

---

# The LDAP plugin for Fuel documentation

*Release 2.0-2.0.0-1*

**Mirantis Inc.**

May 12, 2016

## CONTENTS

<b>1</b>	<b>Plugin Guide</b>	<b>1</b>
1.1	LDAP plugin for Fuel . . . . .	1
1.2	Release notes / Changelog . . . . .	1
1.3	LDAP plugin limitations . . . . .	1
1.4	Installation Guide . . . . .	2
1.5	Configuring LDAP plugin . . . . .	2
1.6	User Guide . . . . .	11
1.7	LDAP plugin validation . . . . .	12
1.8	Troubleshooting . . . . .	13
1.9	Appendix . . . . .	13

## 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	8.0
Pre-configured LDAP server	

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

### 1.2 Release notes / Changelog

#### 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;

## 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-2.0-2.0.0-1.noarch.rpm root@<Fuel_Master_IP>:/tmp
```

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

```
# cd /tmp
# fuel plugins --install ldap-2.0-2.0.0-1.noarch.rpm
```

4. Check if the plugin was installed successfully

```
# fuel plugins
  id | name          | version   | package_version
  ---+-----+-----+-----
    1 | ldap          | 2.0.0     | 3.0.0
```

5. MU-1 ([Maintenance Update](#)) should be installed to provide proper work of keystone providers with domains during deployment process.

## 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:

The screenshot shows the 'OpenStack Settings' page with the 'LDAP plugin for Keystone' tab selected. The page has a navigation bar at the top with icons for Dashboard, Nodes, Networks, Settings (selected), Logs, and Health Check.

**General**

- LDAP plugin for Keystone**

**Security**

- Versions**: 2.0.0

**Compute**

**Storage**

**Logging**

**OpenStack Services**

- Domain name**: [Input field] Name of the Keystone domain
- LDAP URL**: [Input field] URL for connecting to the LDAP server.
- LDAP Suffix**: cn=example,cn=com LDAP server suffix.

**Other**

- Use TLS**: [checkbox] Enable TLS for communicating with the LDAP server.
- CA Chain**: [Input field] CA trust chain in PEM format.
- LDAP User**: cn=admin,dc=local User BindDN to query the LDAP server.
- LDAP User Password**: [Input field] Password for the BindDN to query the LDAP server.
- LDAP Query Scope**: one The LDAP scope for queries, this can be either "one" (onelevel/singleLevel) or "sub" (subtree/wholeSubtree).
- Users Tree DN**: ou=Users,dc=example,dc=com Search base for users.
- User Filter**: [Input field] 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.

The screenshot shows the 'OpenStack Settings' interface with the 'LDAP plugin for Keystone' tab selected. The 'General' section is expanded, showing the 'LDAP plugin for Keystone' checkbox is checked. The 'Security' section shows the 'Versions' dropdown set to 2.0.0. The 'Compute', 'Storage', and 'Logging' sections have their respective configuration fields and validation messages. The 'OpenStack Services' section contains the 'LDAP Suffix' field with the value 'cn=example,cn=com'. The 'Other' section contains the 'Use TLS' checkbox, which is unchecked, with the note 'Enable TLS for communicating with the LDAP server.' Below it is the 'CA Chain' field, which is empty and described as 'CA trust chain in PEM format.'. The 'LDAP User' field contains 'cn=admin,dc=local' and is described as 'User BindDN to query the LDAP server.'. The 'LDAP User Password' field is empty and has a note 'Password must not contain spaces.' The 'LDAP Query Scope' field contains 'one' and is described as 'The LDAP scope for queries, this can be either "one" (onelevel/singleLevel) or "sub" (subtree/wholeSubtree).'