Jenkins

Jeeva S. Chelladhurai
CEO, Comorin Consulting Services
+91 97319 77222
jeeva@comorin.co

4. Configuring Role-based Strategy for Authorization

- Steps to Configure Role-based Strategy for Authorization
  - Steps to Create Users
  - Assign Roles

Configuring Role-based Strategy for Authorization

- Role-based access control (RBAC)
  - Method of restricting network access based on the roles of individual users within an enterprise
  - Lets employees have access rights only to the information they need to do their jobs
  - Prevents them from accessing information that doesn't pertain to them

Steps to Configure role-based strategy for authorization

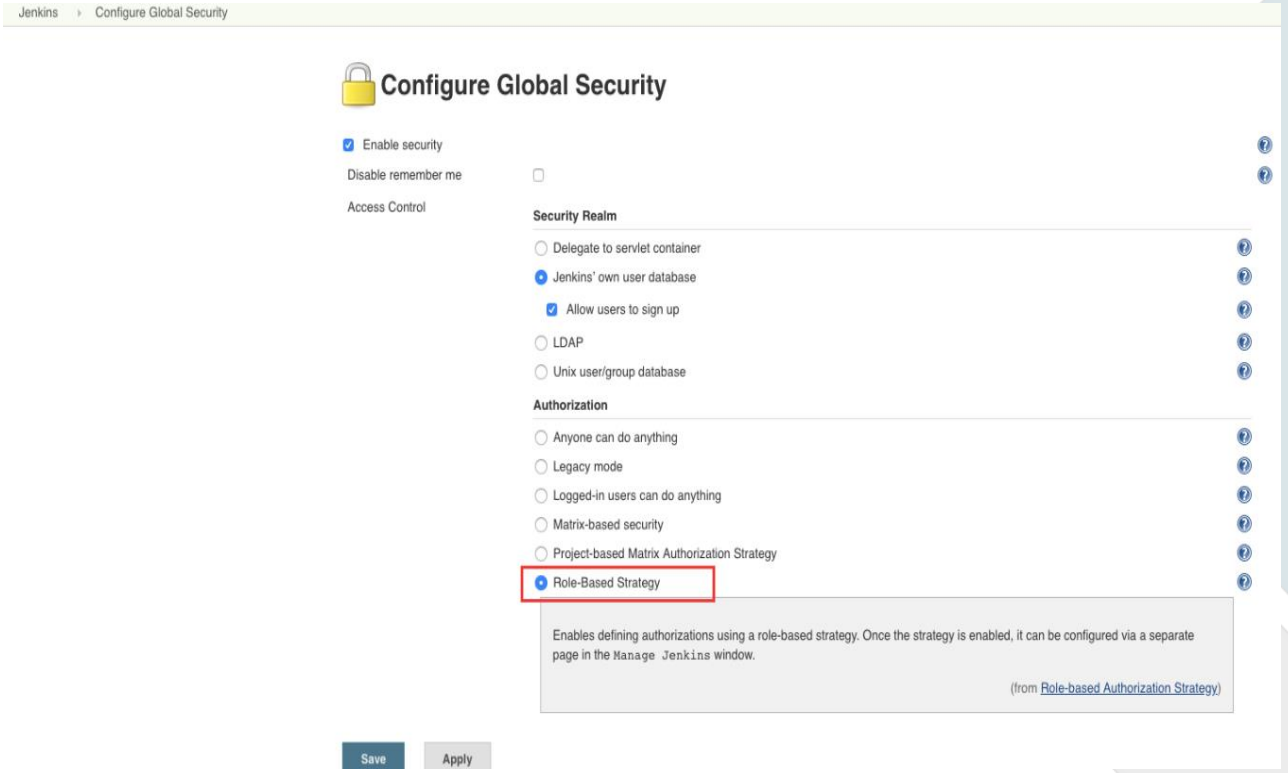
Step 1:

- Go to Jenkins dashboard
- Manage Jenkins->Manage Plugins->search in Available plugins for Role-based Authorization Strategy
- Select checkbox and install without restart
- After installation we can find plugin in available plugins section

Cont'd…

Step 2

- Go to Jenkins dashboard->Manage Jenkins->Configure Global security
- Under Access control->Authorization-> select Role-Based Strategy
- Save and Apply



Cont’d…

Step 3:

- Create users
- To create user:
  - Go to Manage Jenkins->Manage Users->Create User->
  - Enter user name, password, full name and email-id
  - Click on save

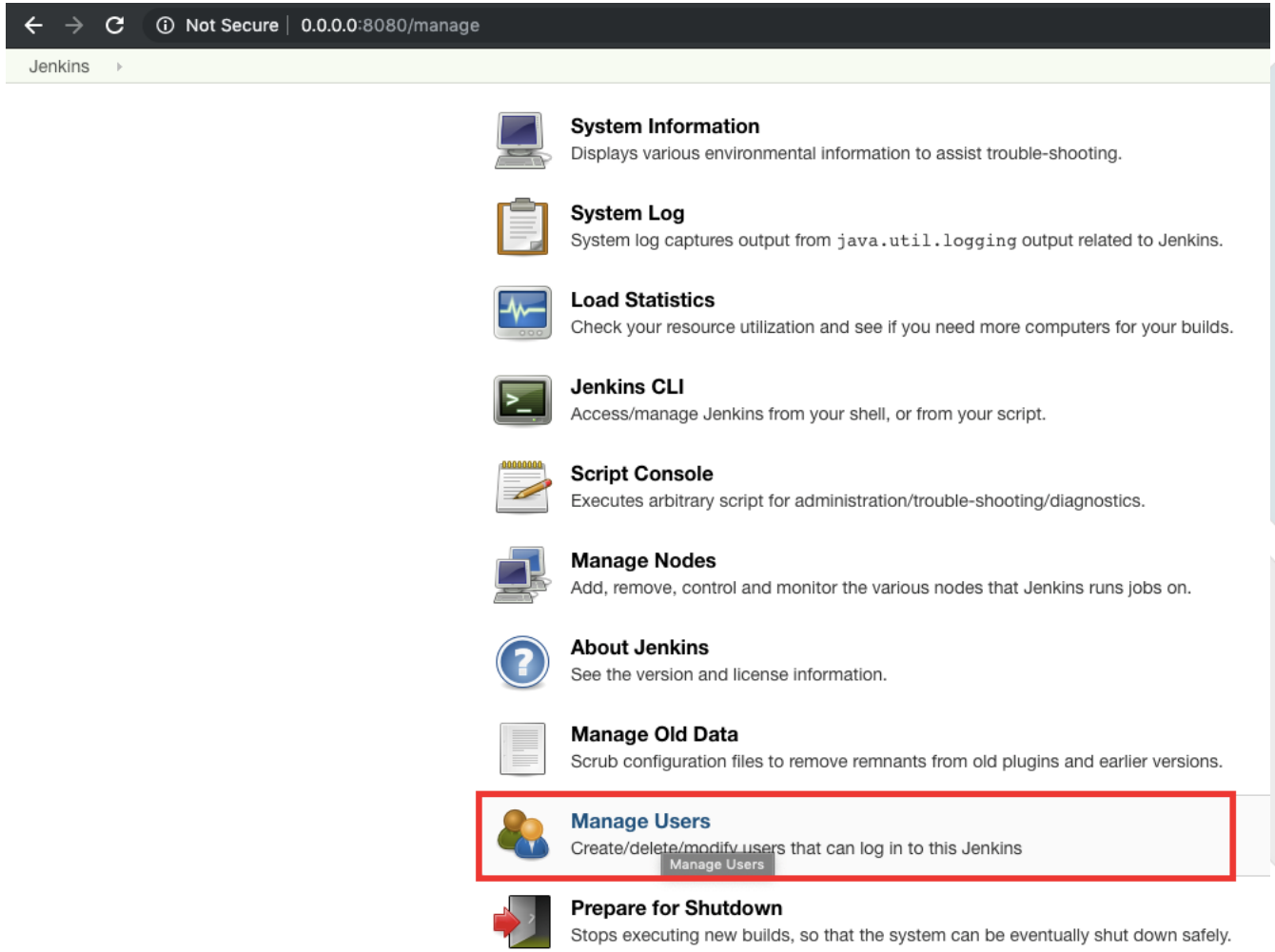
Cont’d…

Step 4:

- Created 3 users
  - user-a, user-b and user-c
  - Follow next slide for steps to create users

