ranger配置从ldap获取用户和组&配置hive(导出)

ldap安装及配置：

LDAP 服务器和客户..南.docx
2.52MB

slap.conf:

```
#######################################################################
# database definitions
#######################################################################

database        bdb
suffix          "dc=asiainfo,dc=com"
checkpoint      1024 15
rootdn          "cn=root,dc=asiainfo,dc=com"
# Cleartext passwords, especially for the rootdn, should
# be avoided.  See slappasswd(8) and slapd.conf(5) for details.
# Use of strong authentication encouraged.
# rootpw                secret
# rootpw                {crypt}ijFYNcSNctBYg
#rootpw                {SSHA}KxwI67Nyx7DcIZOCF2VZ8flzehuxKi1k
```

```
ldapsearch -x -b 'dc=asiainfo,dc=com'
```

```
cd   /usr/hdp/current/ranger-usersync/ldaptool/conf
```

配置：input.properties

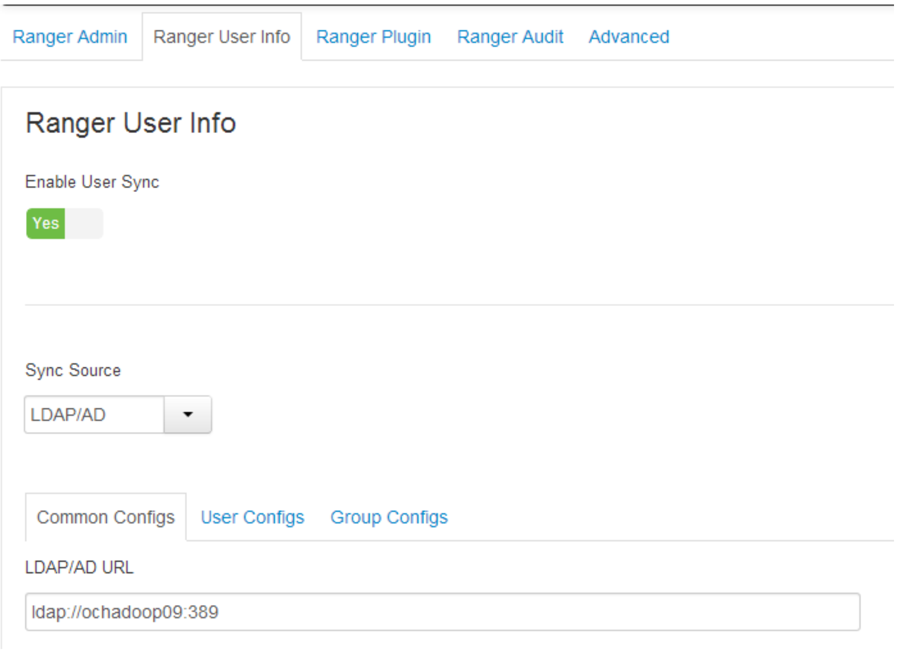
```
ranger.usersync.ldap.url=ldap://ochadoop09:389
ranger.usersync.ldap.binddn=cn=root,dc=asiainfo,dc=com
ranger.usersync.ldap.ldapbindpassword=123456

# Mandatory only for openLdap
ranger.usersync.ldap.user.searchbase=ou=People,dc=asiainfo,dc=com
ranger.usersync.ldap.user.searchfilter=cn=*

# For verifying authentication please provide sample username and password
ranger.admin.auth.sampleuser=usertest
ranger.admin.auth.samplepassword=usertest

# Optional properties will be determined based on the above search
# User attributes
ranger.usersync.ldap.user.nameattribute=uid
ranger.usersync.ldap.user.objectclass=posixAccount
ranger.usersync.ldap.user.groupnameattribute=memberof, ismemberof

# Group attributes
```

```
ranger.usersync.group.searchenabled=true
ranger.usersync.group.memberattributename=memberUid
ranger.usersync.group.nameattribute=cn
ranger.usersync.group.objectclass=posixGroup
ranger.usersync.group.searchbase=ou=Group,dc=asiainfo,dc=com
ranger.usersync.group.searchfilter=cn=*

# Other UserSync related attributes
ranger.usersync.ldap.authentication.mechanism=simple
ranger.usersync.pagedresultsenabled=true
ranger.usersync.pagedresultssize=500
ranger.usersync.ldap.username.caseconversion=lower
ranger.usersync.ldap.groupname.caseconversion=lower
ranger.usersync.ldap.user.searchscope=sub
ranger.usersync.group.searchscope=sub

ranger.usersync.credstore.filename=
ranger.usersync.ldap.bindalias=
ranger.usersync.ldap.searchBase=
ranger.usersync.group.usermapsyncenabled=false

# Authentication properties
ranger.authentication.method=
ranger.ldap.ad.domain=
ranger.ldap.user.dnpattern=
ranger.ldap.group.roleattribute=
ranger.ldap.group.searchbase=
ranger.ldap.group.searchfilter=
```

