**Here are the steps to upgrade Jenkins due to vulnerabilities, explained in short with the perspective of a DevOps engineer:**

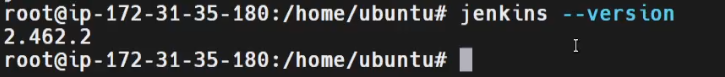
**Summary of Why This Matters (DevOps Perspective):**

* **Vulnerability Management**: Regular updates help mitigate security risks.
* **Minimal Downtime**: Ensuring Jenkins is stopped only during the upgrade prevents errors.
* **Automation Friendly**: This process can be automated using scripts or pipelines for consistency.
* **Backup Ready**: Backing up the old file ensures rollback capability if issues arise with the new version.

This process ensures that Jenkins is **up-to-date** and free from vulnerabilities, maintaining **security and stability** in your CI/CD pipelines.

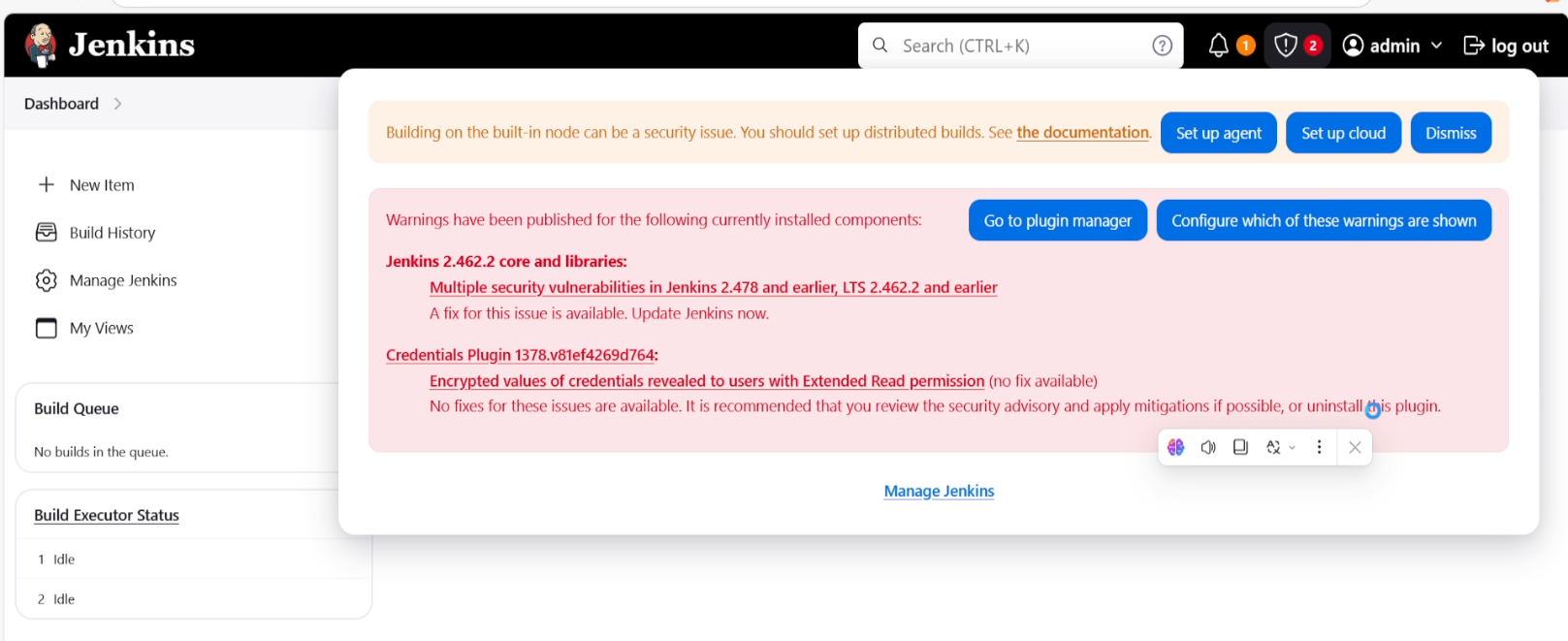
**1. Verify the Existing Jenkins Version**

jenkins –version



* Ensure you know the current version, **2.426.2**.
* This helps verify the upgrade after the process.

