DevOps

Caltech | Center for Technology & Management Education

Post Graduate Program in DevOps

simplilearn

DevOps

Caltech | Center for Technology & Management Education

CI/CD Pipeline with Jenkins

simplilearn

Jenkins Administration

Learning Objectives

By the end of this lesson, you will be able to:

- Outline the options available for authentication in Jenkins
- Discuss the options available for authorization in Jenkins
- Set up roles and permissions for selected users
- Explain how to perform Jenkins maintenance

Jenkins Permissions

Global Security Configuration

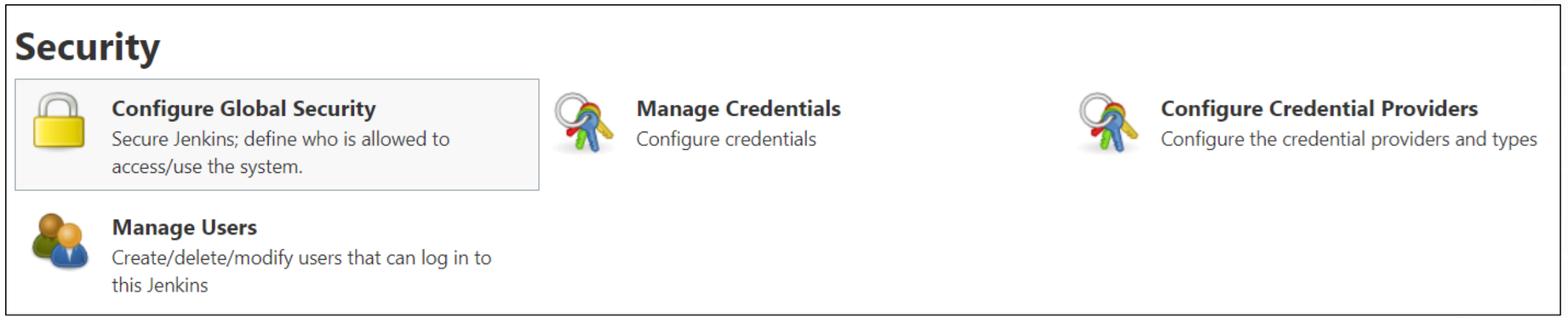
Jenkins supports security features that enable developers to make Jenkins more secure. This can be achieved by using Global Security Configuration.

Global Security Configuration

Includes both authorization and authentication features to restrict access to limited users only	Adds roles and permissions for individual users to restrict Jenkins access	Assigns custom permissions to different users in Jenkins application

Global Security Configuration

To set up security configurations, click **Manage Jenkins** and choose the **Configure Global Security** option.



Jenkins Authentication

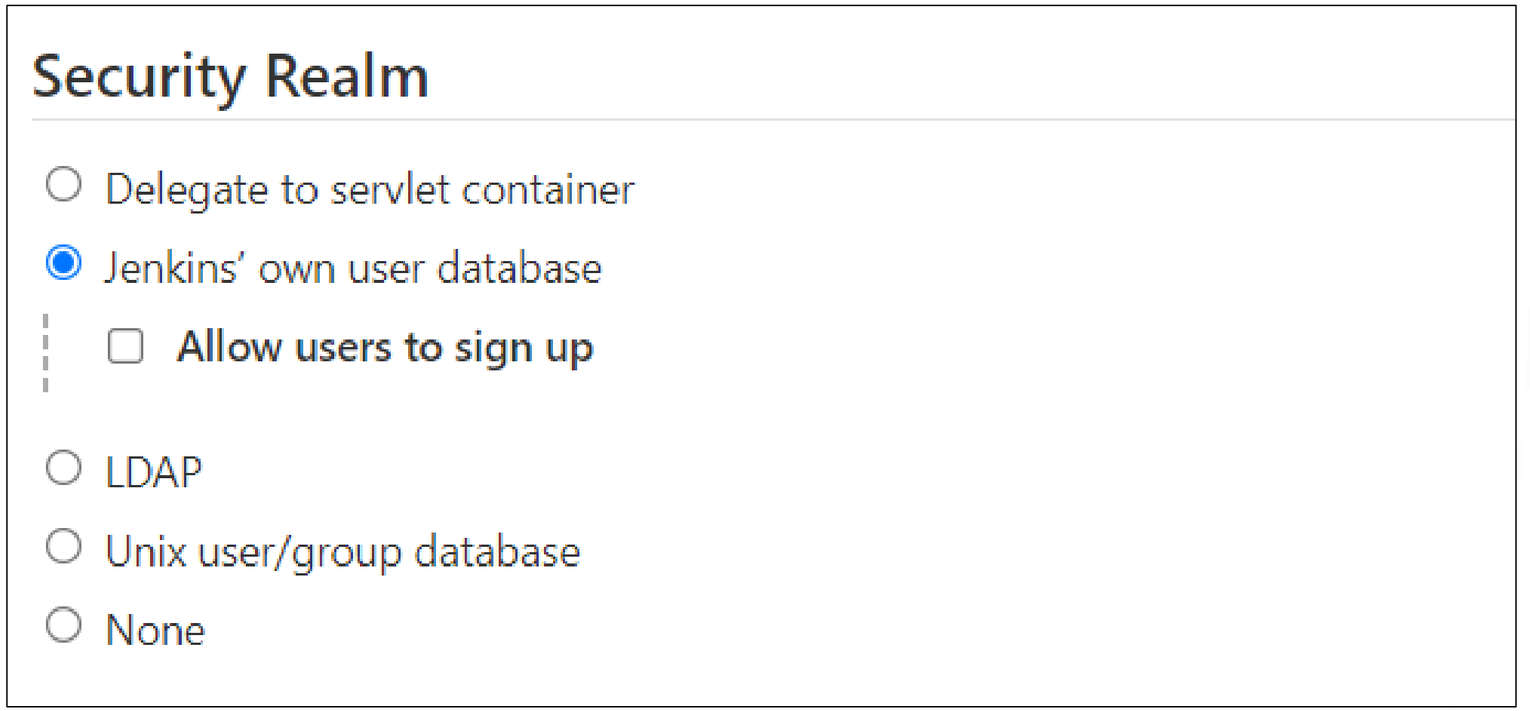
Jenkins Authentication enables developers to restrict usage of Jenkins to authenticated users only.

Jenkins Authentication locks access to Jenkins UI so that only an authenticated user will be able to log into Jenkins to access Build jobs.

