



Jenkins

Running Freestyle Project

JENKINS

BY ALOK SRIVASTAVA - NETWORK NUTS



PRODUCTION READY

Production servers are usually client facing, or in simpler words, web pages that end users actively interact with. Normally, in order to affect a proper production environment, changes need to go through a few more environments for testing and quality assurance.

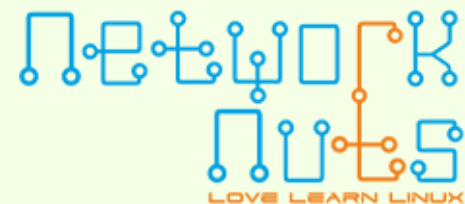


The pages facebook.com or twitter.com are both production sites.
Why is this?

Because these are pages that users open to interact with their products.

Their staging environments could be, for example, staging.facebook.com or staging.twitter.com.

End users won't have access to these, because this is where final changes are tested before they appear on the production sites, for example, new user interface features.



A few best practices mentioned on the Jenkins wiki for production environments include the following:

- Security
- Access limited to the master node
- Backup of Jenkins Home
- Project naming conventions should be followed
- Getting rid of jobs and resources that are not in use

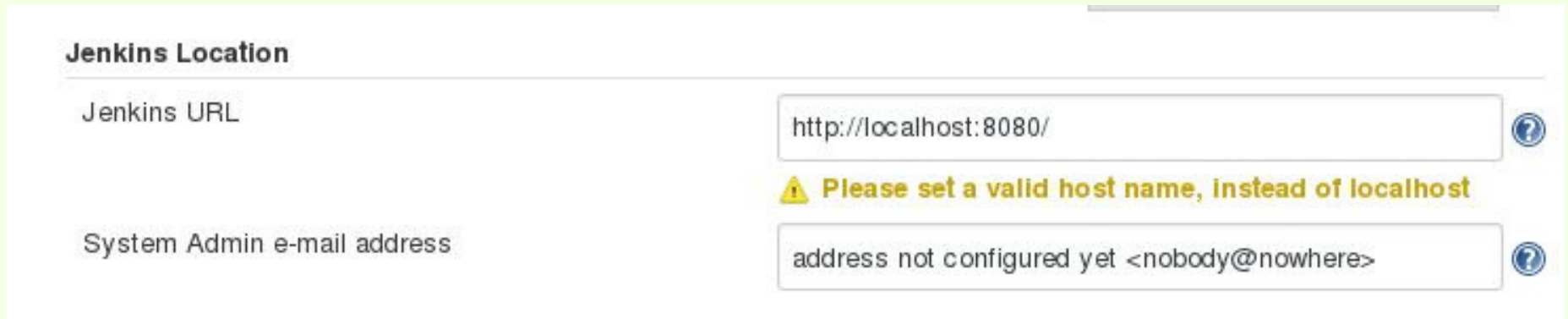
Checking our Jenkins Server

Some of the implications would include the following:

- Vulnerability to hackers
- Data loss
- Attacks such as man-in-the-middle attacks, where traffic is stolen through the imitation and replication of servers

Checking Security of our Jenkins Server - https

Under - Manage Jenkins -> Configure System



Jenkins Location

Jenkins URL

System Admin e-mail address

Please set a valid host name, instead of localhost

We would also need to get SSL certificates and a domain name. Above all that, we can also enforce our server in a VPC, where only people with access to the network can actually get to the Jenkins server. SSL Certificates activate a secure protocol to the server and allow secure connections.

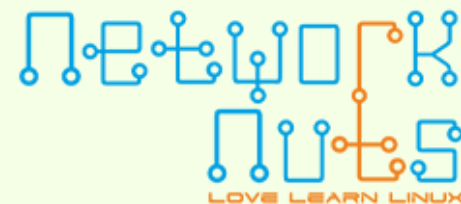
Checking Security of our Jenkins Server - access point

Access points are methods, channels, or ways users can open or access a specific service. These points are vital to what service is offered and can have implications if not properly managed.

Currently, Jenkins can be accessed either through the UI or through Docker, by SSH.

In a production environment, connections would be strictly limited to a specific port number and user interface.

Manage Jenkins -> Configure Global Security



SSH Server

SSHD Port

☐ Fixed :

☐ Random

☒ Disable

Save

Apply


In a production environment, we would have a default of 22 or any of your choice, depending on usage. Always be sure to limit the number of ports open.

Checking Security of our Jenkins Server - remember me

Manage Jenkins -> Configure Global Security



The image shows the 'Configure Global Security' page in Jenkins. At the top, there is a yellow padlock icon followed by the title 'Configure Global Security'. Below the title, there are three settings: 'Enable security' which is checked with a checkbox, 'Disable remember me' which is unchecked with a checkbox, and 'Access Control' which is a link. To the right of 'Access Control' is the 'Security Realm' section, which contains a radio button labeled 'Delegate to servlet container'.

 **Configure Global Security**

☒ Enable security

Disable remember me ☐

Access Control

Security Realm

☐ Delegate to servlet container