. The 'Users Tree DN' field contains 'ou=Users,dc=example,dc=com' and is described as 'Search base for users.'. The 'User Filter' field is empty and described as 'LDAP search filter for users.'. The 'User Object Class' field contains 'inetOrgPerson' and is described as 'LDAP objectclass for users.'. The 'User ID Attribute' field contains 'cn' and is described as 'LDAP attribute mapped to user id.'. The 'User Name Attribute' field contains 'sn' and is described as 'LDAP attribute mapped to user name.'. The 'User Password Attribute' field contains 'userPassword' and is described as 'LDAP attribute mapped to password.'. The 'User Enabled/Disabled Attribute' field contains 'enabled' and is described as 'LDAP attribute mapped to enabled/disabled.'

Setting	Value	Description
General	<input checked="" type="checkbox"/> LDAP plugin for Keystone	
Security	Versions 2.0.0	
Compute	Domain name	Domain name contains unexpected value. Must only contain letters, numbers and characters . / -
Storage	LDAP URL	LDAP URL is not valid. Should be e.g. 'ldap://example.com'.
Logging	LDAP Suffix	LDAP server suffix.
OpenStack Services	cn=example,cn=com	
Other	<input type="checkbox"/> Use TLS Enable TLS for communicating with the LDAP server.	
CA Chain		CA trust chain in PEM format.
LDAP User	cn=admin,dc=local	User BindDN to query the LDAP server.
LDAP User Password		Password must not contain spaces.
LDAP Query Scope	one	The LDAP scope for queries, this can be either "one" (onelevel/singleLevel) or "sub" (subtree/wholeSubtree).
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.

3. Enter plugin settings into the text fields:

LDAP plugin for Keystone

Versions 2.0.0

Domain name	mirantis.tld	Name of the Keystone domain	
LDAP URL	ldap://172.18.196.224	URL for connecting to the LDAP server.	
LDAP Suffix	dc=mirantis,dc=tld	LDAP server suffix.	
<input checked="" type="checkbox"/> Use TLS	Enable TLS for communicating with the LDAP server.		
CA Chain	-----BEGIN CERTIFICATE----- MIIDRzCCAf+gAwIBAgIEVuktDAN -----END CERTIFICATE-----		CA trust chain in PEM format.
LDAP User	cn=admin,dc=mirantis,dc=tld	User BindDN to query the LDAP server.	
LDAP User Password	...	Password for the BindDN to query the LDAP server.	
LDAP Query Scope	sub	The LDAP scope for queries, this can be either "one" (onelevel/singleLevel) or "sub" (subtree/wholeSubtree).	
Users Tree DN	dc=mirantis,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=mirantis,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.	
List of additional Domains	<pre>domain=ldap225 password=1111 group_id_attribute=cn user_filter= user_allow_update=False group_filter= user_allow_delete=False group_member_attribute=member group_objectclass=groupOfNames group_tree_dn=dc=mirantis,dc=tld query_scope=sub suffix=dc=mirantis,dc=tld group_name_attribute=cn user_tree_dn=dc=mirantis,dc=tld group_desc_attribute=description</pre>		
Blocks of additional domains/parameters that should be created			

Specify domain name, LDAP URL, LDAP suffix:

**LDAP plugin for Keystone**

Versions  2.0.0

Domain name	<input type="text" value="mirantis.tld"/>	Name of the Keystone domain
LDAP URL	<input type="text" value="ldap://172.18.196.224"/>	URL for connecting to the LDAP server.
LDAP Suffix	<input type="text" value="dc=mirantis,dc=tld"/>	LDAP server suffix.

Enable TLS use and put certificate if it is needed:

**Use TLS**

Enable TLS for communicating with the LDAP server.

CA Chain