Individual users will not gain unwanted access to critical Jenkins jobs like production deployment jobs and code scan jobs.

Jenkins Authentication

The Security Realm authentication enables developers to select an authentication source that will be used by Jenkins to authenticate users. This can be done as shown below:



Authentication Using Delegate to Servlet Container

The authentication is managed by a servlet container running Jenkins controller such as:

- Apache Tomcat
- Jetty
- Glassfish

Refer servlet container's authentication documentation for implementing authentication using servlet container.

Authentication Using Jenkins' Own User Database

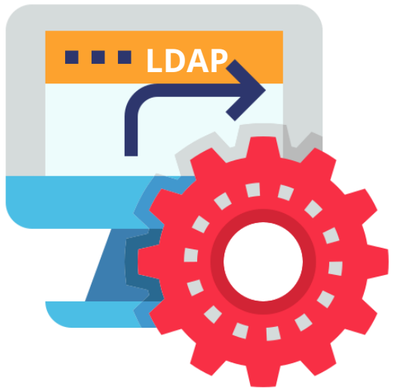
Jenkins provides its own built-in user database, the **Own User Database**, for authentication, instead of depending on an external authentication system.

- Provides **Manage Users** section to add, modify, or delete Jenkins users in Jenkins
- Is enabled by default in new Jenkins 2.0 or later installations
- Facilitates performing authentication for users in small and non-critical environments

User details are stored as an XML file in JENKINS_HOME path and passwords are stored in an encrypted format.

Authentication Using LDAP

Jenkins provides support for **LDAP** server using which admins can authenticate users fetched from the LDAP server.



- This plugin supports different LDAP installations such as Active Directory or openLDAP.
- It is the most common option used by larger organizations.
- It enables admins to manage users within Jenkins, as well as existing identities using LDAP plugins.

Authentication Using Unix User/Group Database

The Jenkins **Unix User/group database** option provides authentication with the help of Unix operating system user database.

- Users can log into Jenkins using the Unix username and password.
- Both Unix users and groups are used as a mode of authentication.
- A PAM library is used to implement authentication.

To use group name, prefix '@' to group name. A normal user can be directly configured in Jenkins without any prefix.

Authentication Using Unix User/Group Database

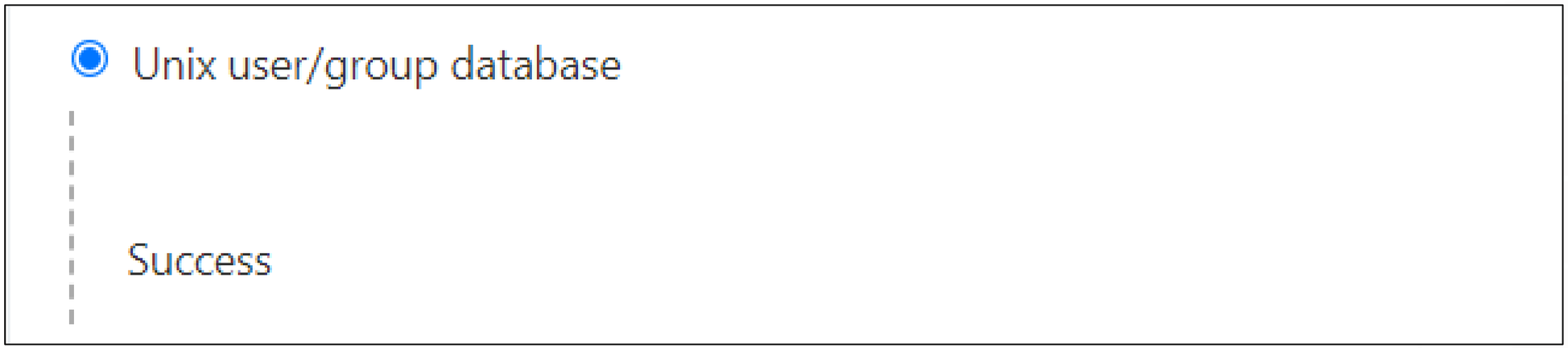
To configure authentication using the Unix User/group Database method, provide the required read permissions to **/etc/shadow** file using the **chmod o+r /etc/shadow** command.

The screenshot below shows the command being entered in the Unix command line.

```
root@ip-172-31-63-38:~# ls -lart /etc/shadow
-rw-r----- 1 root shadow 991 Jul 16 13:11 /etc/shadow
root@ip-172-31-63-38:~# chmod o+r /etc/shadow
root@ip-172-31-63-38:~# ls -lart /etc/shadow
-rw-r--r-- 1 root shadow 991 Jul 16 13:11 /etc/shadow
root@ip-172-31-63-38:~#
```

Authentication Using Unix User /Group Database

Upon successful addition of the required permissions, the Jenkins dashboard will flash a notification as shown:

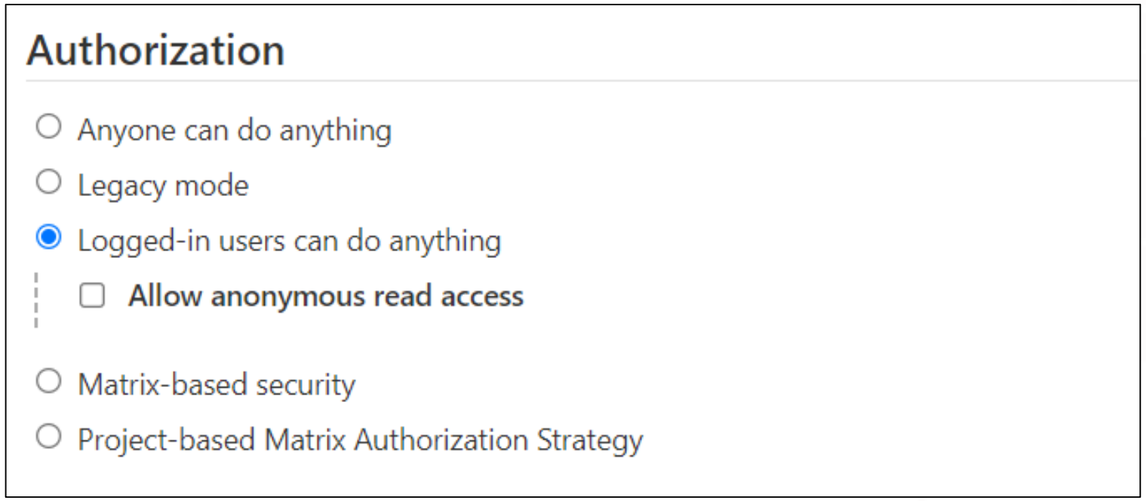


Jenkins Authorization

Authorization indicates what an individual can access in Jenkins CI once authenticated.

