

# 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.openldap.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 LDAP Configuration

Jenkins > Configure Global Security

Provide:

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

# Jenkins LDAP Configuration

☒ LDAP

☐ Server  
Server

192.168.1.100:389 ?

Unable to connect to 192.168.1.100:389 :  
- javax.naming.OperationNotSupportedException: [LDAP: error code 53 - unauthenticated bind (DN with no password) disallowed] ([show details](#))

root DN

dc=maxcrc,dc=com ?

☐ Allow blank rootDN

User search base ?

User search filter

uid={0} ?

Group search base ?

Group search filter ?

Group membership

☐ Parse user attribute for list of LDAP groups  
☐ Search for LDAP groups containing user

Manager DN

cn=Manager,dc=maxcrc,dc=com ?

Manager Password

..... ?

# Jenkins LDAP Configuration

The screenshot shows the Jenkins LDAP configuration page. At the top, there is a section for 'Email Address LDAP attribute' with a text input field containing 'mail'. Below this is the 'Environment Properties' section, which includes a 'Name' input field. A modal dialog box titled 'Test LDAP settings' is open in the foreground. The dialog contains instructions on how to test LDAP settings, a 'User' input field with 'testuser1', a 'Password' input field with masked characters, and a 'Test' button. In the background, there are two red 'Delete' buttons and a 'Test LDAP settings' button. At the bottom right, there is an 'Advanced Configuration...' button.

Email Address LDAP attribute

Environment Properties Name

**Test LDAP settings**

Use your LDAP username and password to test your LDAP settings before saving. This will validate your settings and prevent you from being accidentally locked out.

It is a good practice to verify a few other user accounts as well. You can use an empty password if you don't know their password to validate that user lookup is working.

If you are using LDAP groups, test a user account that is a member of at least one LDAP group to validate reverse group lookup.

User:

Password:

**Test**

**Delete**

**Delete**

**Test LDAP settings**

**Advanced Configuration...**

# Jenkins LDAP Configuration

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
- ou
- 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.

- ⚠ 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+Strategy+Plugin>

# Install Plugin

Manage Plugins > Available > Search “Role”

Filter:

Updates

Available

Installed

Advanced

Install ↓	Name	Version
<input type="checkbox"/>	<a href="#">Role-based Authorization Strategy</a>	2.8.1

Install without restart

Download now and install after restart

Update information obtained: 1 min 59 sec ago

Check now

# 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/groups

# Create 2 Global Roles




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

***Make Sure to provide Overall Read Permission***



## Manage and Assign Roles

### Global roles

Role	Overall	Credentials					Agent										Job							
	Administer	Read	Create	Delete	ManageDomains	Update	View	Build	Configure	Connect	Create	Delete	Disconnect	Provision	Build	Cancel	Configure	Create	Delete	Discover	Move	Read	Workspace	Delete
 admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Job-Creator	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 Job-Viewer	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Role to add

Job-Viewer

Add

# 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