**Installing Fail2ban on Fedora Server to Secure SSH**

**Fail2ban** is a powerful intrusion prevention tool that monitors log files and bans IPs that show malicious signs — like too many failed SSH login attempts. It’s especially useful on public-facing Fedora servers to protect your SSH service from brute-force attacks.

In this article, we’ll walk you through installing and configuring **Fail2ban** on a **Fedora Server** to secure SSH access.

What You'll Learn

* How Fail2ban works
* Installing Fail2ban on Fedora
* Configuring Fail2ban for SSH protection
* Testing and verifying the setup

Step 1: Install Fail2ban

Use DNF to install Fail2ban:

1. sudo dnf install fail2ban -y

Once installed, enable and start the service:

1. sudo systemctl enable fail2ban
2. sudo systemctl start fail2ban

Check its status:

1. sudo systemctl status fail2ban

Step 2: Basic Configuration

Fail2ban uses jail.conf as a template. We will create a custom override file to avoid modifying the default.

1. sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Now open the file:

1. sudo nano /etc/fail2ban/jail.local

Scroll to the **[sshd]** section and update it like so:

1. [sshd]
2. enabled = true
3. port = ssh
4. logpath = %(sshd\_log)s
5. maxretry = 5
6. bantime = 1h
7. findtime = 10m

* enabled = true — Activates this jail
* maxretry = 5 — After 5 failed attempts
* bantime = 1h — Ban lasts for 1 hour
* findtime = 10m — Looks at failed attempts within the last 10 minutes

Step 3: Configure Firewalld (Optional but Recommended)

If you're using **firewalld**, make sure SSH is allowed and the Fail2ban service can ban IPs:

1. sudo firewall-cmd --add-service=ssh --permanent
2. sudo firewall-cmd --reload

Fail2ban will use firewall-cmd for banning by default if firewalld is detected.

Step 4: Restart Fail2ban and Check

Restart the service to apply changes:

1. sudo systemctl restart fail2ban

Check active jails:

1. sudo fail2ban-client status

Check SSH jail status:

1. sudo fail2ban-client status sshd

Step 5: Test Fail2ban

You can simulate failed logins from another machine using:

1. ssh wronguser@your-fedora-ip

After multiple failed attempts, your IP should be banned.

To unban an IP manually:

1. sudo fail2ban-client set sshd unbanip YOUR.IP.ADDRESS.HERE

Summary

You’ve now added an important security layer to your Fedora server. Fail2ban is lightweight, easy to configure, and highly effective against brute-force SSH attacks.