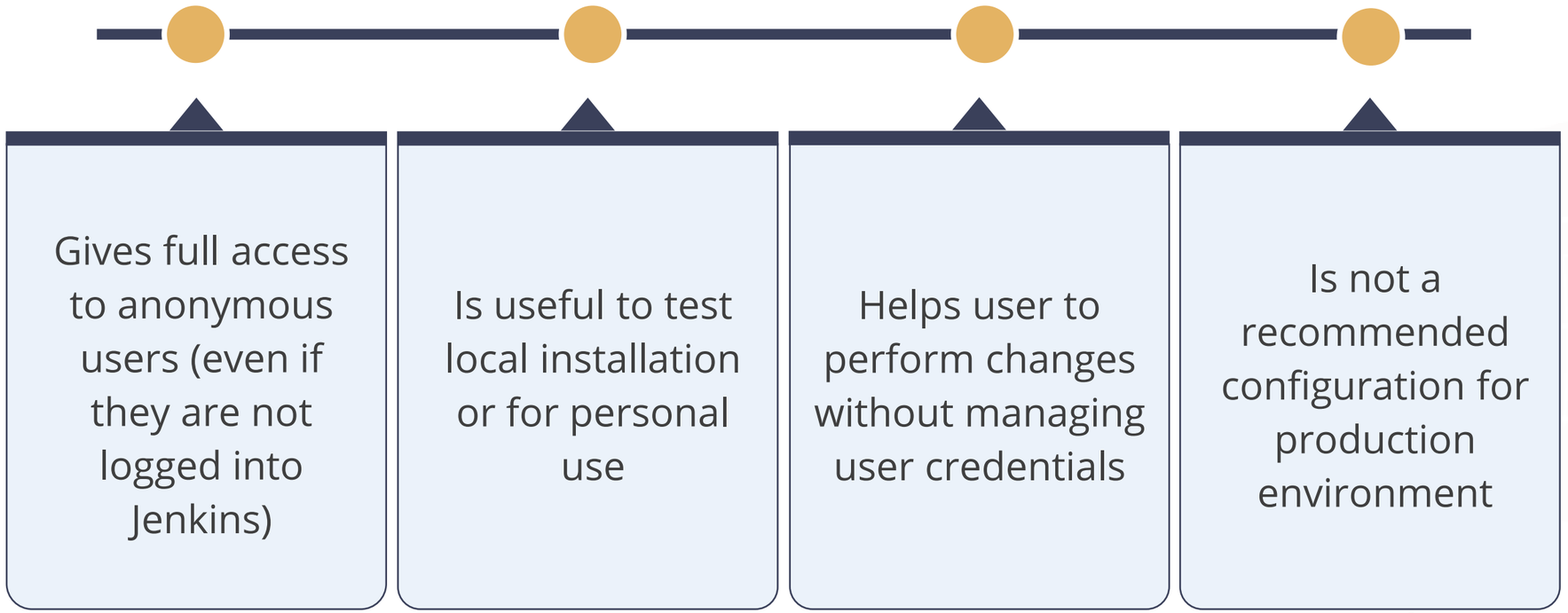
Shown below are the various authorization options available in Jenkins:

Assign specific roles to individual users without giving similar admin access to every user.



Authorization: Anyone Can Do Anything

The **Anyone can do anything** option enables everyone to get full control of Jenkins.



Authorization: Legacy Mode

The **Legacy Mode** option works in the same manner as Jenkins did before version 1.164.

- This configuration looks for a user with name admin to grant full control and administrator access.
- The configuration can be used to grant full access to any user. Other users will be treated as anonymous users with read-only access.
- This option is not encouraged in Jenkins 2.0 or the latest version of Jenkins.

Authorization: Logged-In Users Can Do Anything

Logged-in users can do anything allows every logged in user to gain full control of Jenkins.

1. Gives read-only access to anonymous users
2. Helps in auditing
3. Is suitable for publicly exposed Jenkins

Authorization: Matrix-Based Security

The **Matrix-based security** option is used to configure custom permissions to restrict access to specific components.

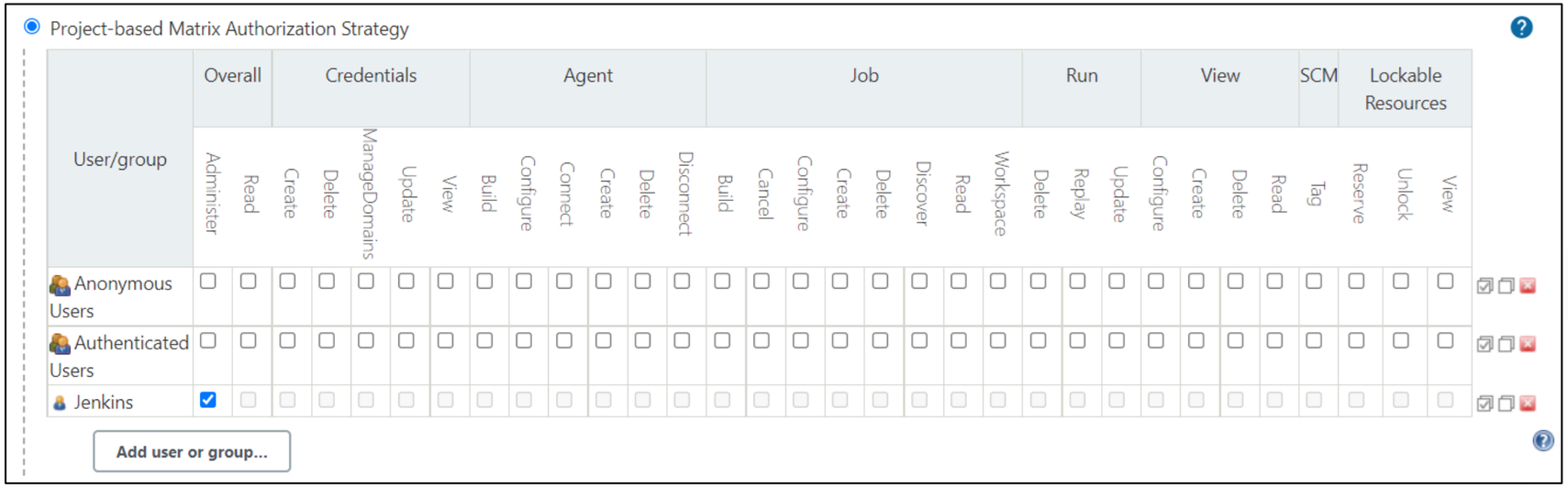
Configure custom permissions to authorize every user allowed access to Jenkins.

