如何在 Ubuntu 22.04 上安装和配置 Fail2ban

在此页

Fail2ban 是免费的开源 IPS（入侵防御软件），可帮助管理员保护 Linux 服务器免受恶意登录和暴力攻击。 Fail2ban 是用 Python 编写的，带有针对 Apache2、SSH、FTP 等各种服务的过滤器。Fail2ban 通过阻止源攻击的 IP 地址来减少恶意登录尝试。

Fail2ban 的工作原理是扫描服务的日志文件 (e.f /var/log/auth.log) 并禁止显示恶意登录尝试的 IP 地址，例如太多不正确的密码、寻求漏洞利用等。Fail2ban 还支持多个防火墙后端，例如 iptables、 ufw 和 firewalld。还允许您为每次被阻止的登录尝试设置电子邮件通知。

在本教程中，我们将向您展示如何安装和配置 Fail2ban 以保护 Ubuntu 22.04 服务器。本指南还涵盖了用于管理 Fail2ban 服务和监狱的 fail2ban-client 的基本命令。

先决条件

- Ubuntu 服务器 22.04
- 具有 sudo 权限的非根用户。

设置 UFW 防火墙

在开始安装 Fail2ban 之前，您需要在 Ubuntu 服务器上设置防火墙。

默认的 Ubuntu 服务器安装带有 UFW 防火墙，它比其他防火墙（如 iptables）更易于管理。

现在使用以下命令检查 UFW 防火墙状态。

```
sudo ufw status
```

如果您收到诸如 \Status: inactive\ 之类的输出消息，则您的 UFW 防火墙尚未启动。但是，如果您收到诸如 \Command ufw not found\ 之类的输出消息，则表明您的服务器上未安装 UFW 防火墙。

要安装 UFW 防火墙包，请运行下面的 apt 命令。

```
sudo apt install ufw -y
```

UFW 安装完成后，运行以下命令将 SSH 服务添加到 UFW 防火墙。

```
sudo ufw allow ssh
```

接下来，运行以下命令启动并启用 UFW 防火墙。

```
sudo ufw enable
```

输入 y 确认并启动 UFW 防火墙。

最后，使用以下命令再次检查 UFW 防火墙。

```
sudo ufw status
```

您可以在下方看到 UFW 防火墙“*状态：活动*”，防火墙规则中添加了 SSH 端口 22。

```
root@server-ubuntu:~#
root@server-ubuntu:~# sudo ufw allow ssh
Rules updated
Rules updated (v6)
root@server-ubuntu:~# sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@server-ubuntu:~#
root@server-ubuntu:~# sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)

root@server-ubuntu:~#
root@server-ubuntu:~#
```

在 Ubuntu 22.04 上安装 Fail2ban

安装和配置 UFW 防火墙后，现在您将在服务器上安装 Fail2ban 包。

运行以下命令来更新和刷新您的 Ubuntu 存储库。

```
sudo apt update
```

现在使用以下命令安装 Fail2ban 包。

```
sudo apt install fail2ban -y
```

安装将开始。

```
root@server-ubuntu:~#
root@server-ubuntu:~# sudo apt install fail2ban -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 58 not upgraded.
Need to get 473 kB of archives.
After this operation, 2,486 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 fail2ban all 0.11.2-6 [394 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/main amd64 python3-pyinotify all 0.9.6-1.3 [24.8 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy/main amd64 whois amd64 5.5.13 [53.4 kB]
```

Fail2ban 安装完成后，启用 Fail2ban 服务并使用以下命令启动该服务。

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

最后，使用以下命令检查 Fail2ban 服务状态。

```
sudo systemctl status fail2ban
```

在下面的屏幕截图中，您将看到 Fail2ban 服务正在 Ubuntu 22.04 服务器上运行。

```
root@server-ubuntu:~#
root@server-ubuntu:~# sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.servic
root@server-ubuntu:~#
root@server-ubuntu:~# sudo systemctl start fail2ban
root@server-ubuntu:~#
root@server-ubuntu:~# sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
     Active: active (running) since Thu 2022-05-19 01:41:12 UTC; 5s ago
       Docs: man:fail2ban(1)
   Main PID: 3284 (fail2ban-server)
      Tasks: 5 (limit: 2242)
     Memory: 26.9M
     CGroup: /system.slice/fail2ban.service
             └─3284 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

配置 Fail2ban

安装 Fail2ban 后，现在是设置和配置 Fail2ban 的时候了。

所有 Fail2ban 配置都存储在 /etc/fail2ban 目录中。下面详细的Fail2ban配置你必须要知道：

- 配置fail2ban.conf是Fail2ban的主要配置。
- 配置jail.conf 是Fail2ban 监狱配置的一个例子。
- *action.d* 目录包含 fail2ban 操作设置，例如邮件设置和防火墙设置。
- 目录 *jail.d* 包含 fail2ban jail 的额外配置。

要开始配置 Fail2ban，您需要使用以下命令将默认监狱配置 *jail.conf* 复制到 *jail.local*。

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

现在使用 *nano* 编辑器编辑配置 *jail.local*。

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

首先，取消注释 ignoreip 选项并添加您的 IP 地址。 *ignoreip* 选项内的所有 IP 地址都不会被 Fail2ban 阻止。

