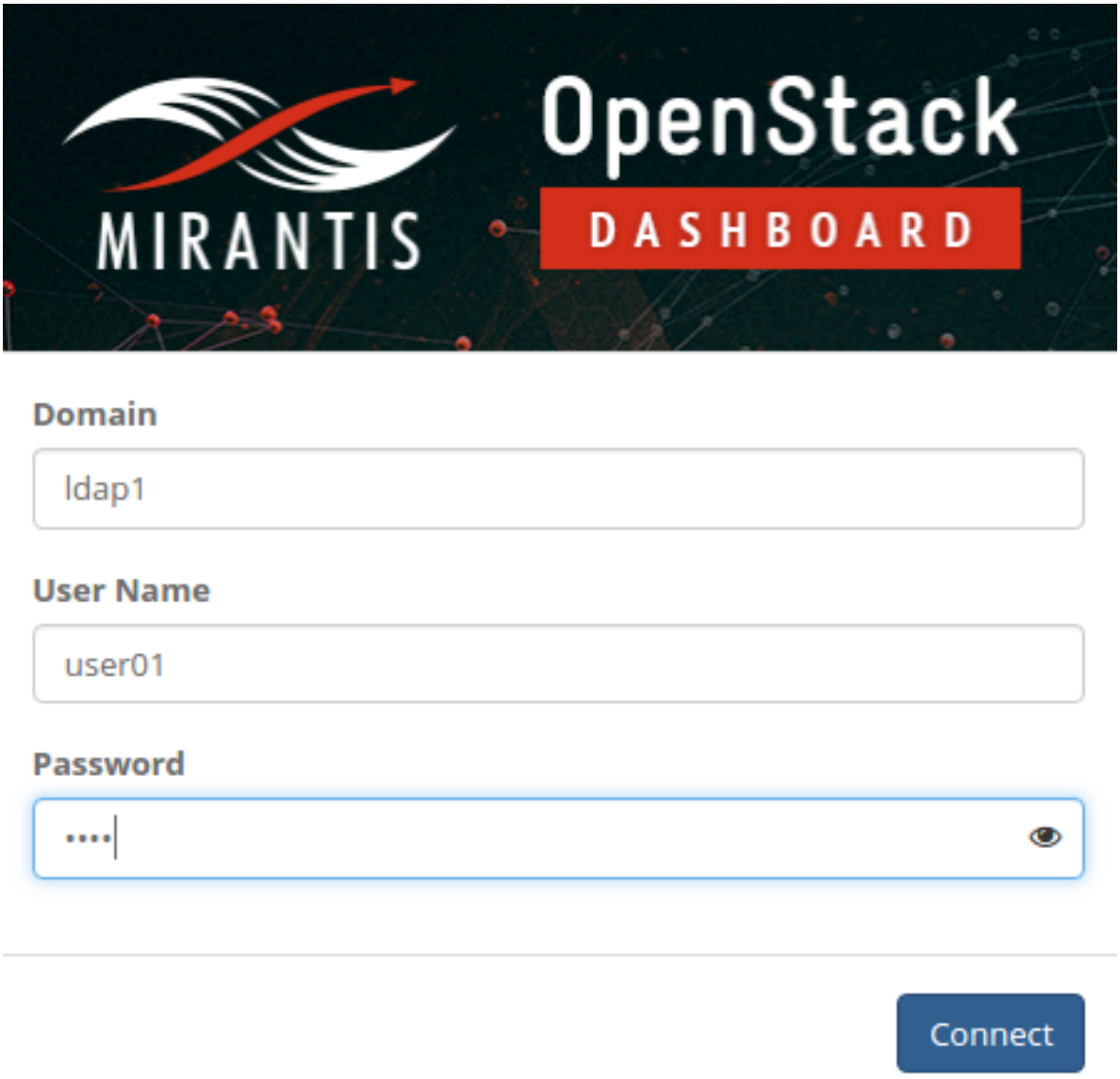


3. Go to Identity -> Projects and select 'Create Project' to create a new project for the domain and add user members to the project:



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:



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