User/group	Overall		Credentials					Agent						Job								Run			View				SCM	Lockable Resources		
	Administer	Read	Create	Delete	ManageDomains	Update	View	Build	Configure	Connect	Create	Delete	Disconnect	Build	Cancel	Configure	Create	Delete	Discover	Read	Workspace	Delete	Replay	Update	Configure	Create	Delete	Read	Tag	Reserve	Unlock	View
Anonymous Users	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Authenticated Users	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Jenkins	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Add user or group...

Authorization: Project-Based Matrix Authorization Strategy

The **Project-based Matrix Authorization Strategy** option is an extension of the Matrix-based security. It allows additional ACL to be configured for every project separately.



Jenkins Roles and Permissions

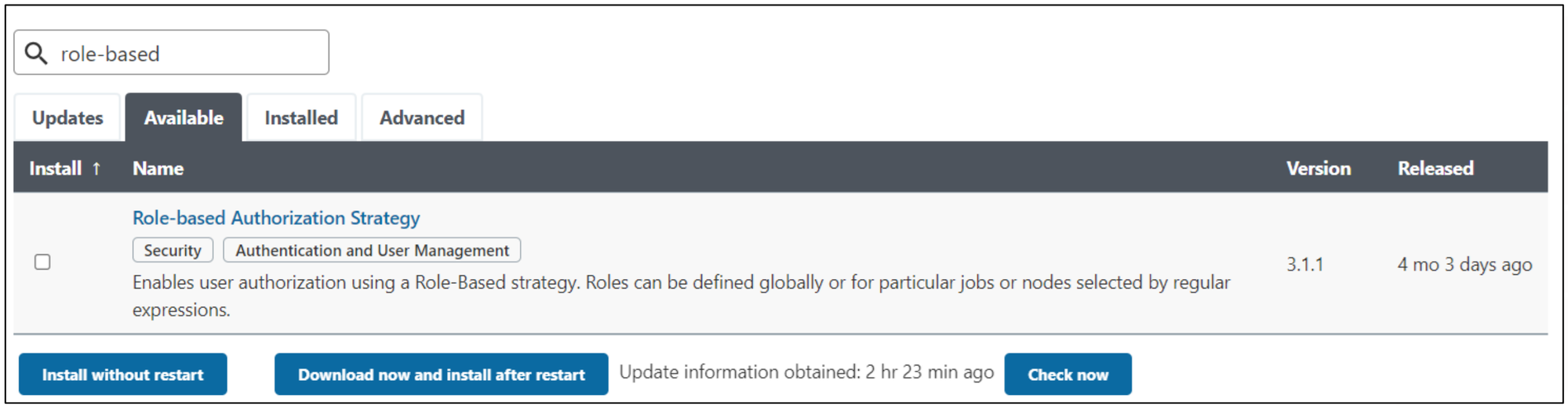
Jenkins uses the **Role-based Authorization Strategy** plugin to implement roles and permissions configurations for Jenkins Authorization.

Role-based Authorization Strategy Plugin

Creates specific roles which can be used to control user permissions	Creates roles such as admin, developer, read only, or anonymous user	Creates and manages project-based roles

Jenkins Roles and Permissions

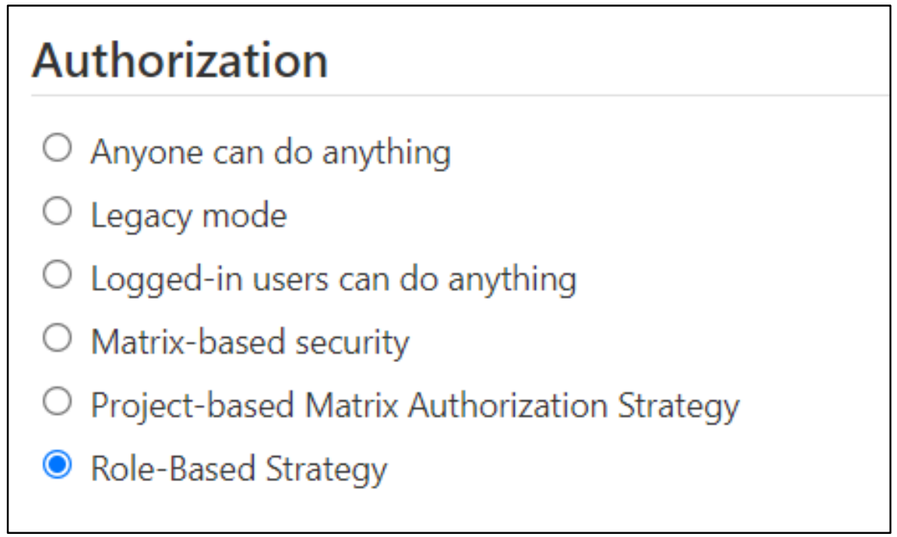
This is a screenshot of the Available tab that displays the Role-based Authorization Strategy plugin, which can be installed by admins.



Jenkins Roles and Permissions

To manage roles, select **Role-Based Strategy** in the Authorization section of Jenkins.

Once the Role-Based Strategy in Authorization is configured, a separate Manage and Assign Roles screen from Manage Jenkins dashboard is displayed.



Jenkins Maintenance

Jenkins Version Upgrade

It is important to keep Jenkins up-to-date with the latest versions to avoid security issues and vulnerabilities.