```
-----BEGIN CERTIFICATE-----
MIIDRzCCAf+gAwIBAgIEVuklzDANBgkqhkiG9w0BAQsFADATMREwDwYDVQQDEwh
t
aXJhbnnRpczAeFw0xNjAzMTYwOTIyMjBaFw0yNjAzMTQwOTIyMjBaMBMxETAPBgN
V
BAMTCG1pcmFudGlzMIIBUjANBgkqhkiG9w0BAQEFAOCAT8AMIIBOgKCATEAtvHJ
m7qJqoTp8XtUNYin1sQQK12bUTCKGo2Qdq8KCVFodnX8trAW7YNpMyyZ/eaKmkA
J
1Ta/SJl5j6KDjh2v2JwmwVZLYz6hXZraaNExvaSe/N0a71s6C3lo2oVvKPxSePgO
Agmv5DOYQLyGV8ccVHVQj0s//Q3Q88+KuMykGQO0l2LBo2z6cBrjDEkds+W34YeP
2ZQ2IFwT1GBCuog4CysFHdi0CYO40JUDNim+UP5EXOP+4f0T1JkbNGP7YnXym9d
/RPbiN8PDcgloa3F4mFKW3kkWMtbfcggM8HkPcNhbLerXYQ3vqUmlKCOPH27x7K9
Bn0THo8hTaDhMfpJgFfruyvt0yXMwfAaxXxtvCjz8AIf5dLZf/QFr/+j81PM6
R6IKmQpIn/UDWG1SAQIDAQABo0MwQTAPBgNVHRMBAf8EBTADAQH/MA8GA1U
dDwEB
/wQFAwMHBAAwHQYDVR0OBBYEFH5Q4yw2+u170/e1+iZScOZ4WPajMA0GCSqGS
Ib3
DQEBCwUAA4IBMQRPExLKa5nQV02vGEr5IRlk9WMD9yJ7ygbKZvKH8QM2d48tn
f
1/1tgqlPwP5Hbl1zCLXdVwQgFjaz+fluGINZ5sqz+AB+av9KXoxVVwTp1b7vo34u
bfKP42EcAAmBlqsS/RW2F2697oQlgdy8koeFsMxFL/DHHm/pEK7AZrjUI5ANCgQ
rpQ5ngdk6UYCcRAet5ccc6pkzewnxixVy4JHcmdHc0CpBGdCzD++QbTlruz8sSq0
Q7A4gCbJNx/FApqhrCeDS6tRIV81qONwy4GsPzo/6QuDHdKzUBsz19yRmjMIxCBU
KivmZtsndZ5Ce/1KV9OCjfjZ6MpDE+OcegAsID1MGelBU9nKT3g2PpZBMHBP95EK
smMYTjyC1AGUSMThafp9nllfnRNurZSeU5GK
-----END CERTIFICATE-----
```

CA trust chain in PEM format.

Specify LDAP user, password and other settings:

LDAP User	<code>cn=admin,dc=mirantis,dc=tld</code>	User BindDN to query the LDAP server.
LDAP User Password	<code>***</code> 	Password for the BindDN to query the LDAP server.
LDAP Query Scope	<code>sub</code>	The LDAP scope for queries, this can be either "one" (onelevel/singleLevel) or "sub" (subtree/wholeSubtree).
Users Tree DN	<code>dc=mirantis,dc=tld</code>	Search base for users.
User Filter		LDAP search filter for users.
User Object Class	<code>inetOrgPerson</code>	LDAP objectclass for users.
User ID Attribute	<code>cn</code>	LDAP attribute mapped to user id.
User Name Attribute	<code>sn</code>	LDAP attribute mapped to user name.
User Password Attribute	<code>userPassword</code>	LDAP attribute mapped to password.
User Enabled/Disabled Attribute	<code>enabled</code>	LDAP attribute mapped to enabled/disabled.

To use LDAP groups provide settings for it:

Groups Tree DN	<code>dc=mirantis,dc=tld</code>	Search base for groups.
Group Filter		LDAP search filter for groups.
Group Object Class	<code>groupOfNames</code>	LDAP objectclass for groups.
Group ID Attribute	<code>cn</code>	LDAP attribute mapped to group id.
Group Name Attribute	<code>cn</code>	LDAP attribute mapped to group name.
Group Member Attribute	<code>member</code>	LDAP attribute that maps user to group.
Group description Attribute	<code>description</code>	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 Suffix	LDAP server suffix.
Use TLS	Enable TLS for communicating with the LDAP server.
CA Chain	CA trust chain in PEM format.
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.
List of additional Domains	Blocks of additional domains/parameters that should be created.

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.

## List of additional Domains

