Openldap: When adding sudo rules is giving error "ldap_add: Invalid syntax (21) additional info: objectClass: value #1 invalid per syntax"

SOLUTION VERIFIED - Updated December 16 2015 at 11:17 AM - English ()

Environment

- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Openldap

Issue

- Adding `sudo` rule in ldap is giving following error.

```
# ldapadd  -x -h '127.0.0.1' -D 'cn=Manager,dc=example,dc=com' -W -f /tmp/sudo-rule.ldif
adding new entry "cn=adminsudo,ou=SUDOers,dc=example,dc=com"
ldap_add: Invalid syntax (21)
        additional info: objectClass: value #1 invalid per syntax
```

Resolution

1. Login into Openldap server as root.

2. Create the file "sudo.schema" in /tmp directory of Openldap server with following information

```
dn: cn=sudo,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: sudo
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.1  NAME 'sudoUser'  DESC 'User(s) who may  run
sudo'  EQUALITY caseExactIA5Match  SUBSTR caseExactIA5SubstringsMatch  SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.2  NAME 'sudoHost' DESC 'Host(s) who may run
sudo'  EQUALITY caseExactIA5Match  SUBSTR caseExactIA5SubstringsMatch  SYNTAX
1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.3  NAME 'sudoCommand'  DESC 'Command(s) to be
executed by sudo'  EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.4  NAME 'sudoRunAs'  DESC 'User(s) impersonated
by sudo (deprecated)'  EQUALITY caseExactIA5Match  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.5 NAME 'sudoOption' DESC 'Options(s) followed by
sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.6 NAME 'sudoRunAsUser' DESC 'User(s)
impersonated by sudo' EQUALITY caseExactIA5Match  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.7 NAME 'sudoRunAsGroup' DESC 'Group(s)
impersonated by sudo' EQUALITY caseExactIA5Match  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.8 NAME 'sudoNotBefore' DESC 'Start of time
interval for which the entry is valid' EQUALITY generalizedTimeMatch  ORDERING
generalizedTimeOrderingMatch  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.9 NAME 'sudoNotAfter' DESC 'End of time interval
for which the entry is valid'  EQUALITY generalizedTimeMatch ORDERING
generalizedTimeOrderingMatch  SYNTAX 1.3.6.1.4.1.1466.115.121.1.24 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.10 NAME 'sudoOrder'  DESC 'an integer to order
the sudoRole entries'  EQUALITY integerMatch   ORDERING integerOrderingMatch  SYNTAX
1.3.6.1.4.1.1466.115.121.1.27 )
olcObjectClasses: ( 1.3.6.1.4.1.15953.9.2.1 NAME 'sudoRole' SUP top STRUCTURAL  DESC
'Sudoer Entries'  MUST ( cn )   MAY ( sudoUser $ sudoHost $ sudoCommand $ sudoRunAs $
sudoRunAsUser $ sudoRunAsGroup $ sudoOption $ sudoOrder $ sudoNotBefore $ sudoNotAfter $
description ) )
```

3. Add the sudo schema to the ldap config.

```
# ldapadd -Q -Y EXTERNAL -H ldapi:/// -f /tmp/sudo.schema
```

4. Try adding the record again.

```
# ldapadd  -x -h '127.0.0.1' -D 'cn=Manager,dc=example,dc=com' -W -f /tmp/sudo-rule.ldif
```

If Openldap server is using `slapd.conf` as configuration file then follow steps should be following

1. Login into Openldap server as root.

2. Copy the sudo schema file provided by sudo package as below.

```
cp /usr/share/doc/sudo-*/schema.OpenLDAP /etc/openldap/schema/sudo.schema
```

3. Edit file `/etc/openldap/slapd.conf` add the below entry.

```
include     /etc/openldap/schema/sudo.schema
```

4. Restart Openldap service.

```
service slapd restart
```

5. Try adding the record again.

```
ldapadd  -x -h '127.0.0.1' -D 'cn=Manager,dc=example,dc=com' -W -f /tmp/sudo-rule.ldif
```

Root Cause

- The error was observe since `sudo` schema was not added in Openldap server.

Product(s) Red Hat Enterprise Linux (/taxonomy/products/red-hat-enterprise-linux)

Component openldap (/components/openldap) sudo (/components/sudo)

Category Troubleshoot (/category/troubleshoot)

Tags configuration (/tags/configuration) ldap (/tags/ldap) rhel_6 (/tags/rhel_6) rhel_7 (/taxonomy/tags/rhel7)

This solution is part of Red Hat's fast-track publication program, providing a huge library of solutions that Red Hat engineers have created while supporting our customers. To give you the knowledge you need the instant it becomes available, these articles may be presented in a raw and unedited form.

People who viewed this solution also viewed

Unable to save sudoers file due to syntax error.

Solution - Mar 19, 2011

Sudo file syntax error

How to manage sudo rules in OpenLDAP using graphical tool (GUI) ?

Solution - May 7, 2014

Comments