Production environment

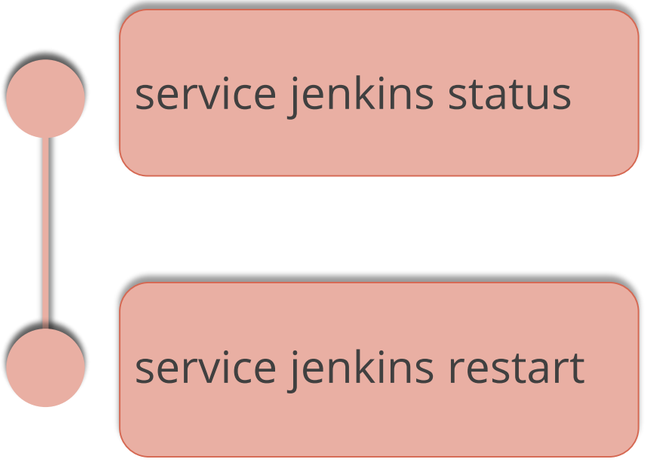
- Use LTS version of Jenkins, which provides stable Jenkins installation

Jenkins installed using apt or yum package manager can be upgraded using apt upgrade Jenkins or yum update Jenkins, based on the OS.

Deploy new LTS version jenkins.war file to /usr/lib/jenkins directory. This can be downloaded using https://www.jenkins.io/download/.

Jenkins Stop and Start Maintenance

Jenkins on Linux OS gets deployed as a Unix service that can be easily bounced using the Linux service command as:

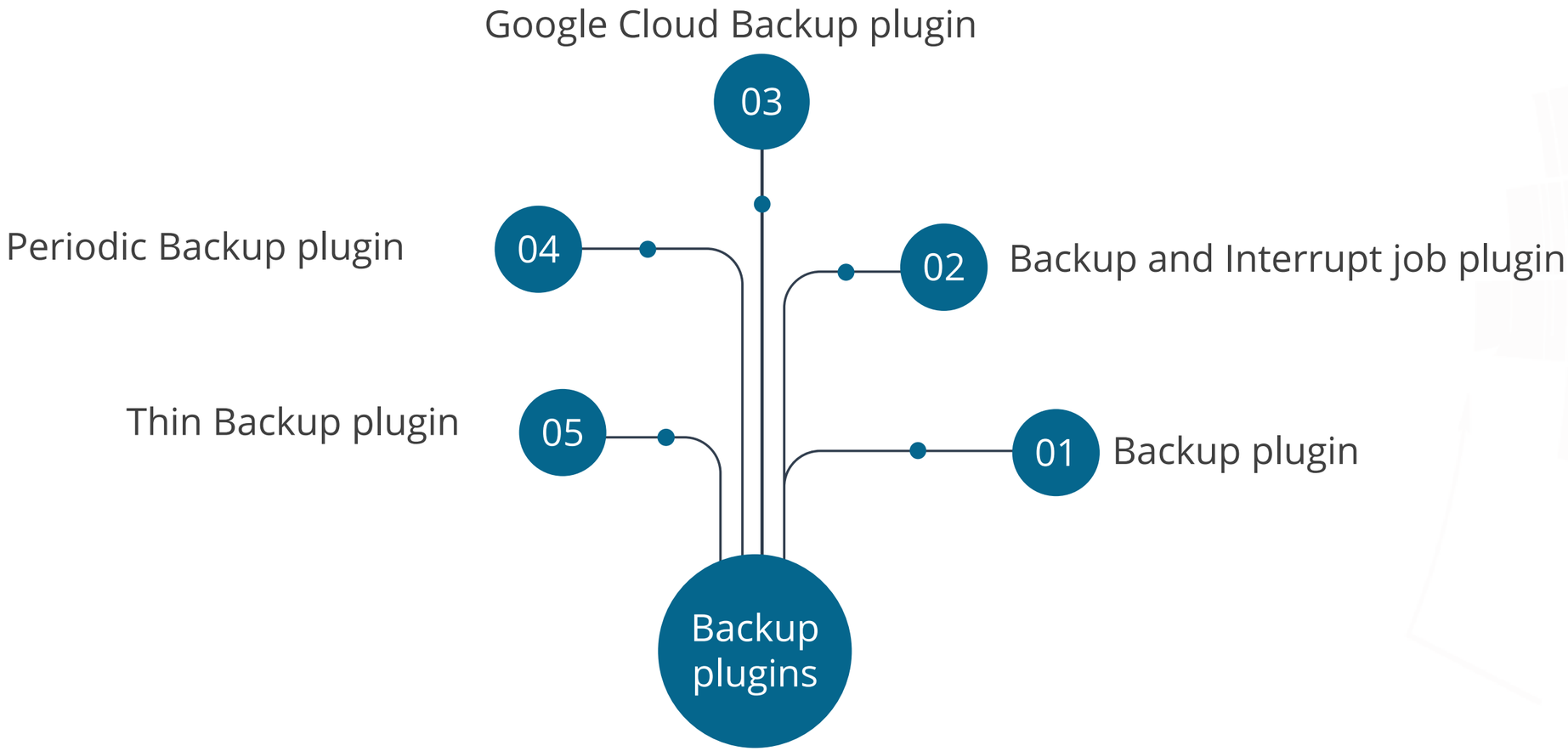


Windows Platform

- If Jenkins is installed on Windows platform, then restart Jenkins from Windows service.
- To access service in Windows, run a program called Services.