```

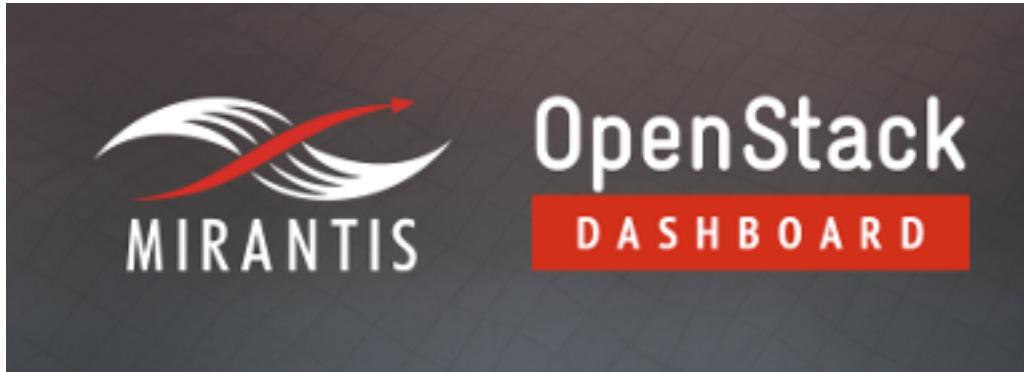
domain=ldap225
password=1111
group_id_attribute=cn
user_filter=
user_allow_update=False
group_filter=
user_allow_delete=False
group_member_attribute=member
group_objectclass=groupOfNames
group_tree_dn=dc=mirantis,dc=tld
query_scope=sub
suffix=dc=mirantis,dc=tld
group_name_attribute=cn
user_tree_dn=dc=mirantis,dc=tld
group_desc_attribute=description
url=ldap://172.18.196.224
user_allow_create=False
user_id_attribute=cn
user_pass_attribute=userPassword
tls_cacertdir=/etc/ssl/certs
group_allow_delete=False
group_allow_create=False
user_cn=admin,dc=mirantis,dc=tld
user_enabled_attribute=enabled
use_tls=True
user_objectclass/inetOrgPerson
group_allow_update=False
user_name_attribute=sn
ca_chain=-----BEGIN CERTIFICATE-----
MIIDRzCCAf+gAwIBAgIEVuklzDANBgkqhkiG9w0BAQsFADATMREwDwYDVQQDE
wh
aXJhbnRpczAeFw0xNjAzMTYwOTIyMjBaFw0yNjAzMTQwOTIyMjBaMBMxETAPB
gNV
BAMTCG1pcmFudGlzMIIBUjANBgkqhkiG9w0BAQEFAOCAT8AMIIBOgKCATEAt
vHJ
m7qlqoTp8XtUNYin1sQQK12bUTCKGo2Qdq8KCVFodnX8trAW7YNpMyyZ/eaK
mkAJ
1Ta/SJI5j6KDjh2v2JwmwVZLYz6hXZraaNEZvaSe/N0a71s6C3io2oVyKPXSePgO
Agmv5DOYQLyGV8ccHVQj0s//Q3Q88+KuMykGQO0I2LBo2z6cBrjDEkds+W34Y
eP
ZZQ2iFwT1GBcuog4CysFHdi0CYO40jUDNim+UP5EXOP+4f0T1JkbNGP7YnXym
9d
/RPbiN8PDcgloa3F4mFKW3kkWMtbfcggM8HkPcNHbLerXYQ3vqUmIKC0PH27x
7K9
Bn0THo8hTaIDhMfpjgFfruyvtn0yXMwfAaxXxtvCjz8AiF5dLZf/QFr-j81PM6
R6IKmQpIn/UDWG1SAQIDAQABoMwQTAPBgNVHRMBAf8EBTADAQH/MA8GA
1UdDwEB
/wQFAwMHBAAwHQYDVR0OBBYE FH5Q4yw2+u170/e1+IZScOZ4WPajMA0GCS
qGSib3
DQEBCwUA4IBMQCRPexLKa5nQV02VbGER5iRlk9WMD9yJ7ygbKZvKH8QM2d4
8tnf
1/tgqlPwP5HbI1zCLXdVwQgFjaz+fluGINZ5sqz+AB+av9KXoxWwTp1b7vo34u
bfKP42ECzAAmBlqsS/RW2F2697oQlgdy8koeFsMxFI/DHHm/pEK7AZrjUi5ANCg
Q
rpQ5ngdk6UYCcRAet5ccc6pkzewnxixVy4JHcmdHc0CpBGdCzD++QbTlruz8sSq0
Q7A4gCbjNx/FApqhrCeDS6tRiV81qONwy4GsPzo/6QuDHdKzUBsz19yRmjMiXC
BU
KivmZtsndZ5Ce/1KV9OCjfjZ6MpDE+OCegAsiD1MGeiBU9nKT3g2PpZBMHBP95
EK
smMYTjyC1AGUSMThafp9nlfnRNurZSeU5GK
----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. Continue with environment configuration and deploy it; for instructions, see [Mirantis OpenStack User Guide](#).
6. After successfull environment deployment log into dashboard in default domain:



**Domain**

**User Name**

**Password**

Eye icon

**Connect**

7. Go to Identity -> Domains, select needed domain and ‘Set Domain Context’ for the domain:

Name	Description	Domain ID	Enabled	Actions
heat	-	52fb539a667c4fa98a7ed43e06492d51	Yes	<input type="button" value="Set Domain Context"/>
mirantis.tld	-	78099cfde5d14904a36cb73fa308e759	Yes	<input type="button" value="Set Domain Context"/>
ldap226	-	ab90441579c4466593163905b500887d	Yes	<input type="button" value="Set Domain Context"/>
Default	Owns users and tenants (i.e. projects) available on Identity API v2.	default	Yes	<input type="button" value="Set Domain Context"/>
ldap225	-	ec3f6118cbfb451c860910fd200ce65d	Yes	<input type="button" value="Set Domain Context"/>

Name	Description	Domain ID	Enabled	Actions
mirantis.tld	-	78099cde5d14904a36cb73fa300e759	Yes	<button>Manage Members</button>

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

**Create Project**

**Project Information \***

- Domain ID: 78099cde5d14904a36cb73fa300e759
- Domain Name: mirantis.tld
- Name \*: mirantis.tld\_project
- Description:
- Enabled:

**Create Project**

**Create Project**

**Project Information \***

**Project Members**

All Users Filter

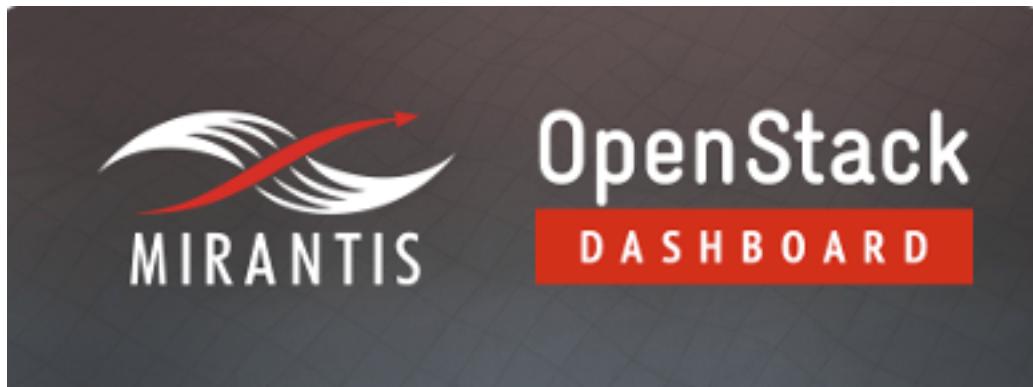
No users found.

Project Members	Role	Action
demo	member	[dropdown]
demo3	member	[dropdown]
demo2	member	[dropdown]

**Create 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**

**User Name**

**Password**

 eye icon

---

**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 OS_AUTH_URL='<http://192.168.0.2:5000/v3/>' openstack domain list
```

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

```
OS_IDENTITY_API_VERSION=3 OS_AUTH_URL='<http://192.168.0.2:5000/v3/>' openstack user list --quiet -d where 'http://192.168.0.2:5000/v3/' is internal keystone url.
```

### 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