**Jenkins Dashboard**



**2. Navigate to the Jenkins WAR File Location**

cd /usr/share/java

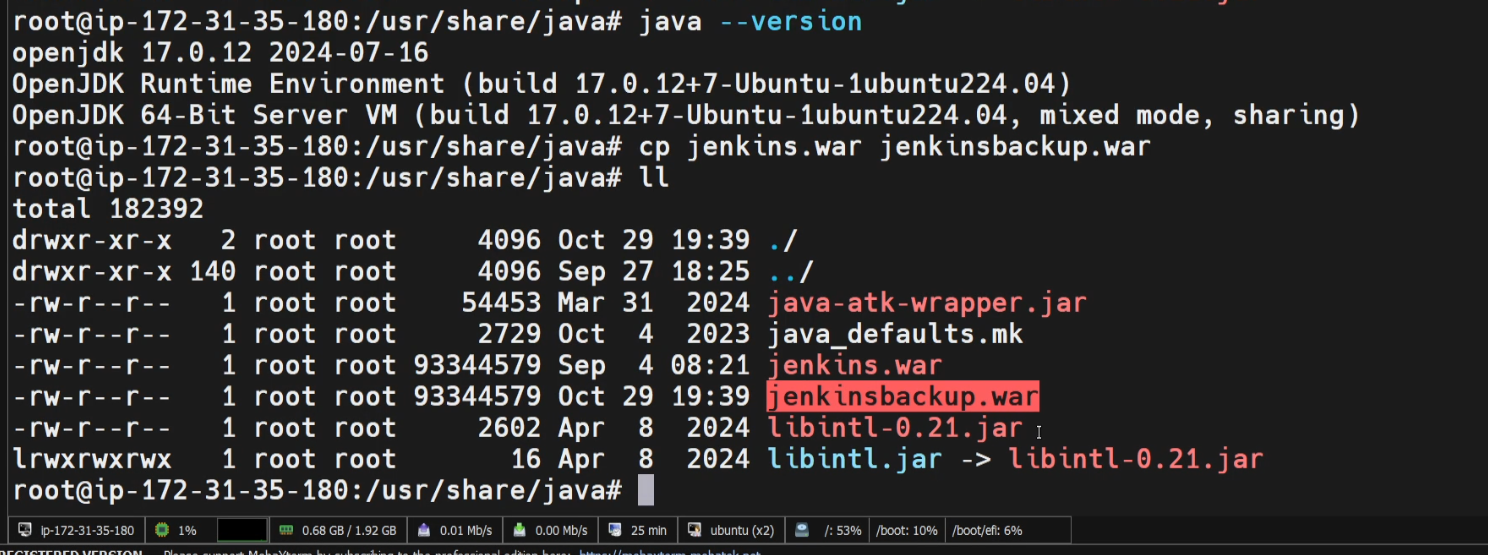


* Jenkins WAR files are usually stored in /usr/share/java.
* This is where you will replace the old WAR file with the latest version.