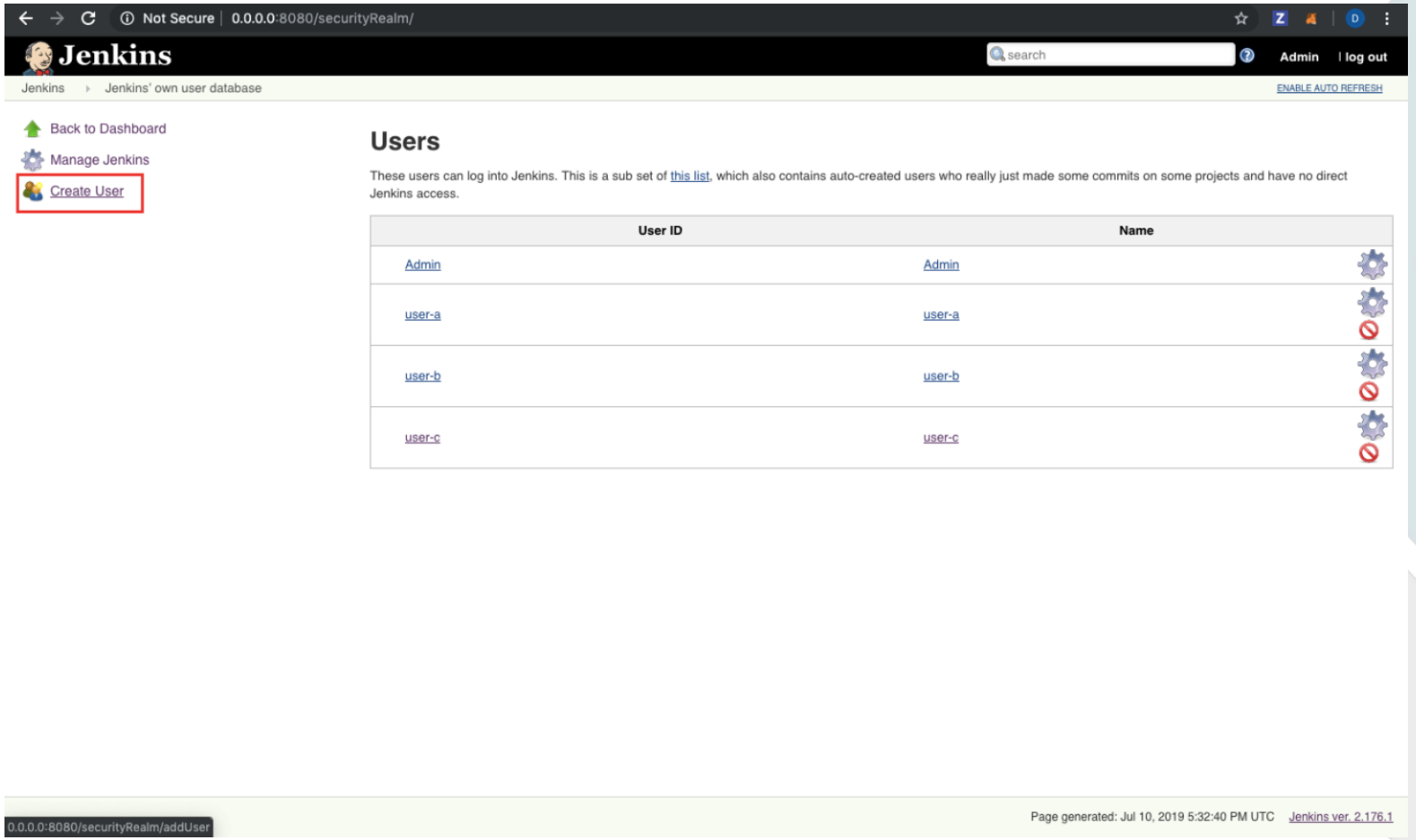
Steps to create users

- Select Manage Users



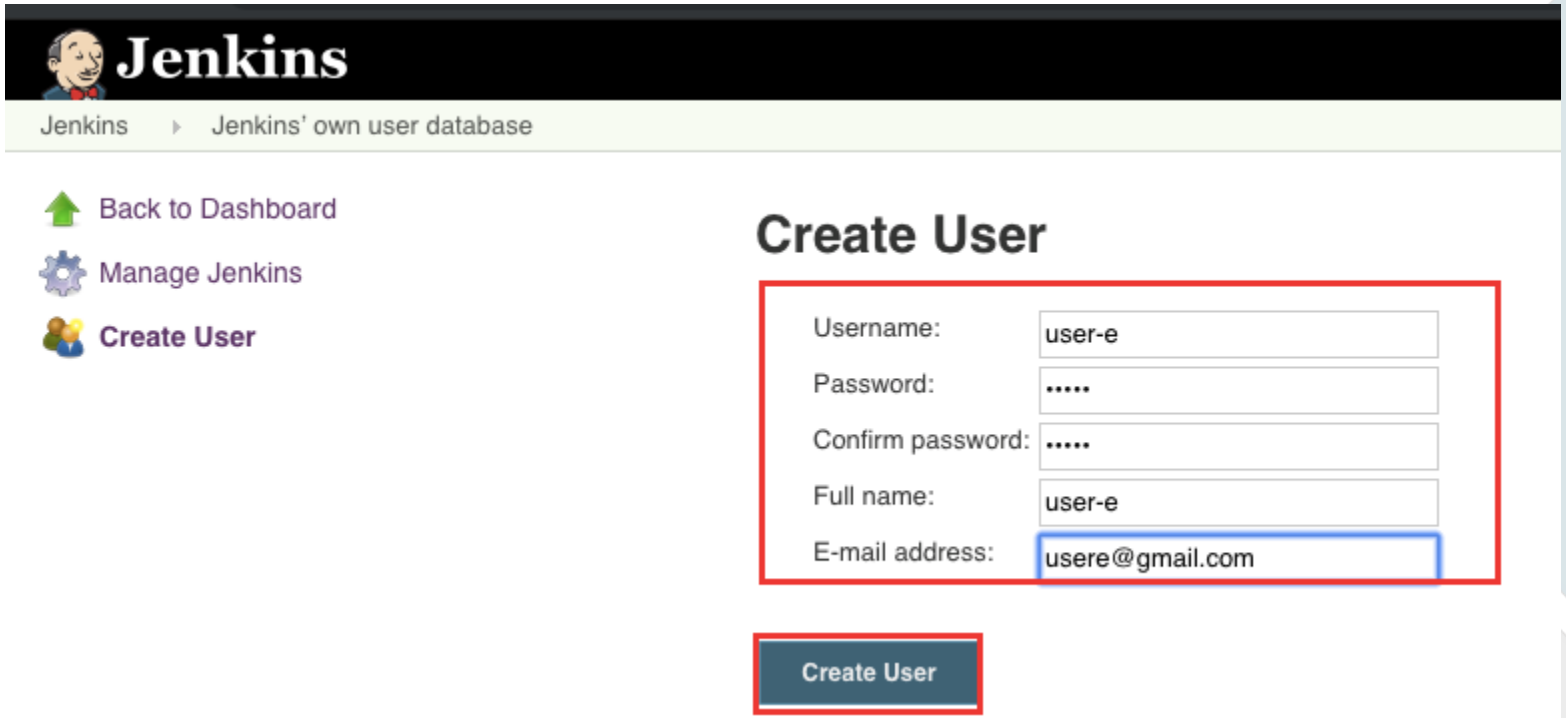
Cont'd…

- Select Create User



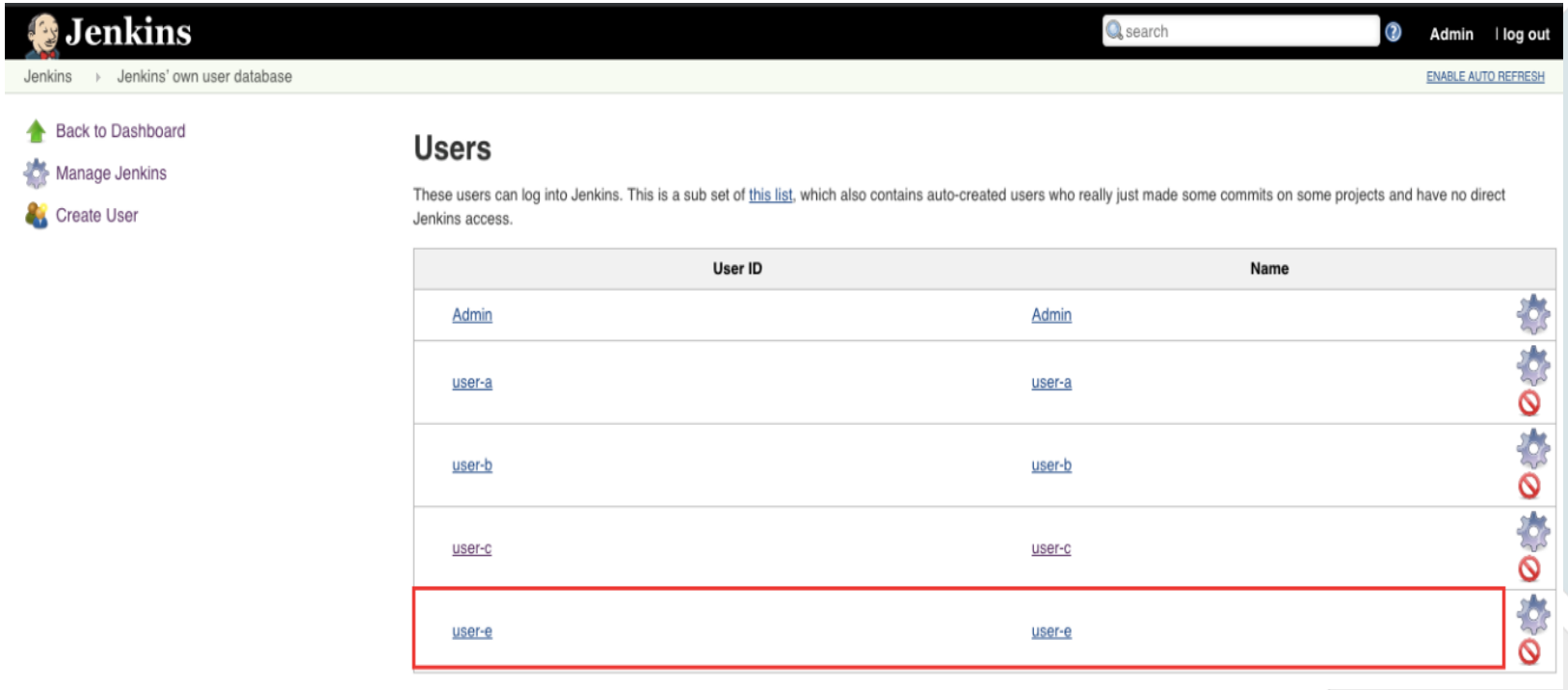
Cont'd…

- Give credentials



Cont’d…

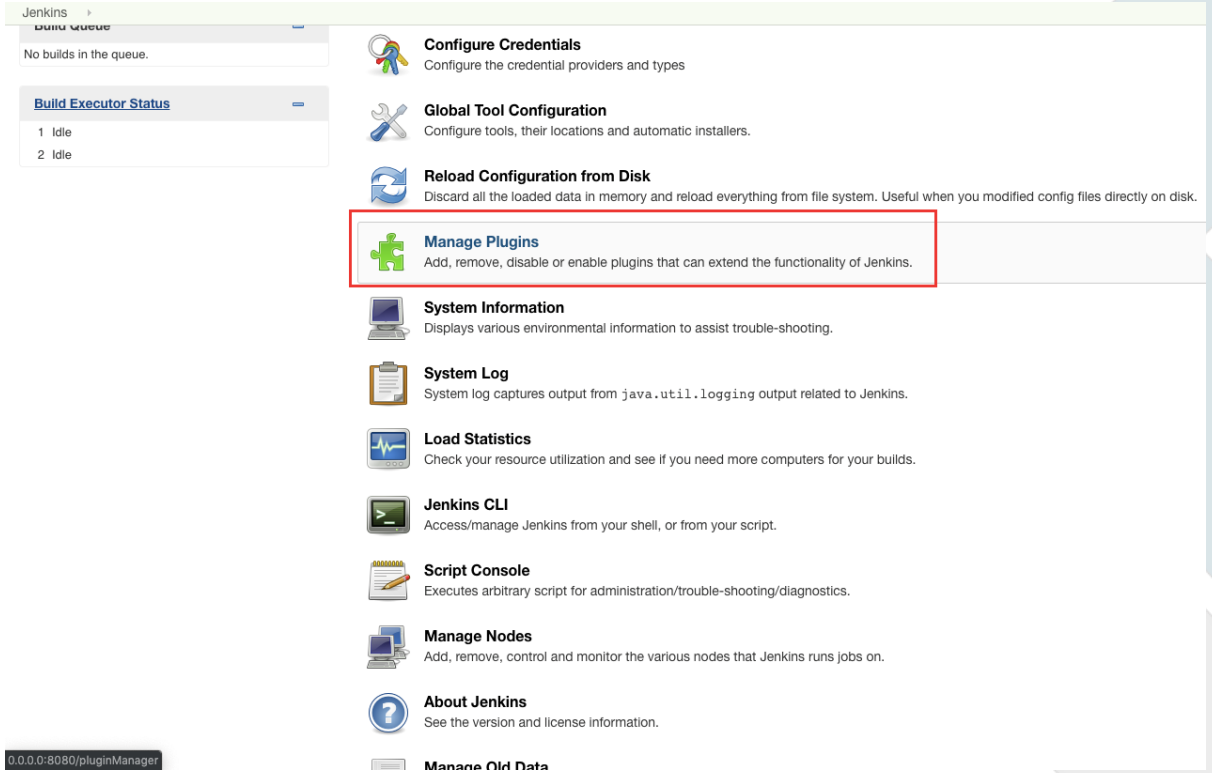
- User created



