```
[users]

# List of users with their password allowed to access Zeppelin.

# To use a different strategy (LDAP / Database / ...) check the shiro doc at
http://shiro.apache.org/configuration.html#Configuration-INISections

admin = ##########,admin

user1 = #####, role1

user3 = user3, role3

testuser1=####, role1

testuser2=#####,role1


# Sample LDAP configuration, for user Authentication, currently tested for single Realm

[main]

### A sample for configuring Active Directory Realm

#activeDirectoryRealm=org.apache.zeppelin.realm.ActiveDirectoryGroupRealm

#activeDirectoryRealm.systemUsername=#####

 #use either systemPassword or hadoopSecurityCredentialPath, more details in
http://zeppelin.apache.org/docs/latest/security/shiroauthentication.html

#activeDirectoryRealm.systemPassword=######

#activeDirectoryRealm.hadoopSecurityCredentialPath=jceks://file/user/zeppelin/zeppelin.jceks

#activeDirectoryRealm.searchBase=OU=#######

 #activeDirectoryRealm.url=#######

 #activeDirectoryRealm.groupRolesMap = "CN=#######”

 #activeDirectoryRealm.authorizationCachingEnabled = true


### A sample for configuring LDAP Directory Realm

ldapRealm = org.apache.zeppelin.realm.LdapRealm

## search base for ldap groups (only relevant for LdapGroupRealm):

#ldapRealm.contextFactory.environment[ldap.searchBase] = OU#########
```

```
ldapRealm.contextFactory.systemUsername=CN=#######
ldapRealm.contextFactory.systemPassword=#######
ldapRealm.contextFactory.authenticationMechanism=simple
ldapRealm.contextFactory.url=########
ldapRealm.searchBase=DC=#######
ldapRealm.userSearchBase=DC=######
ldapRealm.groupSearchBase=DC=#######
ldapRealm.userObjectClass=person
ldapRealm.groupObjectClass=group
ldapRealm.userSearchAttributeName=samAccountName
ldapRealm.userSearchFilter=(&(objectclass=person)(samAccountName={0}))
ldapRealm.memberAttribute=member
ldapRealm.memberAttributeValueTemplate=CN#######3


### A sample PAM configuration
#pamRealm=org.apache.zeppelin.realm.PamRealm
#pamRealm.service=sshd


sessionManager = org.apache.shiro.web.session.mgt.DefaultWebSessionManager
### If caching of user is required then uncomment below lines
cacheManager = org.apache.shiro.cache.MemoryConstrainedCacheManager
securityManager.cacheManager = $cacheManager

cookie = org.apache.shiro.web.servlet.SimpleCookie
cookie.name = JSESSIONID
#Uncomment the line below when running Zeppelin-Server in HTTPS mode
#cookie.secure = true
```

```
cookie.httpOnly = true
sessionManager.sessionIdCookie = $cookie

securityManager.sessionManager = $sessionManager
# 86,400,000 milliseconds = 24 hour
securityManager.sessionManager.globalSessionTimeout = 86400000
shiro.loginUrl = /api/login

[roles]
role1 = *
role2 = *
role3 = *
admin = *

[urls]
# This section is used for url-based security.
# You can secure interpreter, configuration and credential information by urls. Comment or uncomment the below urls that you want to hide.
# anon means the access is anonymous.
# authc means Form based Auth Security
# To enfore security, comment the line below and uncomment the next one
#/api/version = anon
/api/interpreter/** = authc, roles[admin]
/api/configurations/** = authc, roles[admin]
/api/credential/** = authc, roles[admin]
#/** = anon
/** = authc
```