Jenkins – Sample FreeStyle Job, Security & Docker

Exercise for Sample Free Style Job + Scheduler

- Create your First Job "First_Repeat_Job"
- Configure it to just echo "Hello and Time Stamp"
- Run it, check workspace location
- Modify this job to run every minute!!

Jenkins Access Control

Manage Jenkins -> Configure Global Security

- Delegate to Servlet Container (historical behaviour)
- Jenkins Own Database
- LDAP

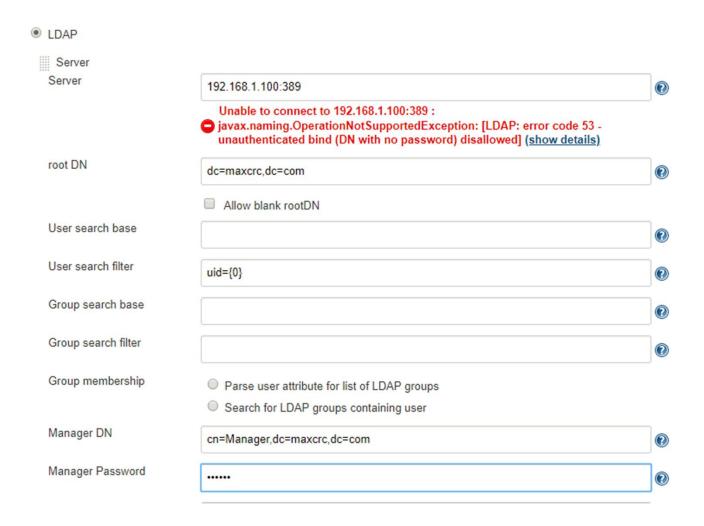
OpenLDAP Authentication

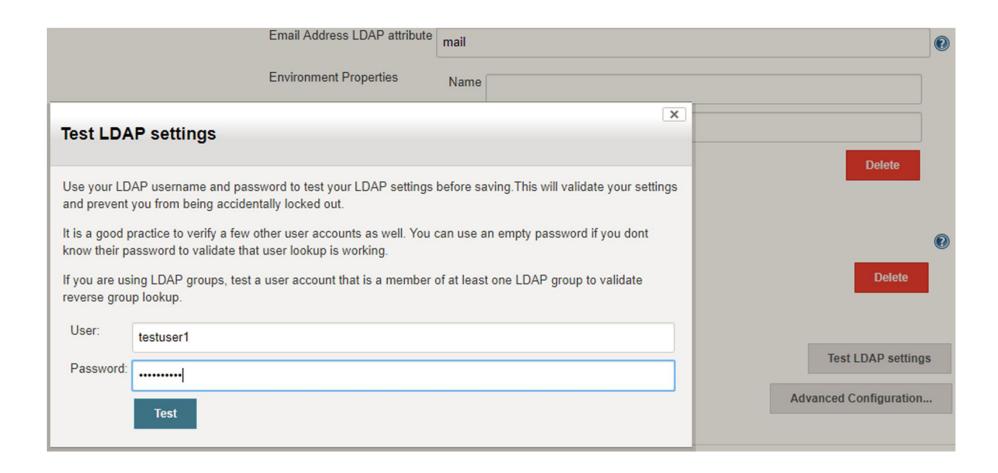
- OpenLDAP : https://www.openIdap.org/
- Port 389
- Base/Root DN : dc=maxcrc,dc=com
- Manager DN: cn=Manager,dc=maxcrc,dc=com
- Create New User using Idapmodify tool
 - Userid : testuser1
 - Password : jenkins123

Jenkins > Configure Global Security

Provide:

- LDAP IP Address with Port
- Root DN
- Manager DN
- Manager Password





Test LDAP settings

Login

- Authentication: successful
- User ID: testuser1
- User Dn: cn=TestUser1,ou=People,dc=maxcrc,dc=com

No display name specified for user! Is the LDAP attribute name "displayname" correct? Available LDAP attributes are:

- sn
- userPassword
- - carLicense
 - mail
 - objectClass
 - · uid
 - homePhone
 - cn
 - description
- User email: testuser1@gmail.com

No LDAP group membership reported.

▲ If the user is a member of some LDAP groups then the group membership settings are probably configured incorrectly.

Lookup

- User lookup: successful
- User groups consistent (login and lookup)

LDAP Group lookup: could not verify.

A Please try with a user that is a member of at least one LDAP group.

Adding Users

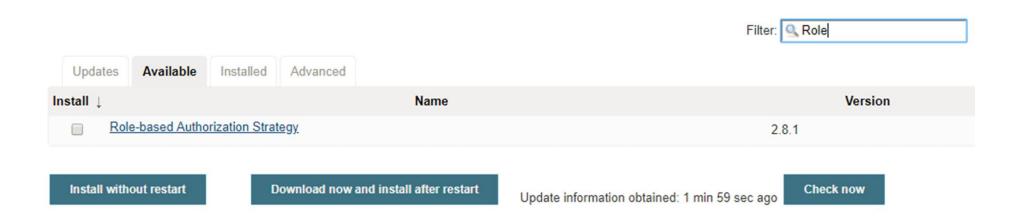
- Switch back to Jenkins Own User Database
- Manage Jenkins > Manage Users > Create User
- Check new user permissions
- Create the following users:
 - developer1
 - developer2
 - qa1
 - qa2

Role Based Authorization

- To provide Granular permission levels (Project, Repo, Workspace, Job etc), use any popular plugins
- Role Based Authorization Strategy Plugin : https://wiki.jenkins.io/display/JENKINS/Role+S trategy+Plugin

Install Plugin

Manage Plugins > Available > Search "Role"



Enable Plugin

Configure Global Security & Choose Role Based Strategy

Access Control

Security Realm

Delegate to servlet container

Jenkins' own user database

Allow users to sign up

LDAP

Authorization

Anyone can do anything

Legacy mode

Logged-in users can do anything

Matrix-based security

Project-based Matrix Authorization Strategy

Role-Based Strategy

Create Global Roles

Jenkins > Manage & Assign Roles



Script Console

Executes arbitrary script for administration/trouble-shooting/diagnostics.



Manage Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.



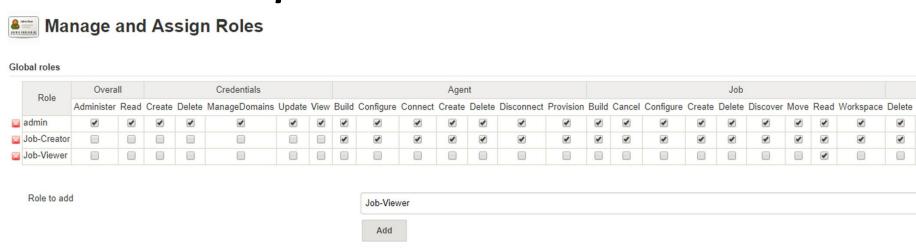
Manage and Assign Roles

Handle permissions by creating roles and assigning them to users/group

Create 2 Global Roles

- QA (Full admin rights)
- Dev (less rights can not create jobs)

Make Sure to provide Overall Read Permission



Assign Different Roles

- Assign Different roles for the users you have created
- For any one user, deny permission to even READ workspace
- Please Note for any user if you deny Overall Read permission, they will not be able to login to Jenkins