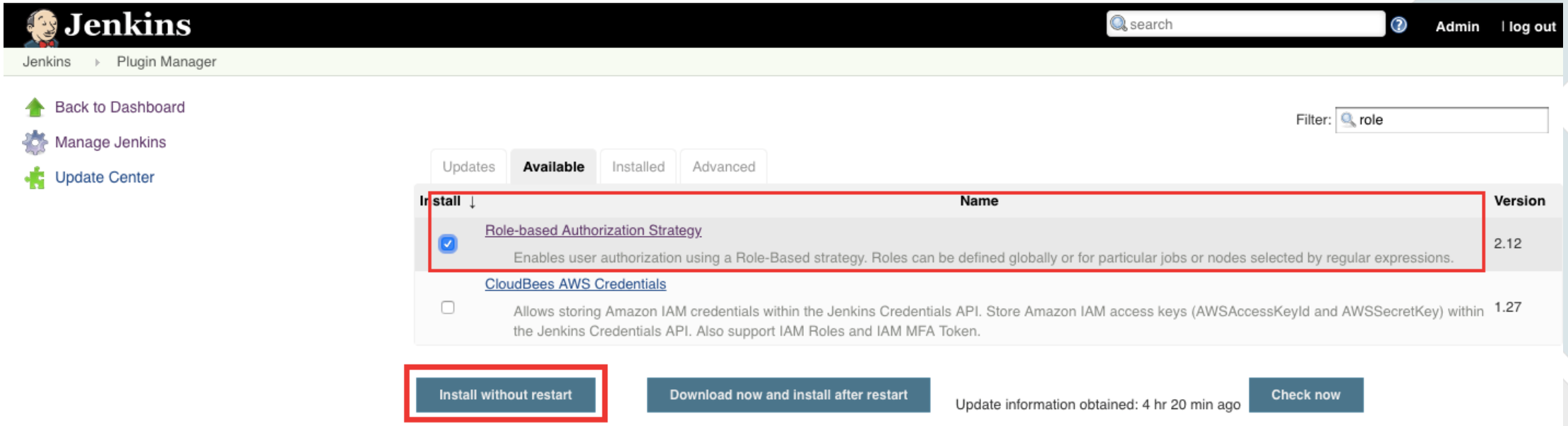
Cont'd…

Step 6:

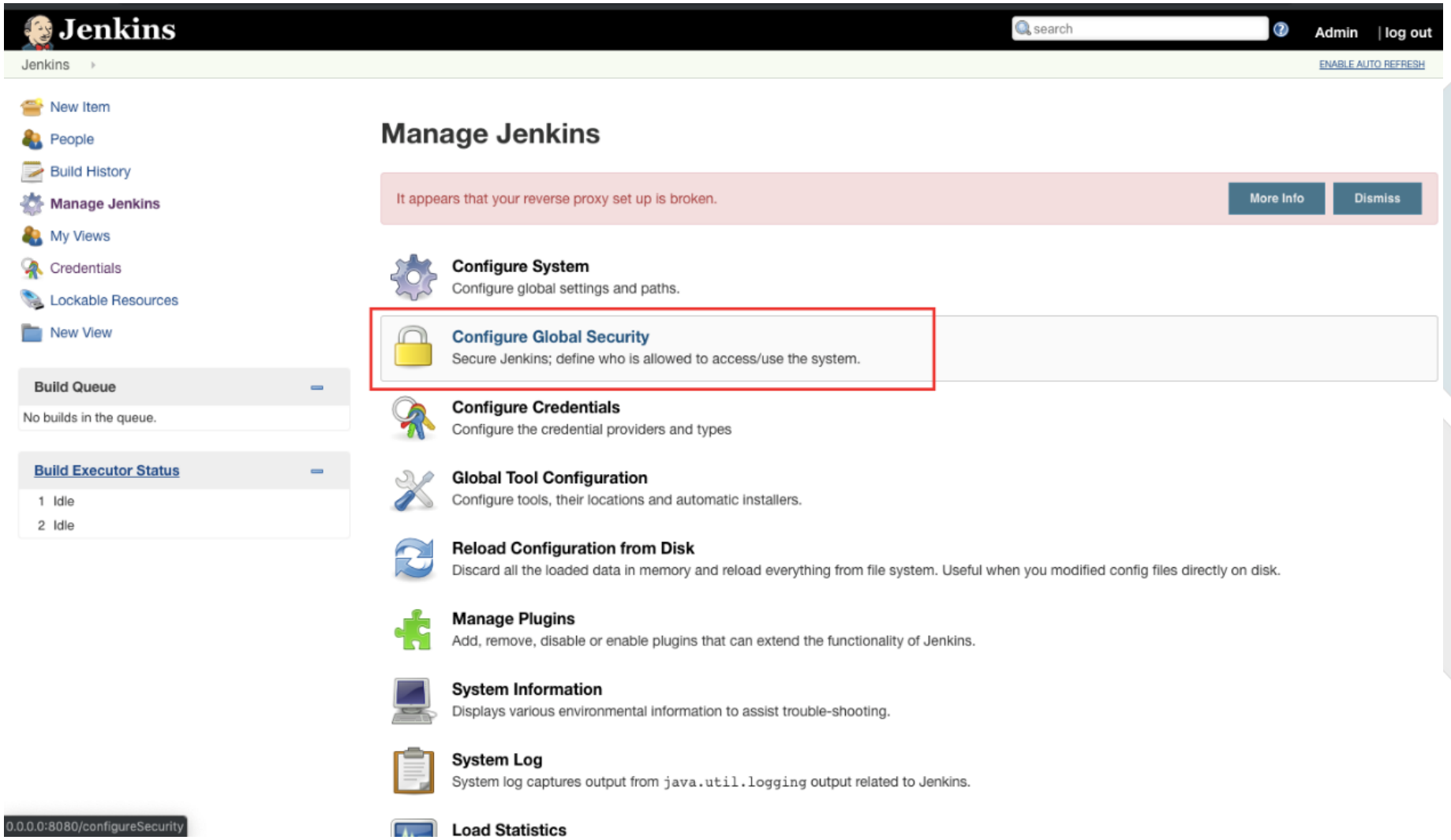
- To create user roles we need to follow the steps below.
  - Go to Jenkins dashboard
  - Manage Jenkins->Manage plugins->Go to available ->Select Role-based Authorization Strategy
  - click on Install without restart