**3. Backup the Existing Jenkins WAR File**

cp jenkins.war jenkins.war\_backup

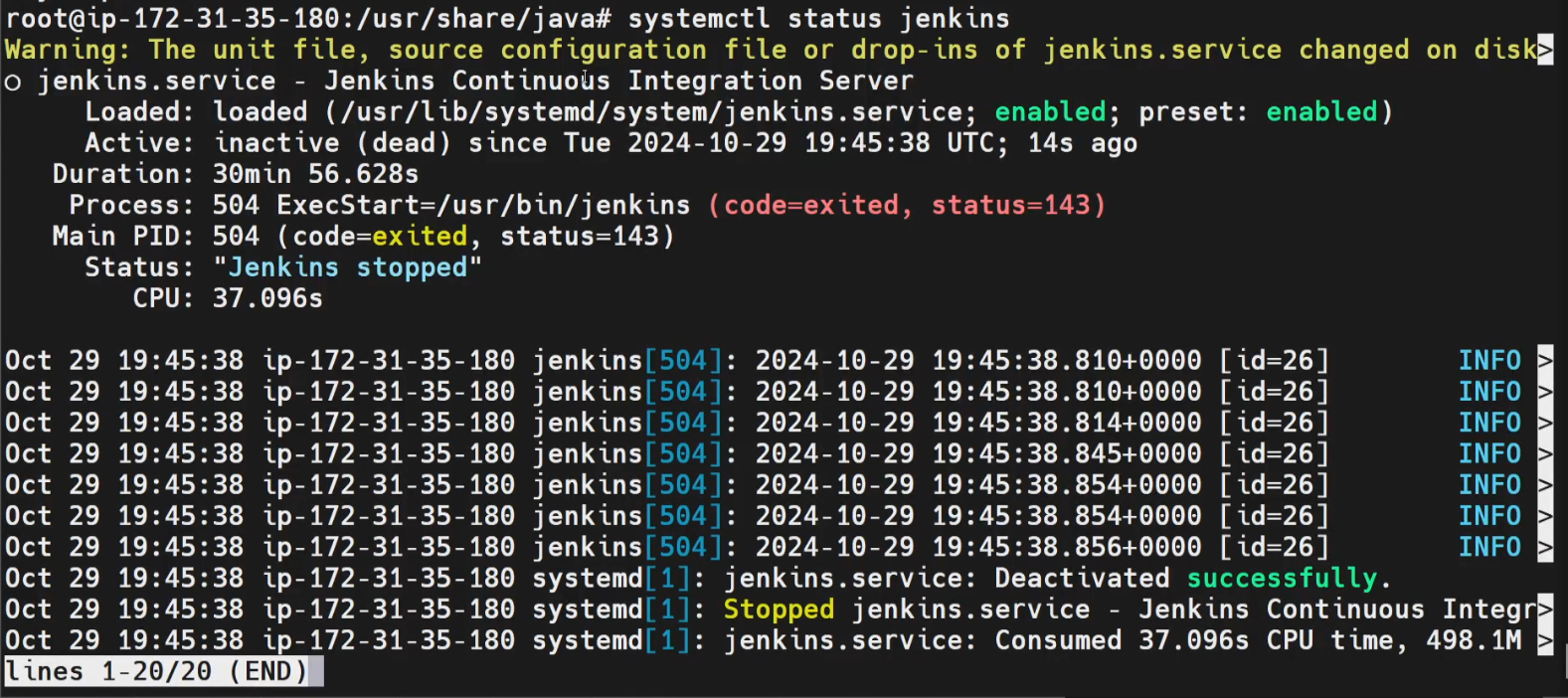
* Always create a backup in case of issues during the update.



**4. Stop the Jenkins Service**

sudo systemctl stop jenkins

* Ensure Jenkins is stopped to prevent conflicts while updating the WAR file.



**5. Remove the Old Jenkins WAR File**

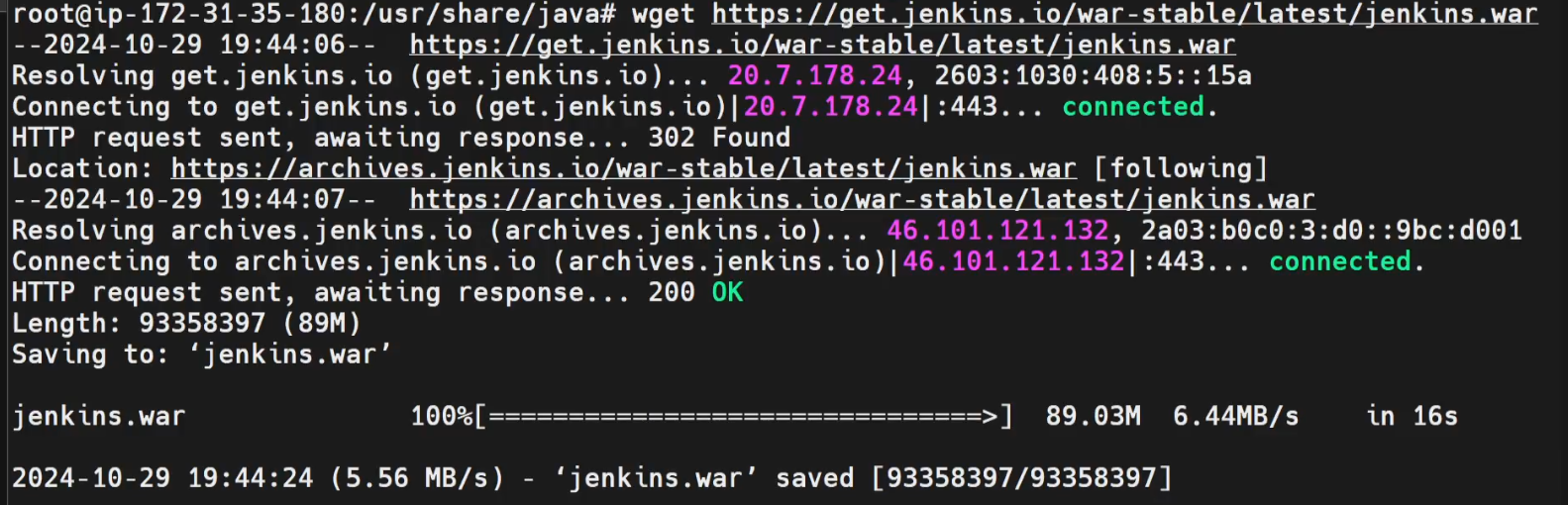
rm jenkins.war

* Delete the outdated version to avoid confusion and vulnerabilities.