测试ldap是否可用：

```
 ./run.sh -r  all -i conf/input.properties
```

如果可以执行则ldap可用，可以在ambari界面进行相关配置。

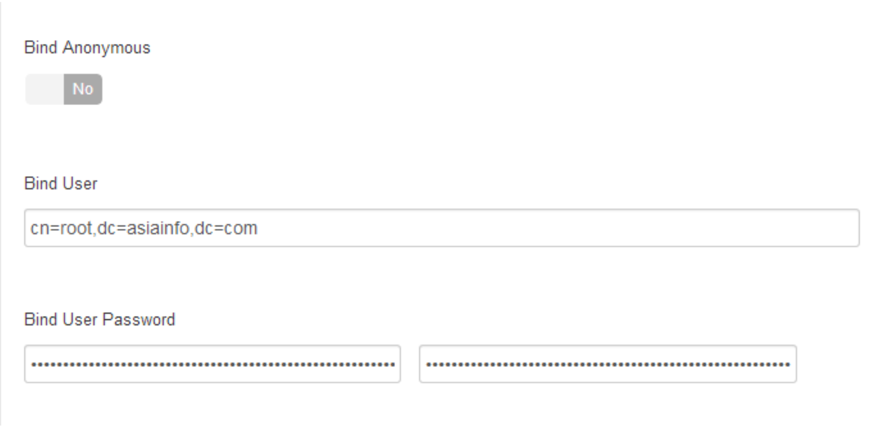


Ranger User Info

Enable User Sync: Yes

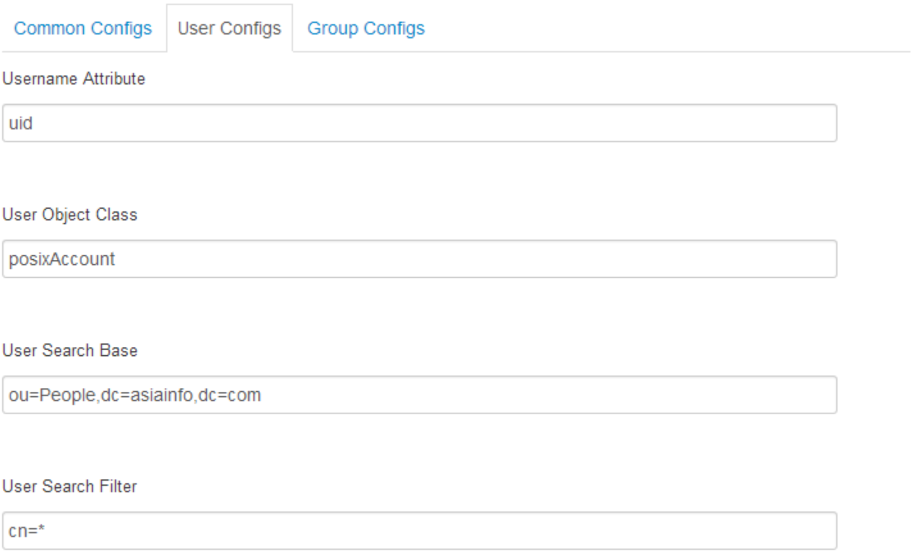
Sync Source: LDAP/AD

LDAP/AD URL: ldap://ochadoop09:389


Bind Anonymous: No

Bind User: cn=root,dc=asiainfo,dc=com

Bind User Password: •• ••

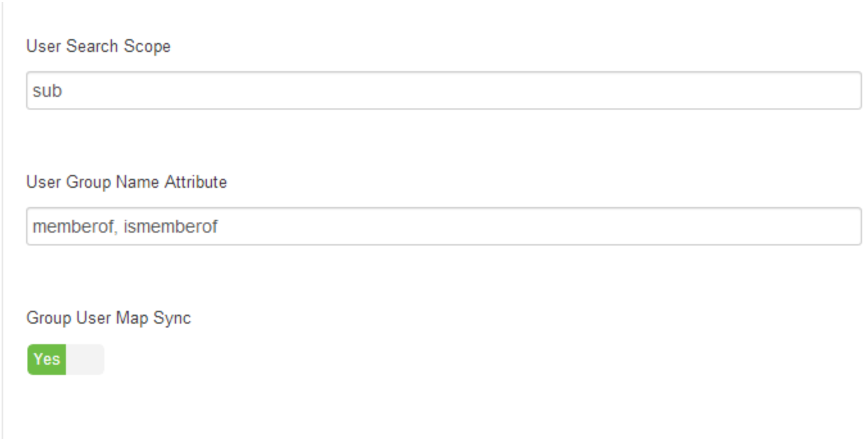


Username Attribute: uid

User Object Class: posixAccount

User Search Base: ou=People,dc=asiainfo,dc=com

User Search Filter: cn=*



User Search Scope

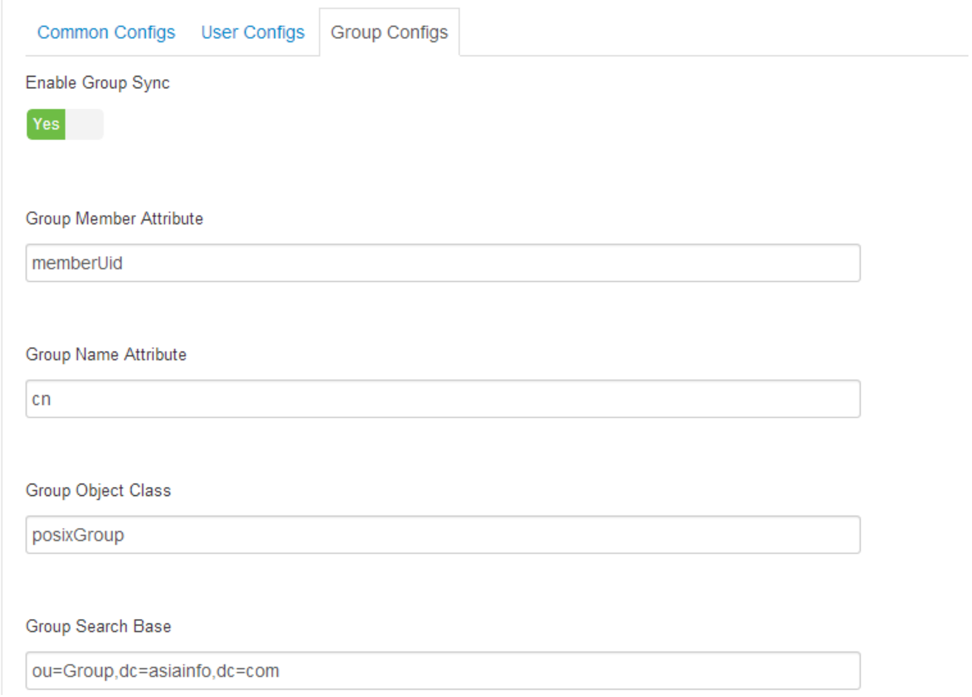