Cont'd…

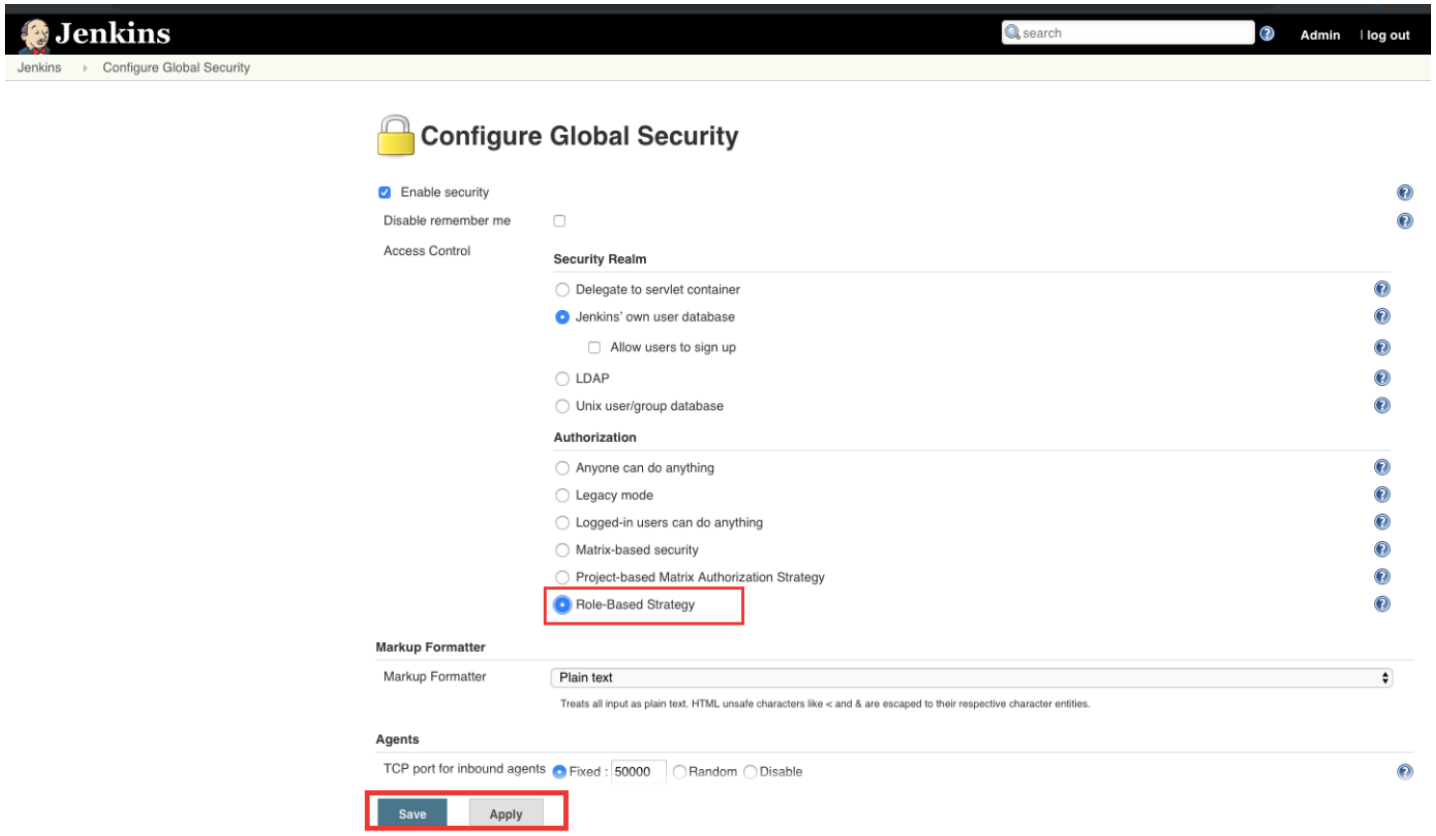

Jenkins
search
Admin
log out
Jenkins
Plugin Manager
Back to Dashboard
Manage Jenkins
Update Center
Filter: role
Updates
Available
Installed
Advanced
Install
Name
Version
Role-based Authorization Strategy
Enables user authorization using a Role-Based strategy. Roles can be defined globally or for particular jobs or nodes selected by regular expressions.
2.12
CloudBees AWS Credentials
Allows storing Amazon IAM credentials within the Jenkins Credentials API. Store Amazon IAM access keys (AWSAccessKeyId and AWSSecretKey) within the Jenkins Credentials API. Also support IAM Roles and IAM MFA Token.
1.27
Install without restart
Download now and install after restart
Update information obtained: 4 hr 20 min ago
Check now

Cont'd…


Jenkins
search
Admin
| log out
Jenkins
ENABLE AUTO REFRESH
New Item
People
Build History
Manage Jenkins
My Views
Credentials
Lockable Resources
New View
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle
Manage Jenkins
It appears that your reverse proxy set up is broken.
More Info
Dismiss
Configure System
Configure global settings and paths.
Configure Global Security
Secure Jenkins; define who is allowed to access/use the system.
Configure Credentials
Configure the credential providers and types
Global Tool Configuration
Configure tools, their locations and automatic installers.
Reload Configuration from Disk
Discard all the loaded data in memory and reload everything from file system. Useful when you modified config files directly on disk.
Manage Plugins
Add, remove, disable or enable plugins that can extend the functionality of Jenkins.
System Information
Displays various environmental information to assist trouble-shooting.
System Log
System log captures output from java.util.logging output related to Jenkins.
Load Statistics
0.0.0.0:8080/configureSecurity

Cont'd…

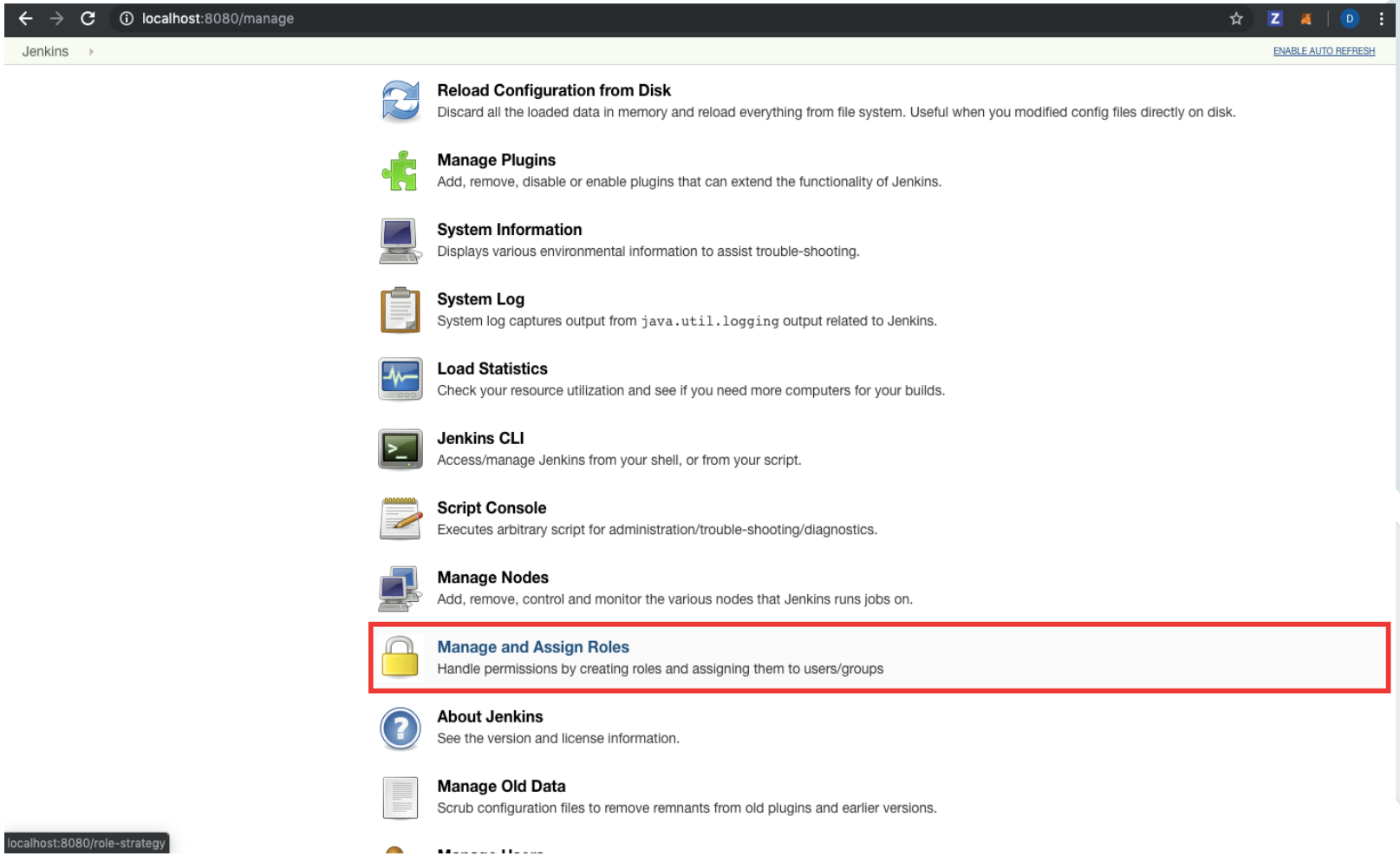
Now go to Configure global security->select Role Based Strategy



