Jenkins

Securing Jenkins

Lesson Objectives

In this lesson, you will learn about:

- Introduction
- Securing Jenkins using Security realms
  - Authentication
  - Authorization
- How to configure/setup matrix based security

Introduction

- As default in Jenkins, all users are allowed to create, configure and run build jobs.
- To secure project configuration in a larger organization setups, Jenkins supports with enabling of security.
- Jenkins supports several security models, and can integrate with several user repositories.
- Also Jenkins supports with Authentication and authorization mechanisms.
- For authenticating users, Jenkins offers number of options.
- Authorization can be either project specific, or Jenkins environment specific.

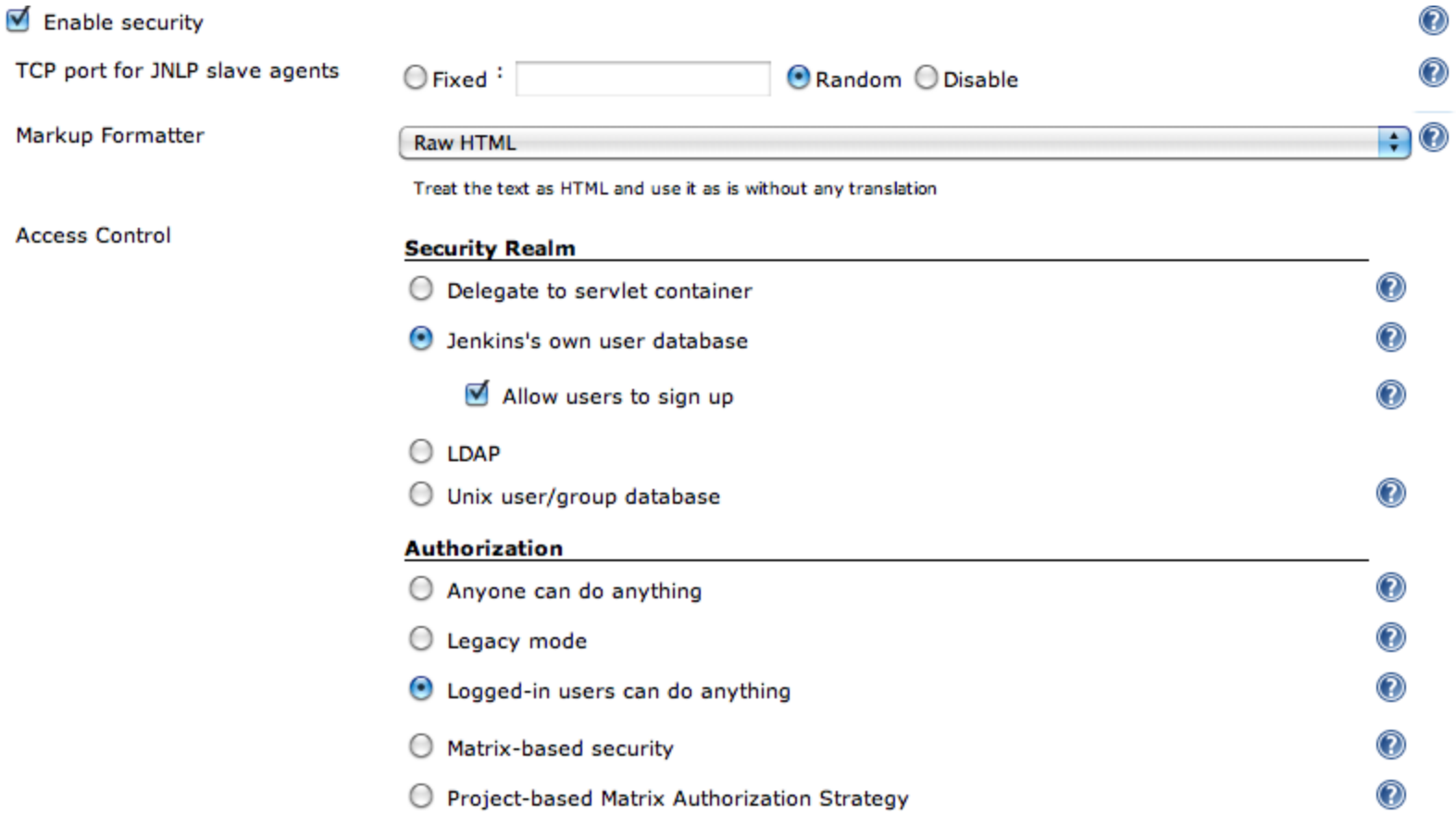
Securing Jenkins using Security realms

- Jenkins identifies and manage users in a number of ways from built-in user database to integration with enterprise directories.
- Users can be authenticated in any on the way as listed below:
  - Simple Security
  - Using Jenkins Built-in User database.
  - Using an LDAP Repository.
  - Using Microsoft Active Directory
  - Using Unix Users and Groups
  - Delegating to the servlet Container,
  - Integrating with other systems.

Securing Jenkins using Security realms

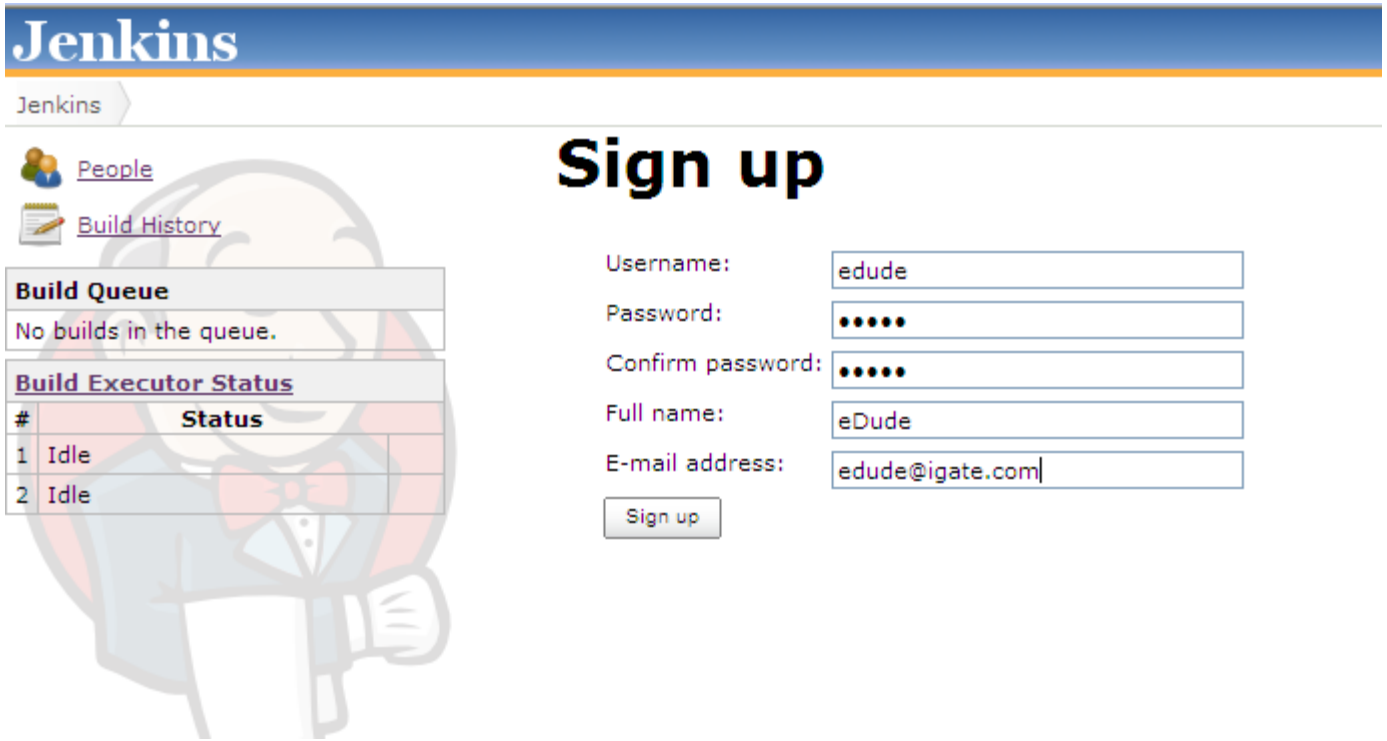
Activating Security in Jenkins

- In “Manage Jenkins” screen, Click on “ Configure Global Security” link and do the configuration as shown below:



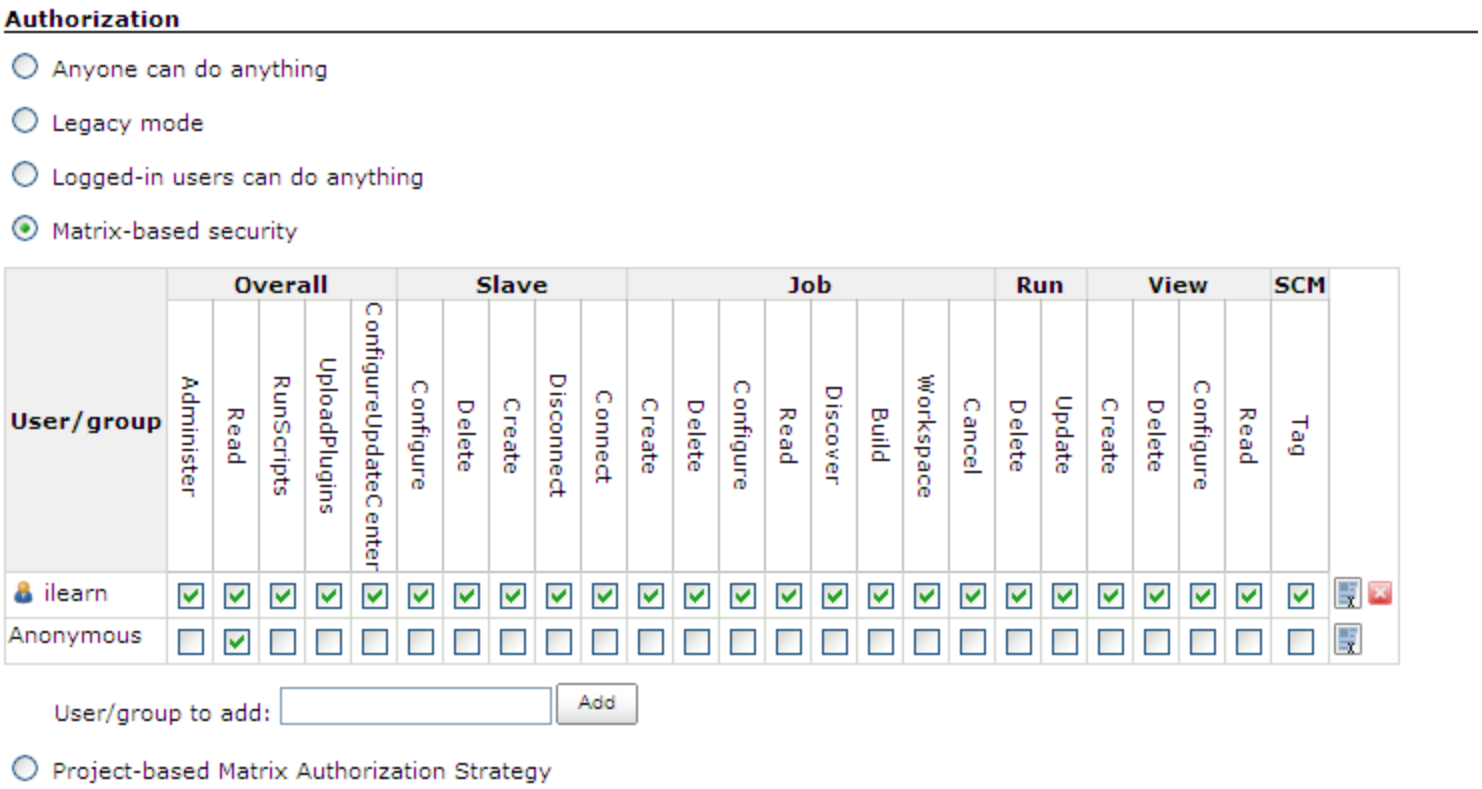
Securing Jenkins using Security realms- Simple Security in Jenkins

- In Jenkins dashboard screen, click on “signup” link to create a new user and fill the details as shown below:



Securing Jenkins using Security realms- Authentication and Authorization

To assign authentication strategies for authorized persons, do the configuration as shown below in “enabling security”:



Summary

In this lesson, you have learnt about:

- Introduction
- Securing Jenkins using Security realms
  - Authentication
  - Authorization
- How to setup/configure matrix based security and use it