Jenkins Recommendations

Jenkins

Ensure Jenkins is not available as public over the internet.

K**eep Jenkins Up to Date**

Access Controls : Implement role-based access control (RBAC) to restrict user permissions. Use the built-in matrix-based security or external authentication providers like LDAP, Active Directory, or OAuth.

User Authentication: Choose strong authentication methods, such as using a username and password combination, or better yet, utilize two-factor authentication (2FA) or single sign-on (SSO) with tools like GitHub or Google.

Plugin Security: Review and regularly update the plugins used in Jenkins.

Secure Jenkins Configuration: Apply the principle of least privilege when configuring Jenkins.

Secure Jenkins Secrets: Store sensitive information like passwords, API keys, and certificates using the built-in Jenkins Credential Plugin or a secure secret management tool.

Securing Jenkins Server: Firewall and Network Segmentation , Secure the Operating System, Secure Communication:

Jenkins

Audit and Monitoring: Enable Jenkins logs and monitor them for any suspicious activities or errors

Implement Automated Security Testing

Educate Users: Provide training and awareness programs for Jenkins users, emphasizing security best practices, such as avoiding insecure plugin installations, writing secure pipeline scripts, and handling sensitive information properly.

Regular Backups: Regularly back up your Jenkins configuration, job configurations, and plugin configurations. Store backups securely and test restoration procedures periodically.

SSHD hardened: Disable SSHD server(Ensure underlying server is hardened as per CIS benchmark)

Jenkins

Ensure headers are set Properly wherever its hosted from like tomcat app server, load balancer, Reverse proxy, Jenkins plugin or Jenkins Script console

Strict-Transport-Security (HSTS) : header instructs browsers to always use HTTPS, even if a user types in HTTP.

Content-Security-Policy (CSP): Implement a Content Security Policy to restrict the types of content that can be loaded on your Jenkins server.

X-Content-Type-Options: header to prevent MIME-type sniffing. This header helps protect against content-type confusion attacks

X-Frame-Options: header to prevent clickjacking attacks by ensuring your Jenkins server is not embedded within an iframe on other websites

Referrer-Policy: header to control how much information is included in the Referer header when a user navigates to external websites. X-XSS-Protection: Enable the X-XSS-Protection header to enable the built-in XSS protection offered by modern browsers

Access Control & various other measures.

Manage Roles

Jenkins

Global roles

Role	Overall		Credentials					Agent							Job									Run			View				Job Config History	SCM	Metrics			Job Import
	Administer	Read	Create	Delete	ManageDomains	Update	View	Build	Configure	Connect	Create	Delete	Disconnect	Provision	Build	Cancel	Configure	Create	Delete	Discover	Move	Read	Workspace	Delete	Replay	Update	Configure	Create	Delete	Read	DeleteEntry	Tag	HealthCheck	ThreadDump	View	JobImport
admin	✓																																		
developer		✓																																	
qa		✓																																	

Role to add

ScriptApproval

Approve / Deny System Commands script from admin :

Approve / Deny Groovy script from admin :

You can also remove all previous script approvals: Clear Approvals

No pending signature approvals.