Create roles

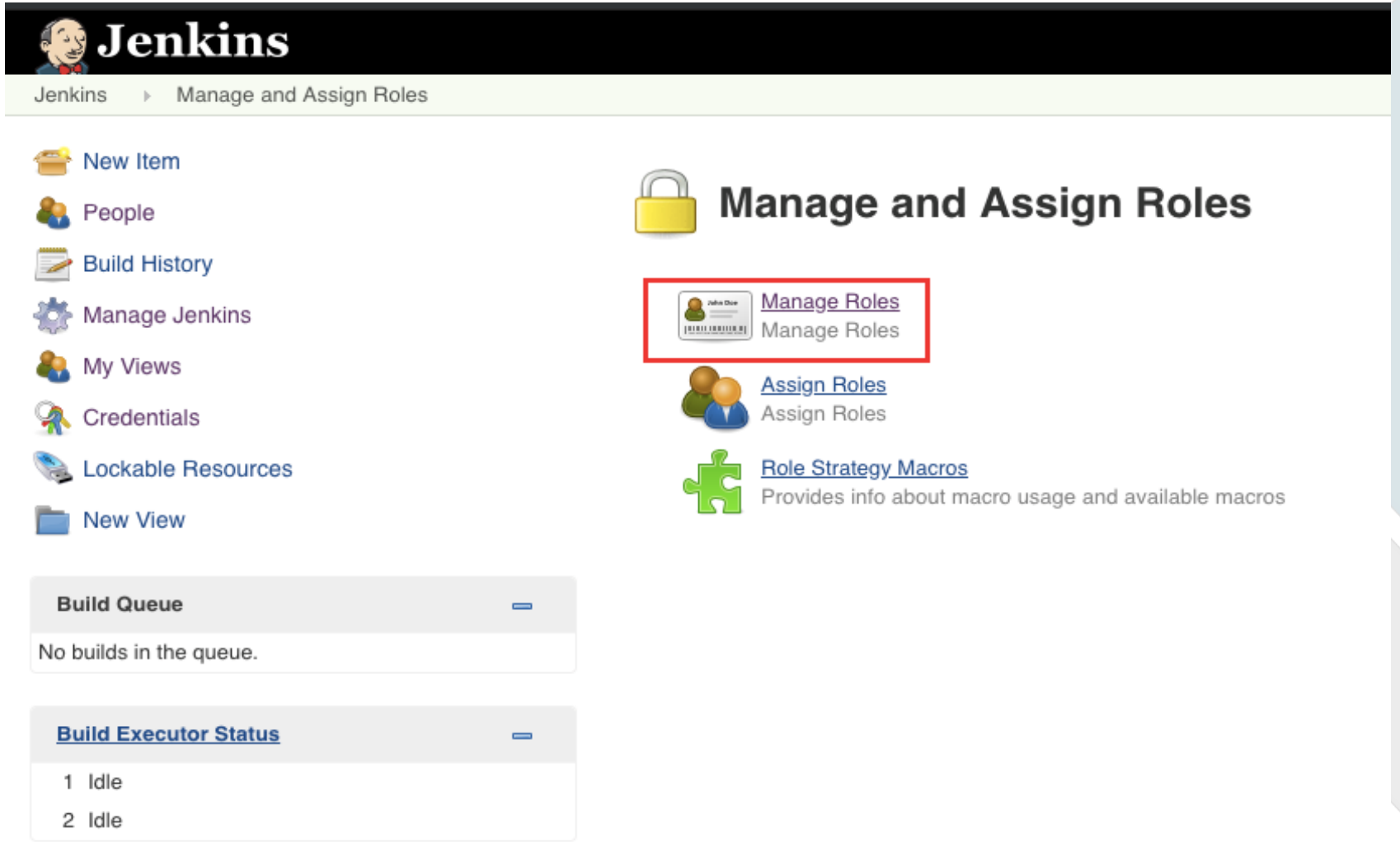
- To create roles:

Go to Manage Jenkins->Manage and Assign Roles



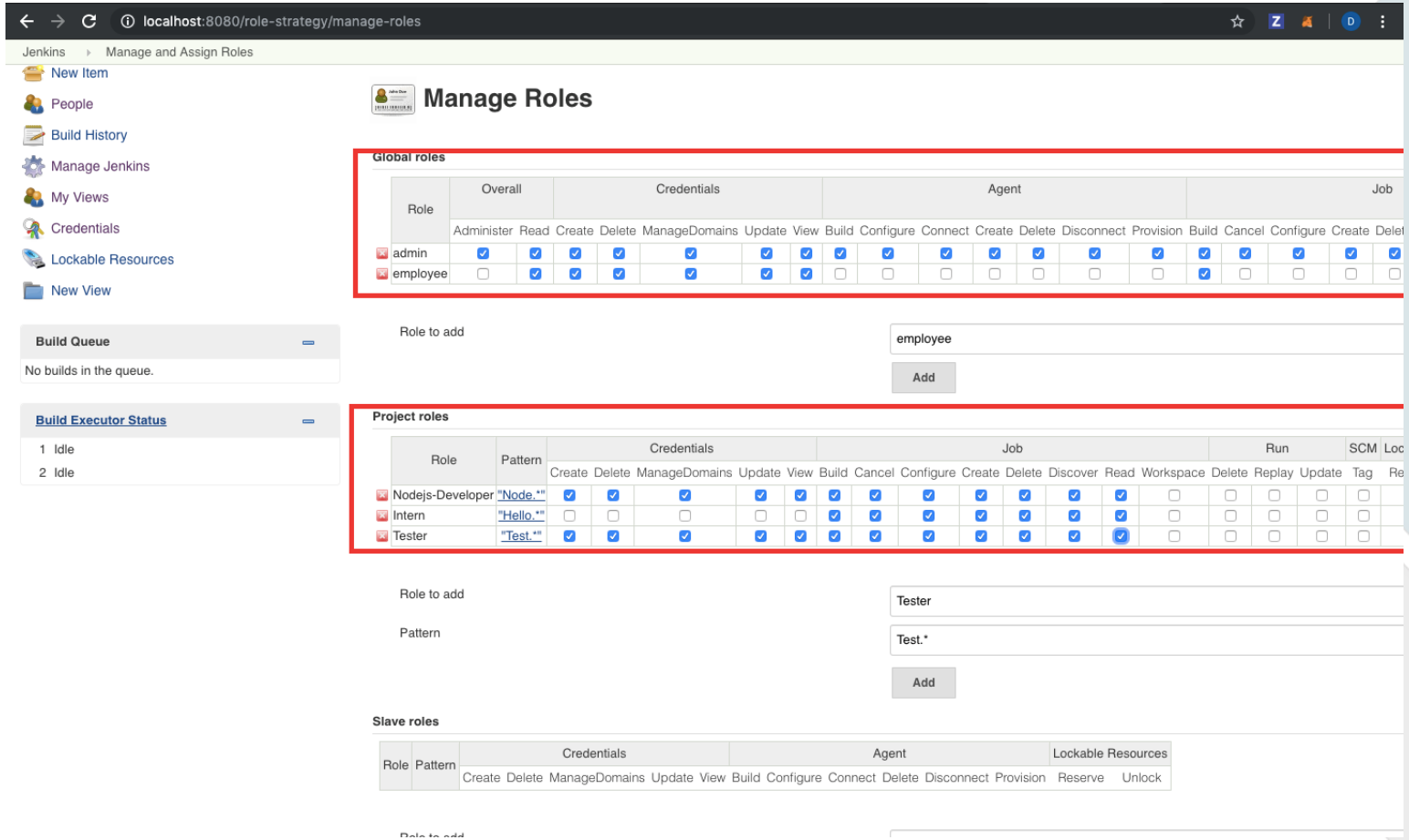
Cont'd…

- Click on Manage Roles



Cont'd…

- Create Global roles and project roles

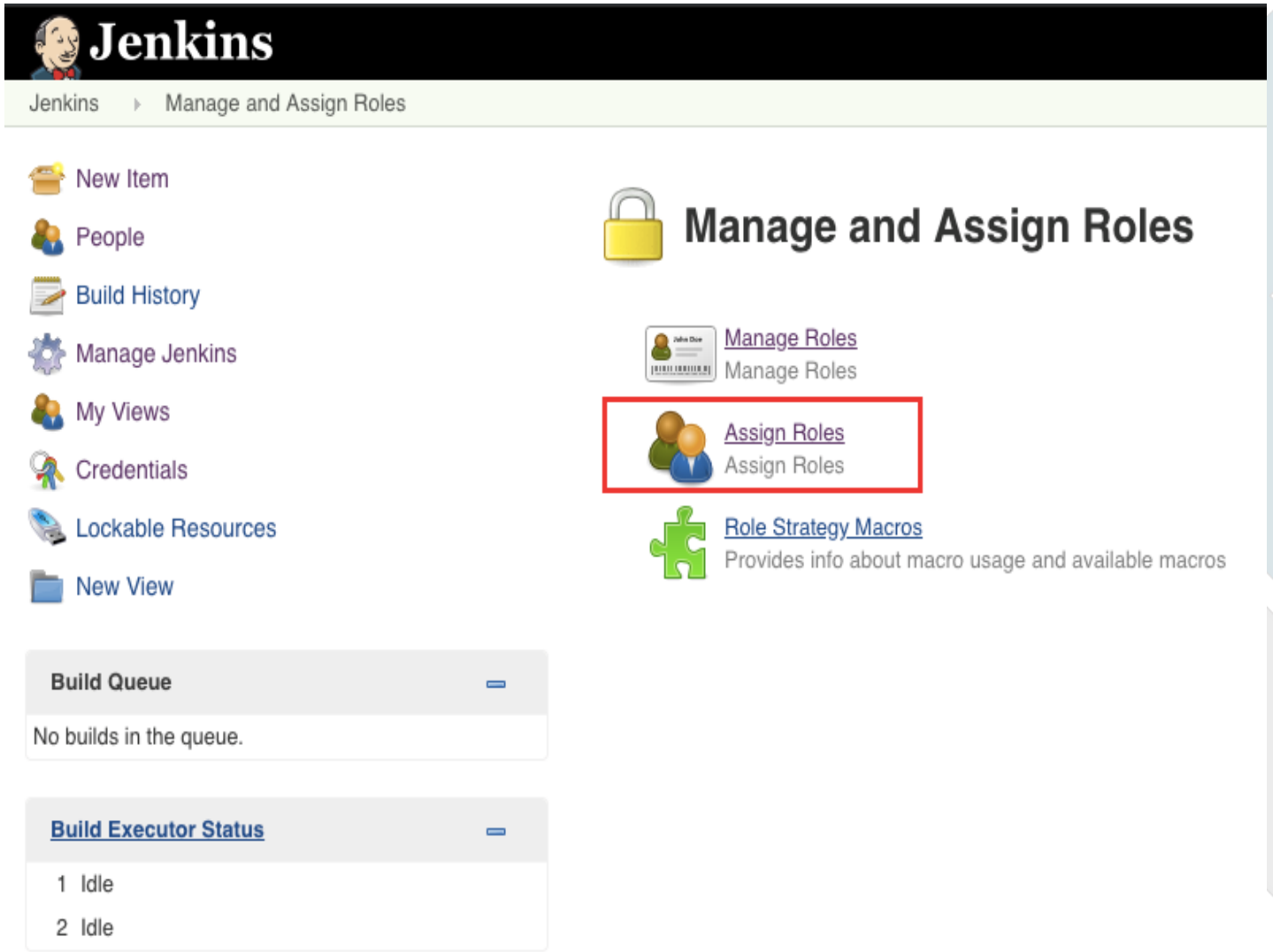


Cont'd…

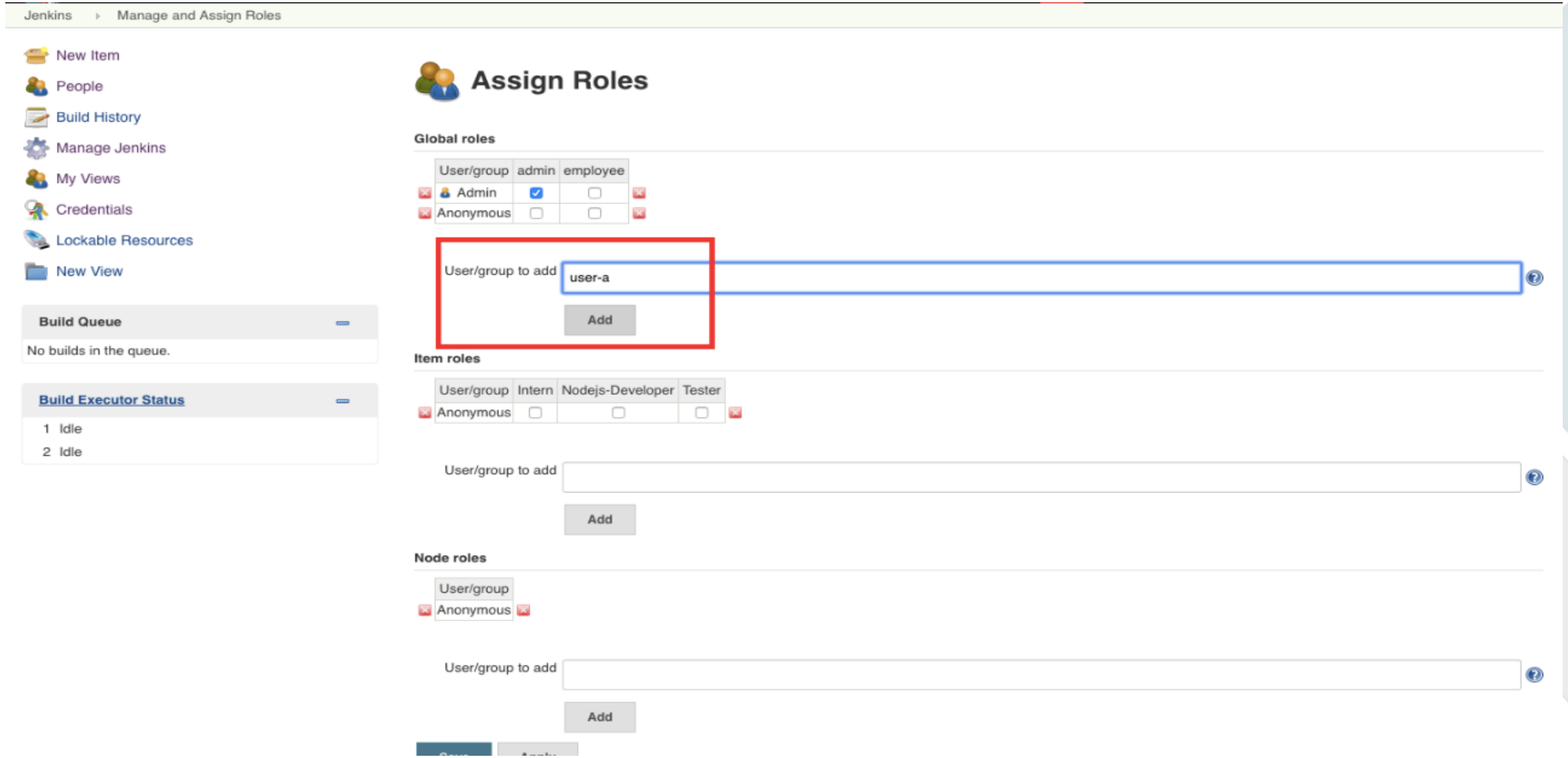
- Here we have added employee as global role, Under that we have created 3 Project roles as shown before
  - Global Role
  - Employee
  - Project Role
  - Nodejs-Developer - Pattern: Node.*
  - Tester - Pattern: Test.*
  - Intern - Pattern: Hello.*
- Created 3 new roles as developer, tester and intern
- Gave pattern of jobs
  - Nodejs-Developer only can access jobs which starts with Node.*
  - Tester can only access jobs with starts with Test.*
  - Interns can only access jobs starts with Hello.*

Assign Roles

- To assign roles:
  - Enter user name in User/group to add and click on Add to add user

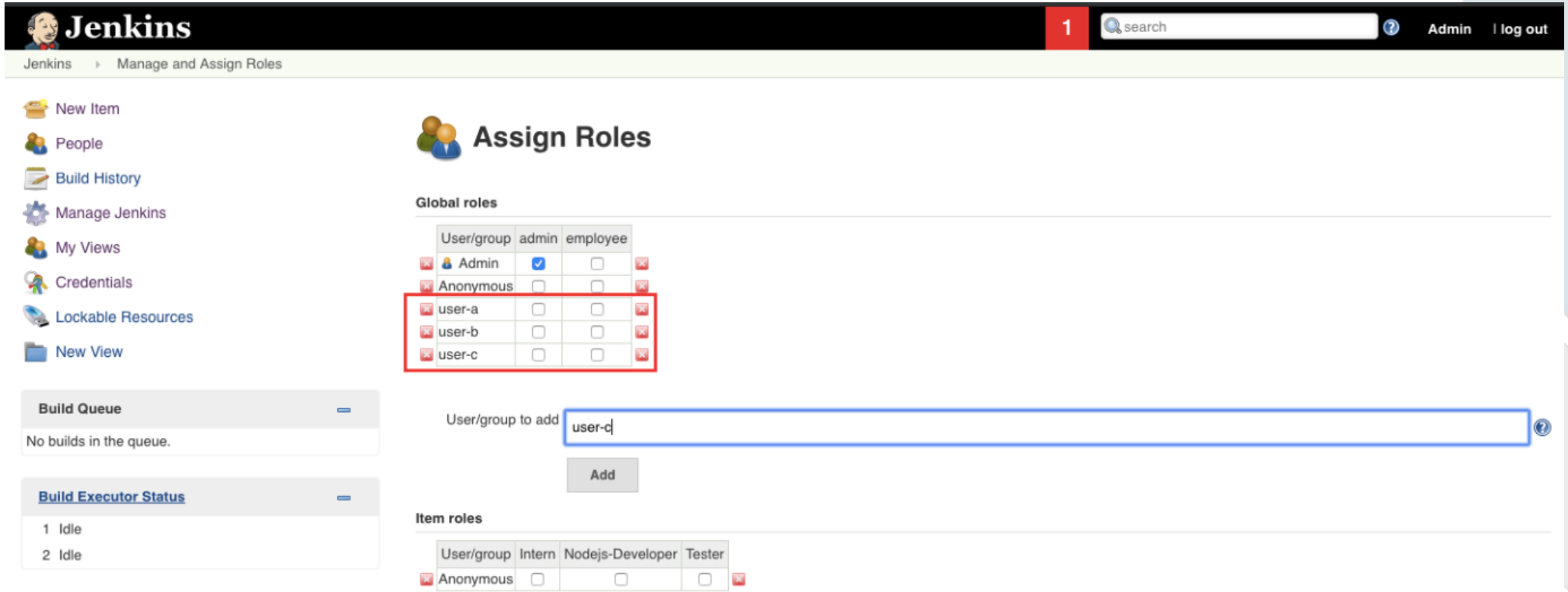


Cont'd…


Jenkins
Manage and Assign Roles
New Item
People
Build History
Manage Jenkins
My Views
Credentials
Lockable Resources
New View
Build Queue
No builds in the queue.
Build Executor Status
1 Idle
2 Idle
Assign Roles
Global roles
User/group
admin
employee
Admin
Anonymous
User/group to add
user-a
Add
Item roles
User/group
Intern
Nodejs-Developer
Tester
Anonymous
User/group to add
Add
Node roles
User/group
Anonymous
User/group to add
Add