sub

User Group Name Attribute

memberof, ismemberof

Group User Map Sync

Yes



Enable Group Sync

Yes

Group Member Attribute

memberUid

Group Name Attribute

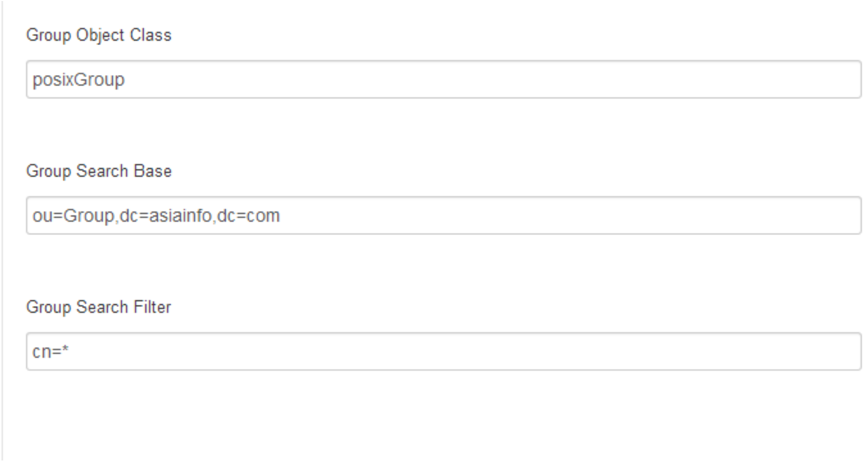
cn

Group Object Class

posixGroup

Group Search Base

ou=Group,dc=asiainfo,dc=com



Group Object Class

posixGroup

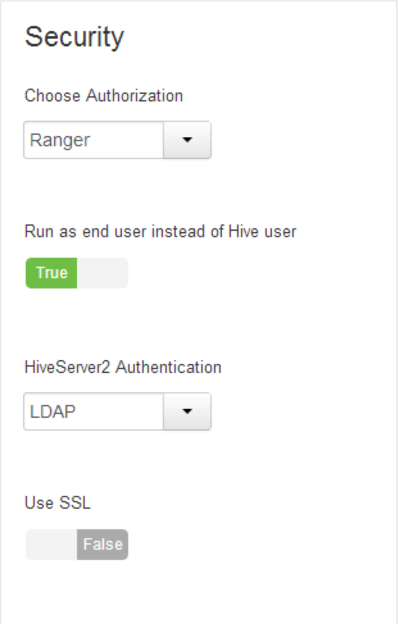
Group Search Base

ou=Group,dc=asiainfo,dc=com

Group Search Filter

cn=*

hive配置ldap认证：



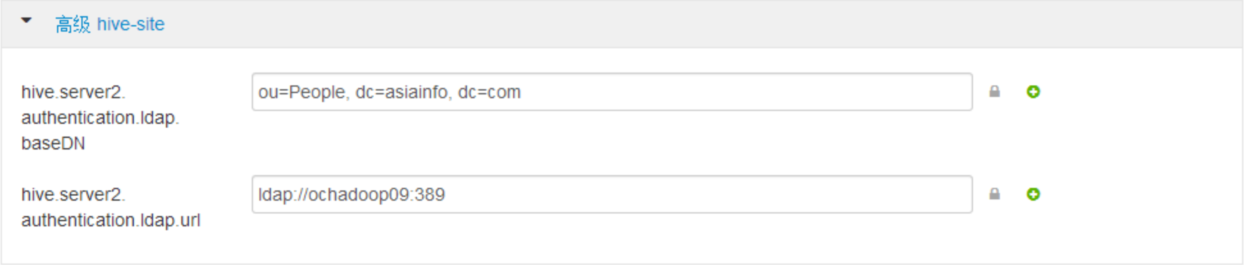
Security

Choose Authorization: Ranger

Run as end user instead of Hive user: True

HiveServer2 Authentication: LDAP