```
ignoreip = 127.0.0.1/8 ::1 192.168.1.0/24 192.168.10.20
```

对于禁止设置，您可以根据需要更改配置。在这个例子中，global bantime 为 1day，findtime 为 10minutes，maxretry 为 5 次。

bantime选项是IP地址将被禁止访问服务器的时间。 findtime 选项是禁止操作之前失败次数之间的持续时间。而 maxretry 选项是 IP 地址被禁止的失败次数。

```
bantime  = 1d
findtime  = 10m
maxretry = 5
```

Fail2ban 的默认操作只是禁止 IP 地址。但您也可以在 IP 地址被禁止时设置邮件通知。

如下更改操作选项并更改默认发件人和目标邮件地址。

```
action = %(action_mw)s
destemail =
```

接下来，对于 UFW 防火墙集成，您需要将 *banaction* 选项更改为 ufw，如下所示。

```
banaction = ufw
```

最后，对于监狱配置。此部分是您添加服务并使用 fail2ban 保护它的地方。

在此示例中，我们将为 SSH 服务启用监狱，但我们也会覆盖 sshd 监狱的全局默认配置。 bantime 将是 1 周，最大失败重试次数为 3 次，查找时间为 10 分钟。

```
[sshd]
enabled   = true
maxretry  = 3
findtime  = 1d
bantime   = 1w

port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s
```

完成后保存并关闭文件。

现在运行以下命令重新启动 Fail2ban 服务并将新更改应用于 jail.local 配置。

```
sudo systemctl restart fail2ban
```

您现在已经完成了 Fail2ban 配置，启用了电子邮件通知并启用了 sshd 监狱以保护 SSH 服务。

使用 Fail2ban-client 验证 Fail2ban 状态

fail2ban 提供了一个命令行 fail2ban-client 用于与 Fail2ban 服务进行交互。这允许您从命令行管理和配置 Fail2ban，还允许您管理 Fail2ban 监狱。

要验证 fail2ban 安装和配置，请运行以下命令的 *fail2ban-client*。

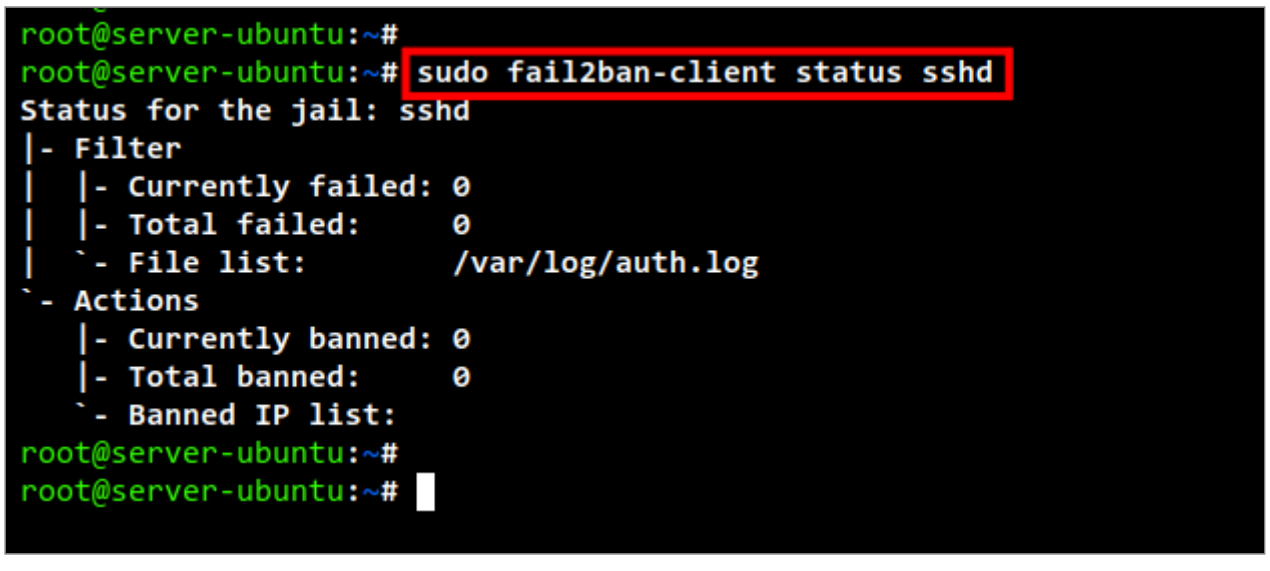
```
sudo fail2ban-client ping
```

如果您收到诸如“服务器回复：pong”之类的输出消息，这意味着 Fail2ban 正在正常运行。

接下来，运行下面的 *fail2ban-client* 命令来检查 sshd jail 的状态。