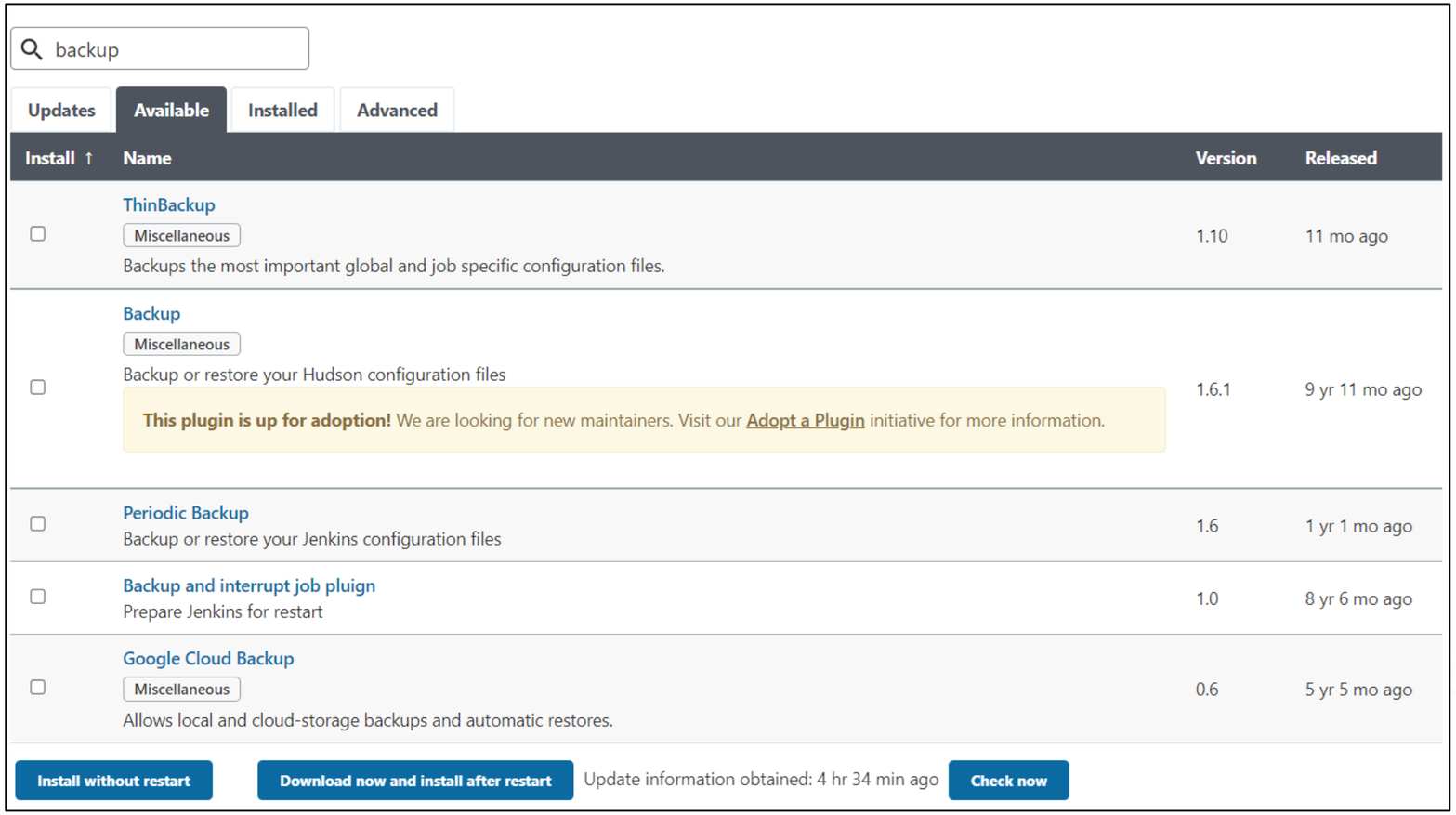
Jenkins Backup and Restore Plugin Integration

While working with Jenkins, it is important to keep a backup of data and configurations so that admins can take a backup of Jenkins configurations before any upgrade or server patching.



Jenkins Backup and Restore Plugin Integration

This is a screenshot of the Available tab that displays the various plugins for data and configuration back up.



Jenkins Backup and Restore Plugin Integration

Shown below are the plugins and their features:

Backup

- Helps admins restore Jenkins home directory
- Customizes backups
- Is a manual trigger
- Does not support scheduling

Backup & Interrupt Job

- Can take a running job backup
- Interrupts a scheduled job
- Schedules the job back once Jenkins is up and running again

Google Cloud Backup

- Supports backup to Google Cloud
- Supports auto restoration

Jenkins Backup and Restore Plugin Integration

Periodic Backup

- Is an extension of the Backup plugin
- Provides an extensive feature of scheduled backup
- Provides more features as compared to Backup plugin

Thin Backup

- Is the most reliable backup and restoration plugin
- Allows both manual and automated backups

Jenkins Build Monitoring

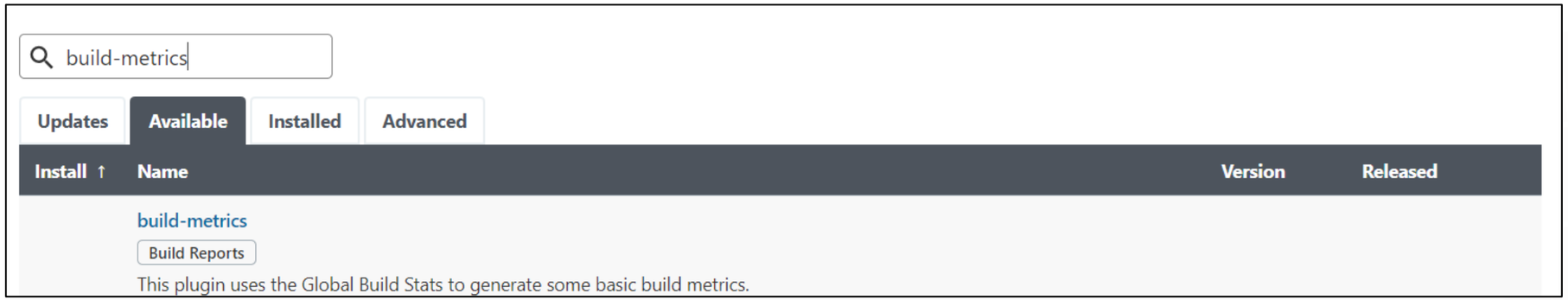
Jenkins provides support to check Build metrics and trends with the help of plugins like Build-metrics plugin.

Jenkins Build Monitoring Plugins

- Gather information within Builds
- Display the information gathered n a graphical format

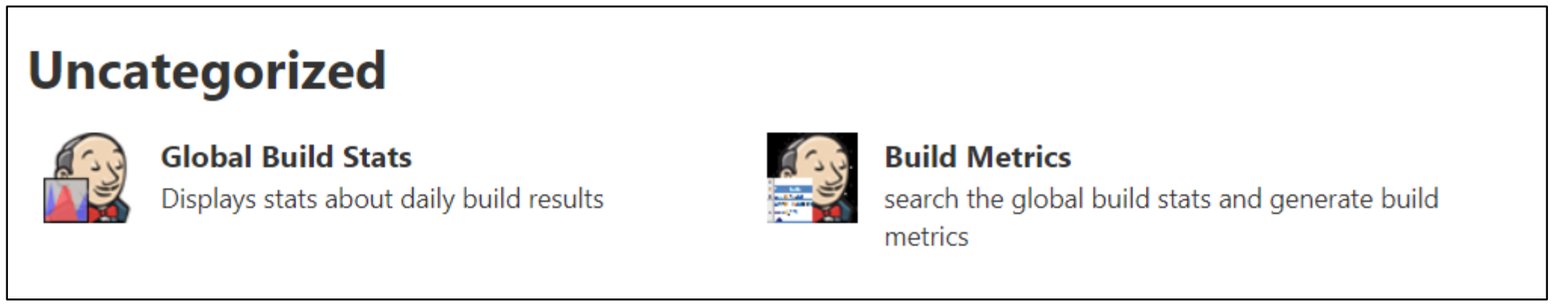
Jenkins Build Monitoring

To install the **build-metrics** plugin, go to **Manage Jenkins** and click **Plugin Management**. Install the plugin listed in the **Available** tab.