Use SSL: False



高级 hive-site

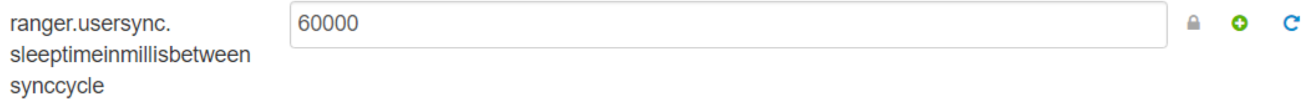
hive.server2.authentication.ldap.baseDN: ou=People, dc=asiainfo, dc=com

hive.server2.authentication.ldap.url: ldap://ochadoop09:389

ldap添加用户：

```
 cat /etc/passwd |grep usertest  >  testpwd.in
 /usr/share/migrationtools/migrate_passwd.pl testpwd.in >  testpwd.ldif

 ldapadd -x -D "cn=root,dc=asiainfo,dc=com" -w 123456 -f  testpwd.ldif

ldapsearch -x -b 'dc=asiainfo,dc=com'
```

ranger 同步用户间隔时间：可以调小



ranger.usersync.sleeptimeinmillisbetweensynccycle: 60000

这个参数没有作用。重启一下Ranger Usersync 新加的用户立刻就可以同步到ranger。