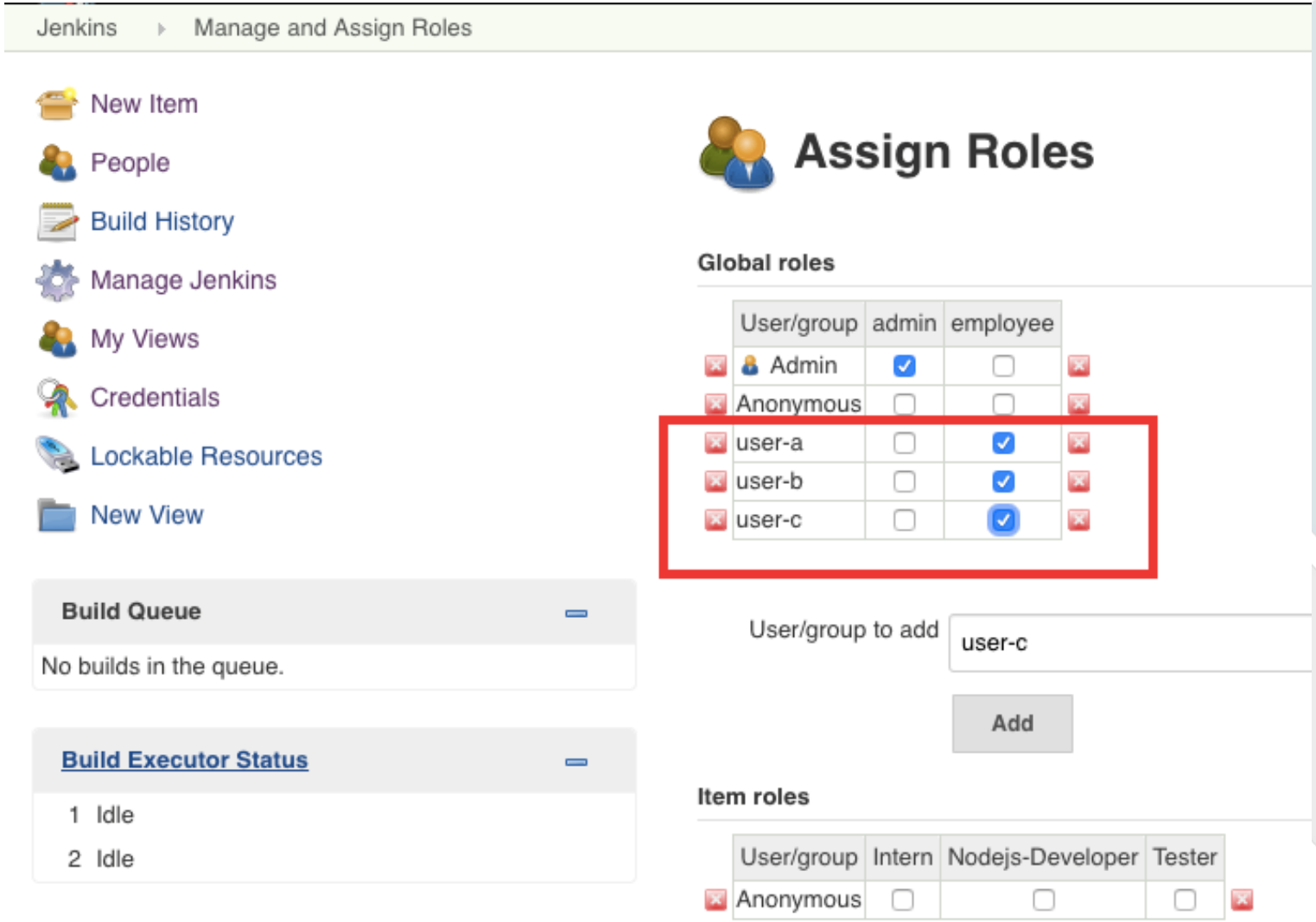
Cont'd…

- Assign the global role as employee for the created 3 users



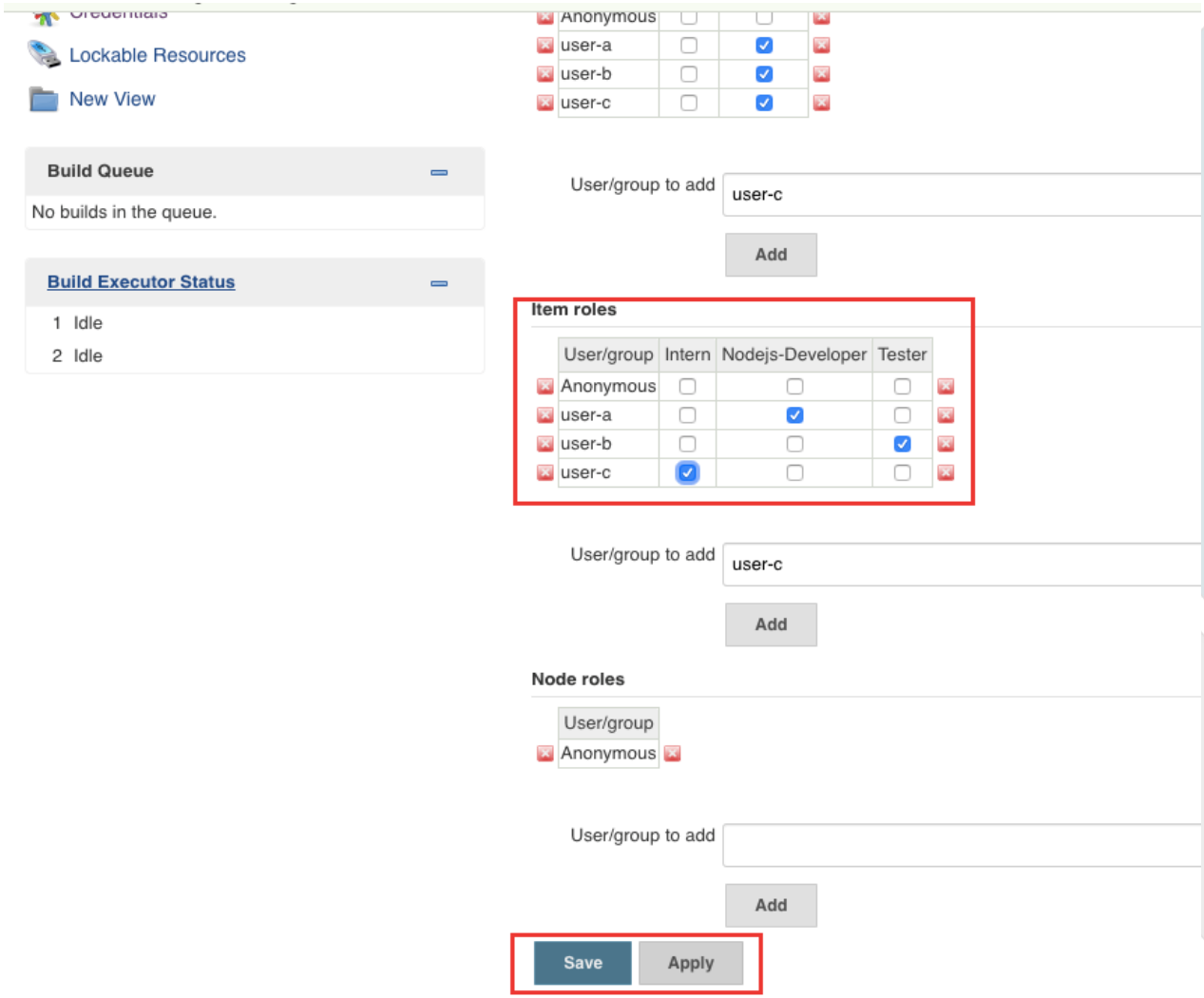
Cont'd…

- Add users to assign for project roles



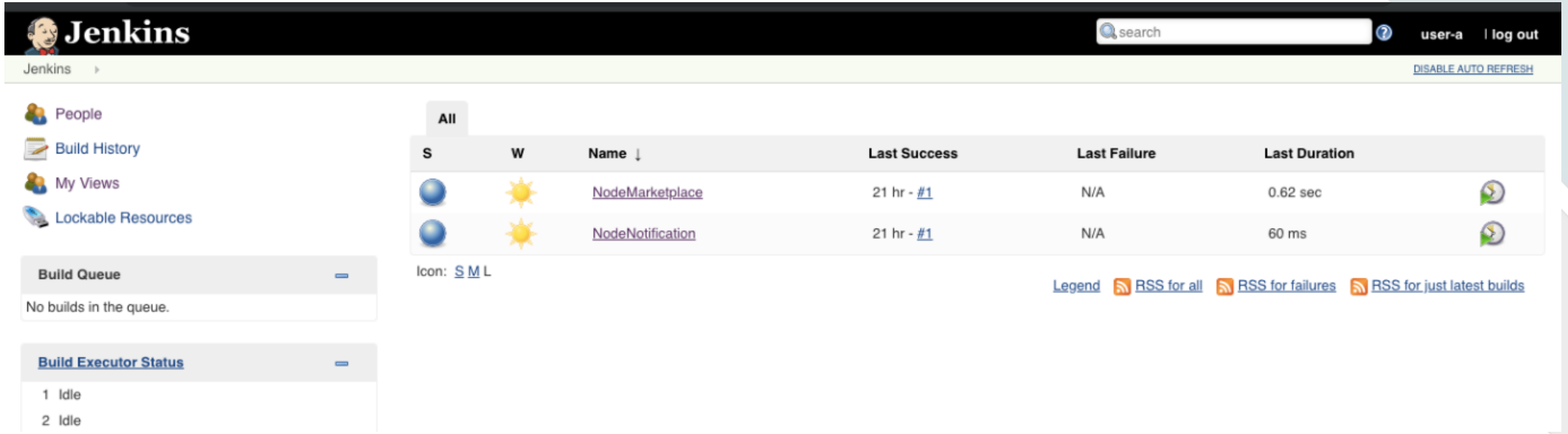
Cont’d…

- Add users to assign for project roles
- Save and exit



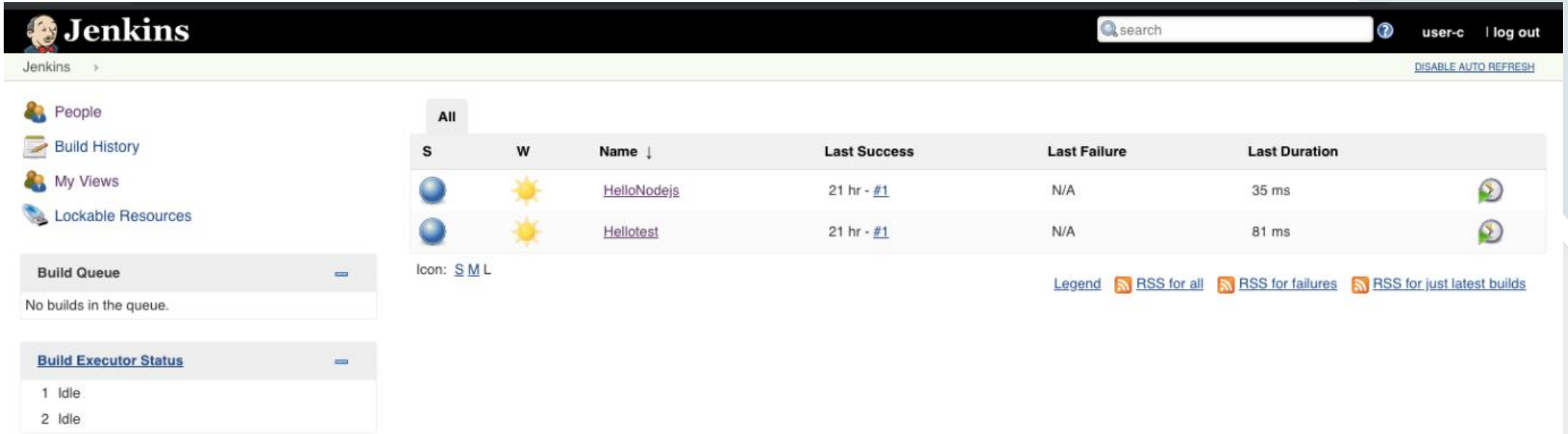
Cont’d…

- Logout and login as user-a