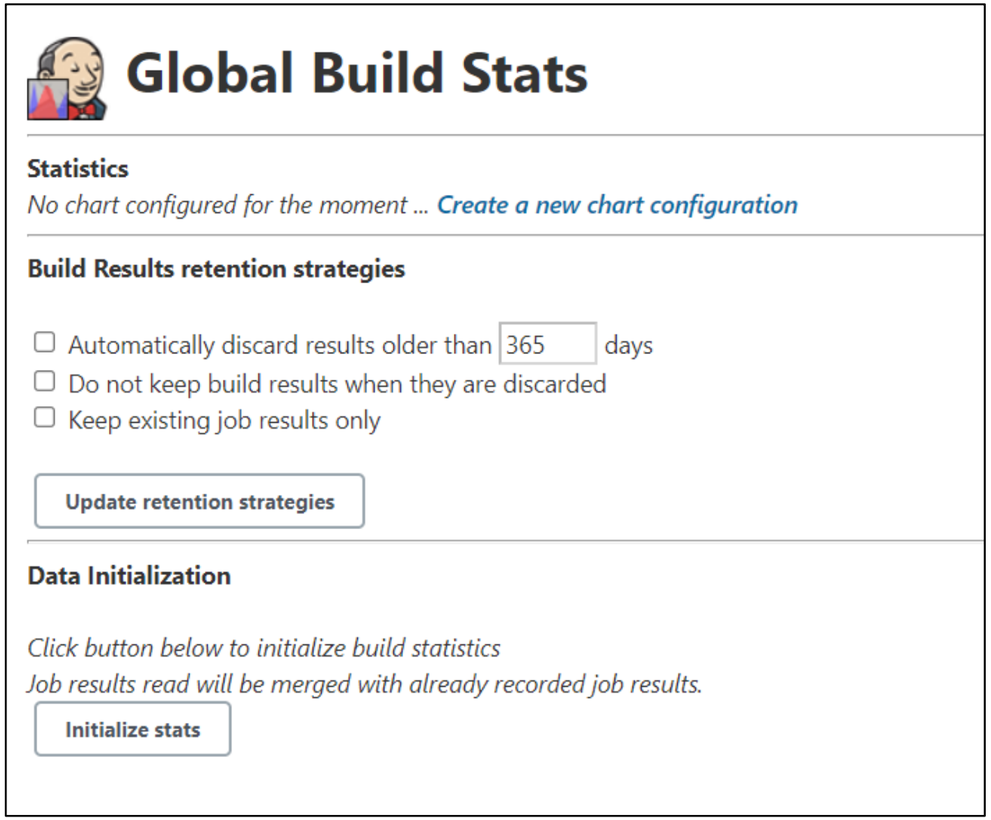
Jenkins Build Monitoring

The **Global Build Stats** option is used to fetch and show Build stats from all jobs executing on Jenkins. This option can be found in **Manage Jenkins**.



Jenkins Build Monitoring

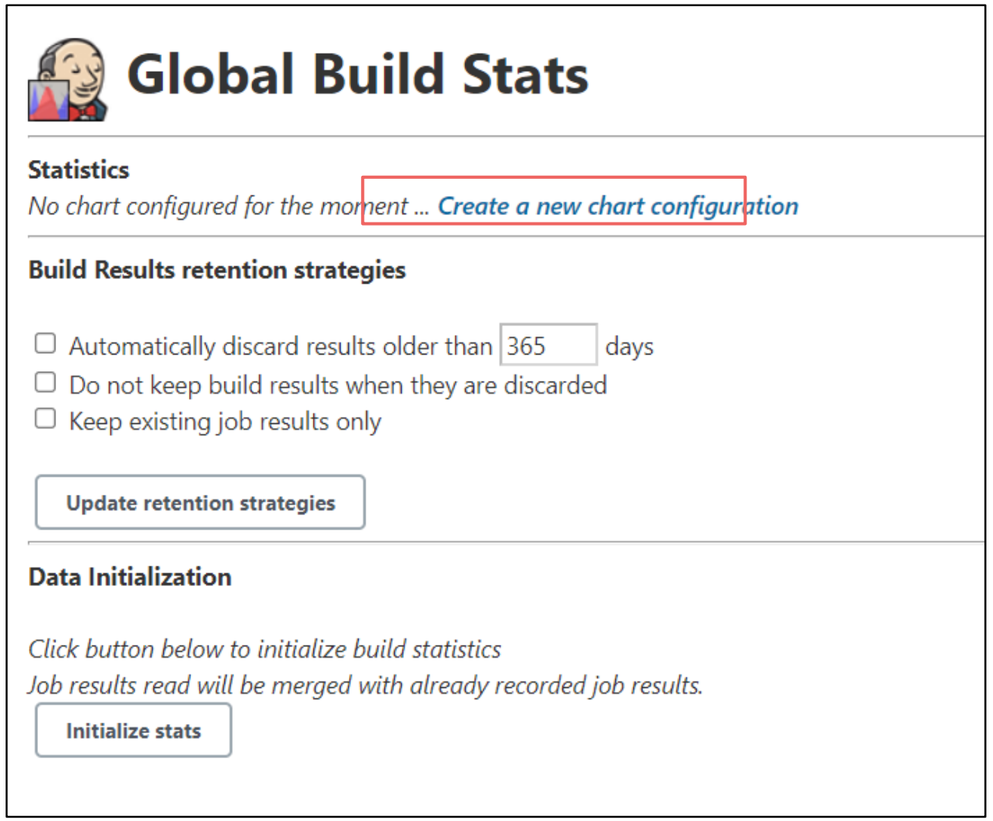
This is a screenshot of the **Global Build Stats** section, which allows the admin to configure Build stats.