```
sudo fail2ban-client status sshd
```

下面你可以看到 sshd jail 的详细状态。这包括 SSH 服务的日志文件和 sshd jail 上被禁止的 IP 地址列表。



现在如果你想获得 sshd 监狱的详细配置，你可以使用 fail2ban-client 命令如下。

检查 sshd jail 的 bantime 配置。您将在几秒钟内获得 bantime 的输出。

```
sudo fail2ban-client get sshd bantime
```

检查 sshd jail 的 maxrtey 配置。你会看到这里的 maxretry 是 3，因为它被全局配置覆盖了，也就是 maxrety 5 次。

```
sudo fail2ban-client get sshd maxretry
```

对于sshd jail中的banaction，可以使用以下命令。并且您应该将 ufw 的输出作为 sshd jail 的默认禁令。

```
sudo fail2ban-client get sshd actions
```

对于此处的查找时间，您还将看到 sshd 监狱的覆盖值。此处的输出也将采用秒格式。

```
sudo fail2ban-client get sshd findtime
```

最后，您还可以使用以下命令检查 sshd jail 的默认 ignoreip。你会看到 ignoreip 与全局 Fail2ban 配置具有相同的值。

```
sudo fail2ban-client get sshd ignoreip
```

```
root@server-ubuntu:~#
root@server-ubuntu:~# sudo fail2ban-client get sshd bantime
604800
root@server-ubuntu:~# sudo fail2ban-client get sshd maxretry
3
root@server-ubuntu:~# sudo fail2ban-client get sshd actions
The jail sshd has the following actions:
ufw
root@server-ubuntu:~# sudo fail2ban-client get sshd findtime
86400
root@server-ubuntu:~# sudo fail2ban-client get sshd ignoreip
These IP addresses/networks are ignored:
|- 127.0.0.0/8
|- 192.168.1.0/24
|- 192.168.10.20
`- ::1
root@server-ubuntu:~#
```

使用 Fail2ban-client 禁止和取消禁止 IP

关于 Fail2ban 的另一个重要事项是如何在 Fail2ban 上禁止和取消禁止 IP 地址。为此，您还可以使用 fail2ban-client 命令。

要在 sshd jail 上手动禁止 IP 地址，您可以使用下面的 fail2ban-client 命令。将 IP 地址更改为您要禁止的 IP 地址。

```
sudo fail2ban-client set sshd banip IP-ADDRESS
```

要从 sshd jail 中解禁 IP 地址，您可以使用下面的 fail2ban-client 命令。请务必将 IP 地址更改为您要取消禁止的 IP 地址。

```
sudo fail2ban-client set sshd unbanip IP-ADDRESS
```

现在，在您手动禁止 IP 地址或取消禁止 IP 地址后，您可以使用下面的 fail2ban-client 命令进行验证。

```
sudo fail2ban-client status sshd
```

如果您手动禁止某个 IP 地址，请确保该 IP 地址在禁止 IP 地址列表中可用。但是，如果您取消禁止某个 IP 地址，请确保该 IP 地址从禁止 IP 地址列表中消失。

结论

恭喜！您现在已成功安装和配置 Fail2ban 以保护 Ubuntu 22.04。您还学习了如何启用 UFW 防火墙，以及如何将 Fail2ban 与 UFW 防火墙集成。最后，您还学习了如何使用 fail2ban-client 命令管理 Fail2ban，其中包括如何从 Fail2ban 中禁止和取消禁止 IP 地址。