**6. Download the Latest Jenkins WAR File**

wget https://get.jenkins.io/war-stable/latest/jenkins.war

* Download the **latest stable version** from Jenkins' official site to patch known vulnerabilities.



**7. Start and Reload Jenkins Service**

sudo systemctl start jenkins

sudo systemctl reload jenkins

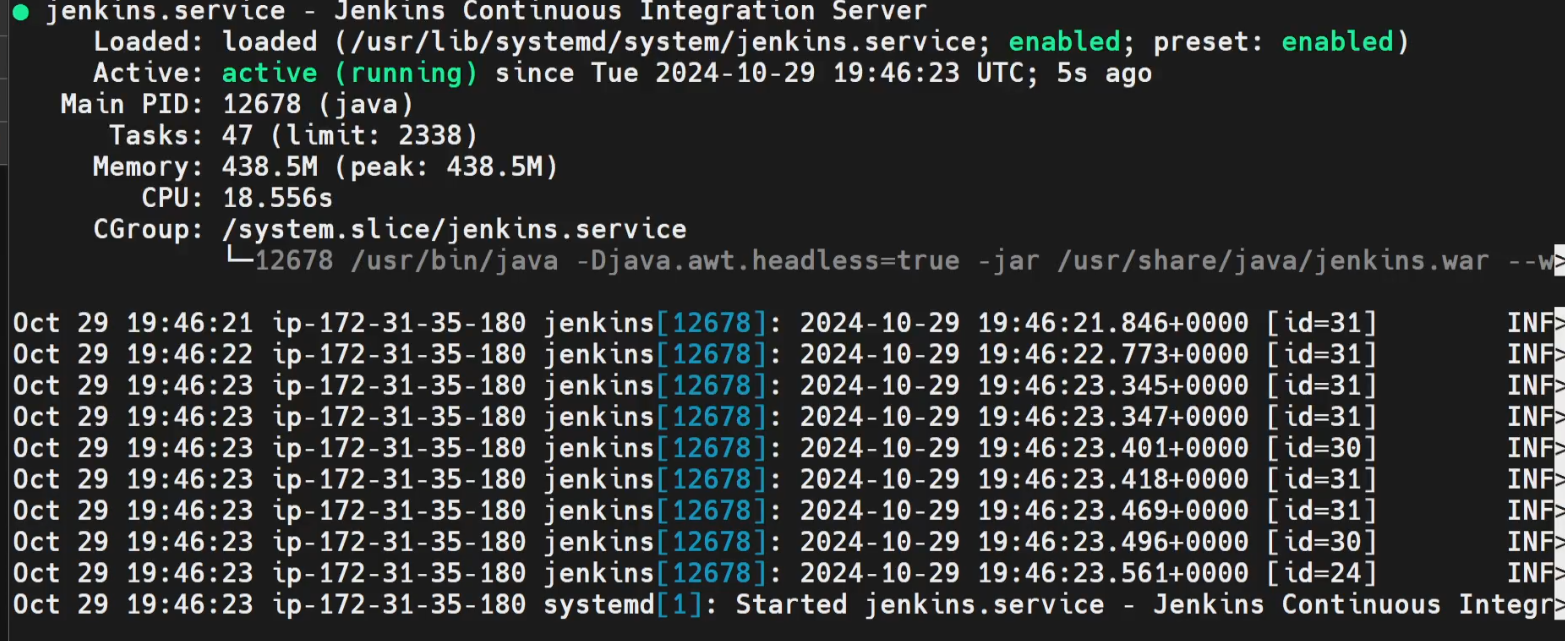
* Start the Jenkins service and reload the configuration to apply updates.

**8. Verify Jenkins Status and Updated Version**

sudo systemctl status jenkins

jenkins --version

* Ensure the service is active and verify the new version, **2.462.3**.

  
  
  
  
Access Jenkins Server on Browser IP:8080  
  
Review the no Vulnerabilities Suggestions .  
  