- Creates graphical charts
- Initializes data

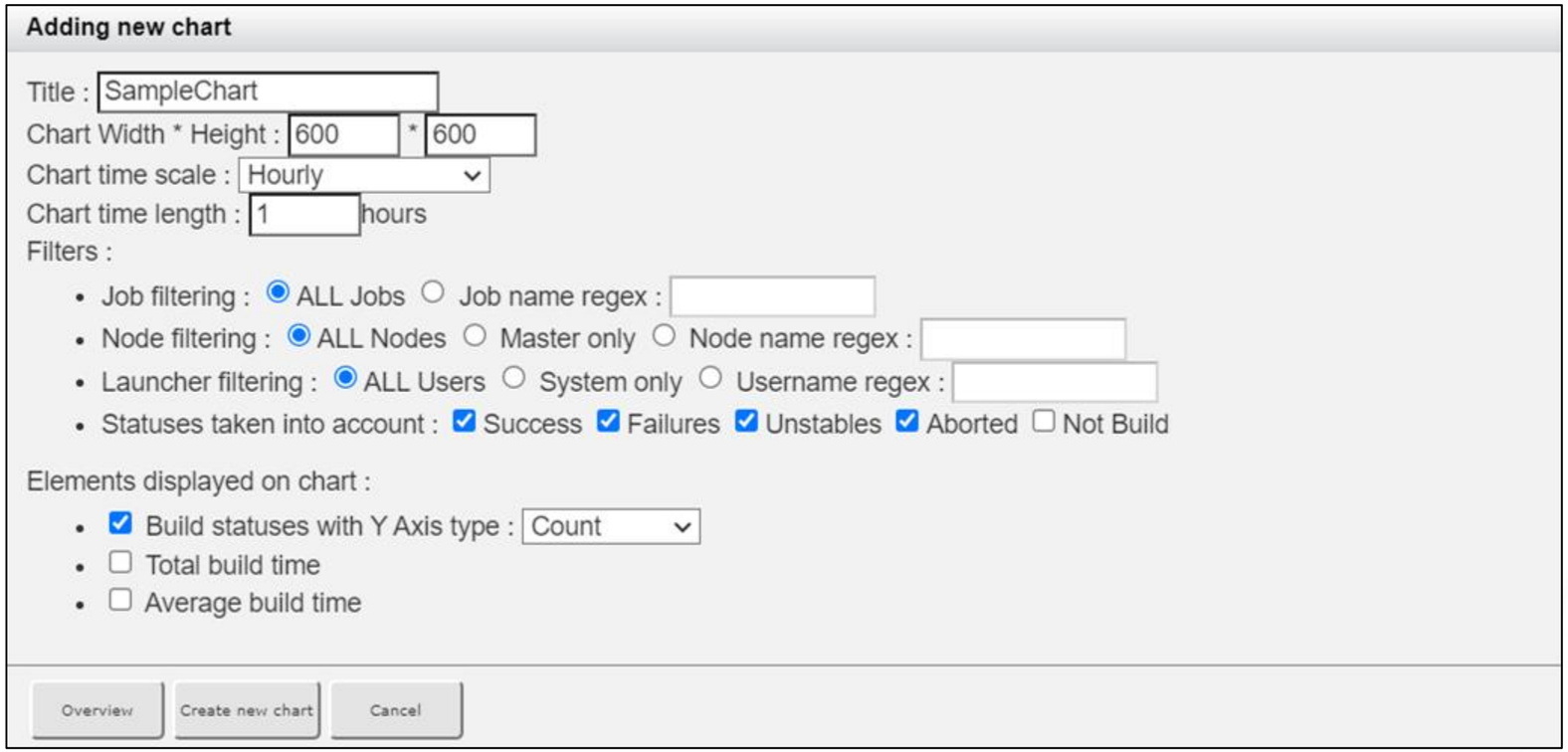
Jenkins Build Monitoring

Once the data has been initialized, admins can create new charts to represent the Build stats graphically. This can be done by clicking the **Create new chart configuration** link in the Global Build Stats screen.



Jenkins Build Monitoring

After clicking **Create new chart configuration**, admins must key in the chart details and click **Create new chart** to create a chart.



Jenkins Disk Usage Monitoring

There is an file system utilization where source code would be checked out and build related files are getting created on file system.

More builds would result in increase in utilization of a file system

Jenkins support disk usage plugin which shows usage trends and disk utilization

Admins can calculate disk usage every 60 minutes

Disk usage and CloudBees Disk Usage plugins support disk usage.

Jenkins Logging

Logging is important for any application from the perspective of troubleshooting. Jenkins supports logging like any Java application.

Jenkins log files are available at:

/var/log/jenkins/jenkins.log in Linux machines

%JENKINS_HOME%/jenkins.out and **%JENKINS_HOME%/jenkins.err** in Windows machines

Assisted Practice

Performing Stop/Start for Jenkins application

Duration: 10 min

Problem Statement:

Demonstrate how a Jenkins application can be started and stopped.

Assisted Practice: Guidelines

Steps to demonstrate how to perform Stop/Start for Jenkins application:

1. Login to Jenkins Master server and then perform bounce activity for Jenkins.

Assisted Practice

Configuring Jenkins backup and restore

Duration: 10 min

Problem Statement:

Configure backup and restore in Jenkins.

Assisted Practice: Guidelines

Steps to demonstrate how to configure backup and restore in Jenkins:

1. Login to Jenkins Master server and then perform bounce activity for Jenkins

Key Takeaways

- Jenkins supports security features and configurations that make existing Jenkins more secure.
- Jenkins Authentication helps to restrict usage of Jenkins to authenticated users only.
- Jenkins installed using apt or yum package manager can be upgraded using apt upgrade Jenkins or yum update Jenkins, depending on the OS.
- Jenkins provides support to check Build metrics and trends with the help of plugins like Build-metrics plugin.
- Global Build Stats option is used to fetch and show Build stats from all jobs executing on Jenkins.

Lesson-End Project

Setup Developer and Admin roles and permissions in Jenkins

Problem Statement:

Perform the following:

- Set up developer and admin roles and permissions.

Access: Click on the **Labs** tab on the left side panel of the LMS. Copy or note the username and password that is generated. Click on the **Launch Lab** button. On the page that appears, enter the username and password in the respective fields, and click **Login**.

Thank You