- As user-a is a developer, access to jobs which starts with Node



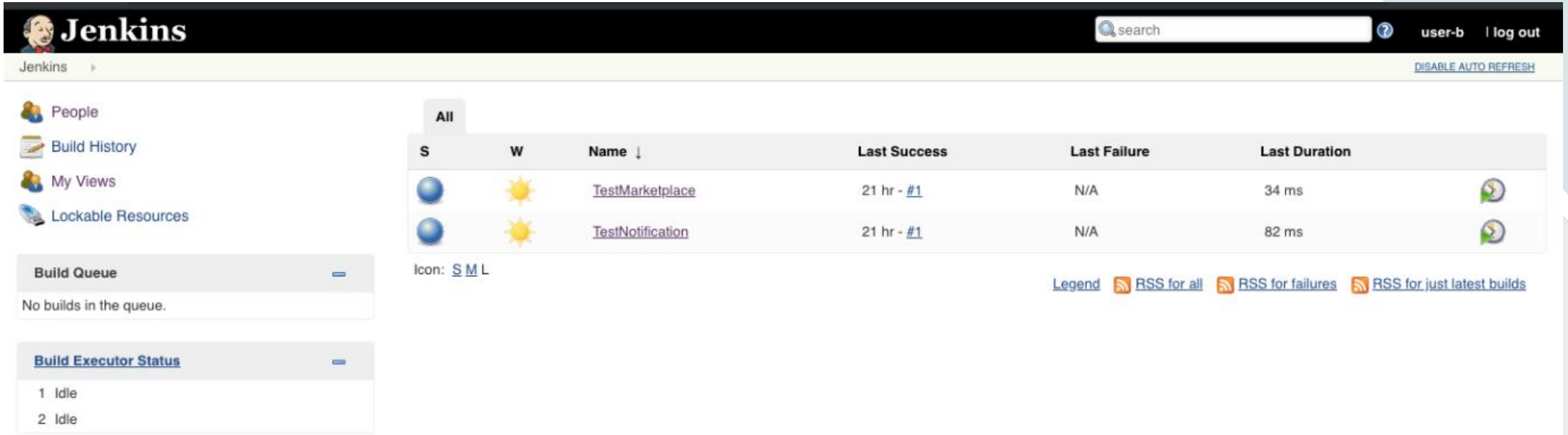
Cont'd…

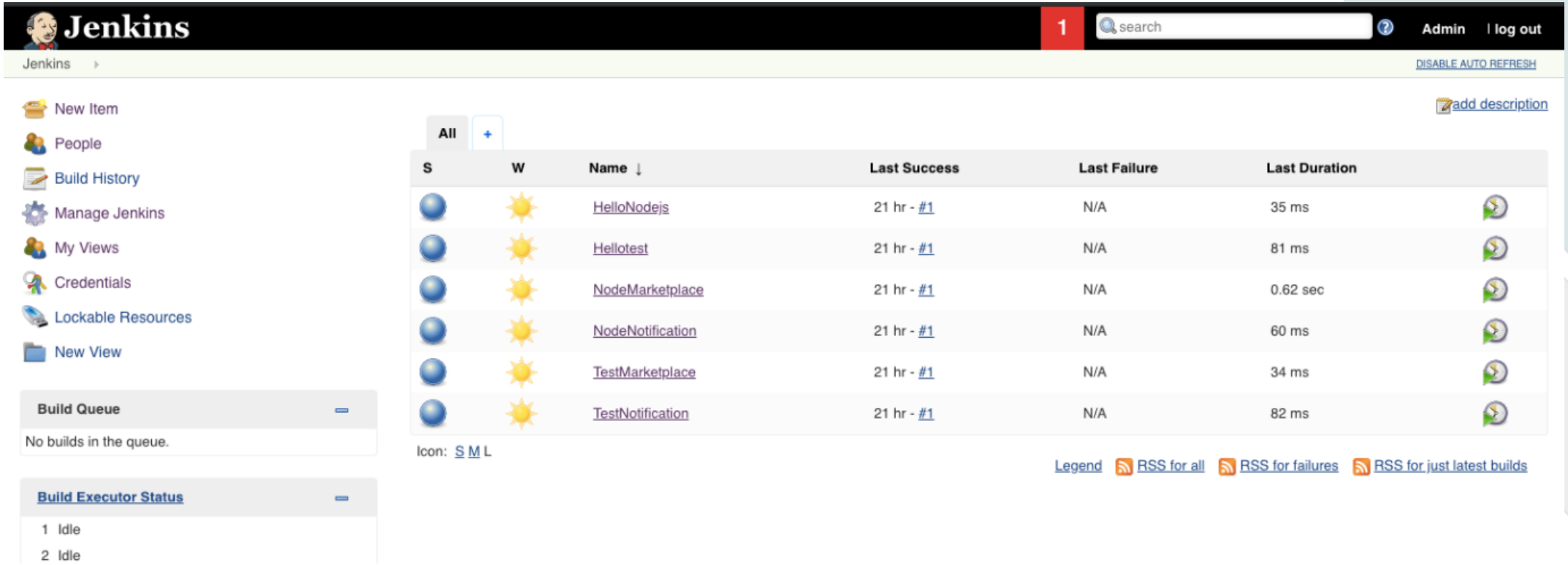
- Login as user-c
- To access jobs which starts with Hello



Cont'd…

- Login as user-b
- To access jobs which starts with Test



Cont'd…

- Login as Admin to access all jobs
- Create role-based access for the users in Jenkins