


Prashant Lakhera

Follow

May 6, 2019 · 2 min read ·  Listen

100 Days of DevOps — Day 85- Shell Script to find the failed login

To view the updated DevOps course(101DaysofDevOps)

Course Registration link: <https://www.101daysofdevops.com/register/>

Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>

YouTube link: <https://www.youtube.com/user/laprashant/videos>

Welcome to Day 85 of 100 Days of DevOps, Focus for today is Shell Script to find the failed login

Once again this is one of the common tasks we used to encounter as a part of our daily job as SysAdmin/DevOps.

First Approach

- Check if there is a builtin utility/command already available

```
last - show listing of last logged in users
```

- It shows a listing of last logged in users

```
# last
root      pts/0      192.168.0.2    Fri Apr 13 17:18    still logged in
root      pts/1      192.168.0.2    Fri Apr 13 10:11 - 12:32
root      pts/0      192.168.0.2    Fri Apr 13 10:08 - 12:29
root      tty1              Fri Apr 13 10:08    still logged in
reboot    system boot  3.10.0-693.el7.x Fri Apr 13 10:08 - 17:27
(07:19)
```

- As per last man page

```
Last searches back through the file /var/log/wtmp (or the file designated by the -f flag) and displays a list of all users logged in (and out) since that file was created.
```

- So this doesn't solve my purpose, so what else I can do

```
lastb is the same as last, except that by default it shows a log of the file /var/log/btmp, which contains all the bad login attempts.
```

- YAY this is the command I was looking for

```
# lastb
root      ssh:notty    192.168.0.2    Fri Apr 13 17:25 - 17:25
root      ssh:notty    192.168.0.2    Fri Apr 13 17:25 - 17:25
plakhera  ssh:notty    192.168.0.2    Fri Apr 6 18:45 - 18:45
(00:00)
```

- We can also check inside /var/log/secure for any failed attempt

```
# grep -i failed /var/log/secure

Apr 13 17:25:28 docker unix_chkpwd[2247]: password check failed for user (root)

Apr 13 17:25:30 docker sshd[2245]: Failed password for root from 192.168.0.2 port 54837 ssh2

Apr 13 17:25:51 docker unix_chkpwd[2249]: password check failed for user (root)

Apr 13 17:25:53 docker sshd[2245]: Failed password for root from 192.168.0.2 port 54837 ssh2
```

- Let's put together everything in a simple shell script

```
#!/bin/bash
LOGFILE=/var/log/secure
SEARCHSTRING="Failed password for"
grep "$SEARCHSTRING" "$LOGFILE"
```

- Make it executable

```
# chmod +x failedlogin.sh
```

- Execute it

```
./failedlogin.sh

Apr 13 17:25:30 docker sshd[2245]: Failed password for root from 192.168.0.2 port 54837 ssh2

Apr 13 17:25:53 docker sshd[2245]: Failed password for root from 192.168.0.2 port 54837 ssh2
```

- But we can do much better than this based on USER

```
#!/bin/bash
LOG=/var/log/secure
if [ -n "$1" ]
then
NEWUSER="$1"
else
NEWUSER="root"
fi
MESSAGE="Failed password for $NEWUSER"
grep -i "$MESSAGE" "$LOG"
```

Looking forward from you guys to join this journey and spend a minimum an hour every day for the next 100 days on DevOps work and post your progress using any of the below medium.

- Twitter: [@100daysofdevops](https://twitter.com/100daysofdevops) OR [@lakhera2015](https://twitter.com/lakhera2015)
- Facebook: <https://www.facebook.com/groups/795382630808645/>
- Medium: <https://medium.com/@devopslearning>
- Slack: <https://devops-myworld.slack.com/messages/CF41EFG49/>
- GitHub Link:<https://github.com/100daysofdevops>

Reference

100 Days of DevOps — Day 0

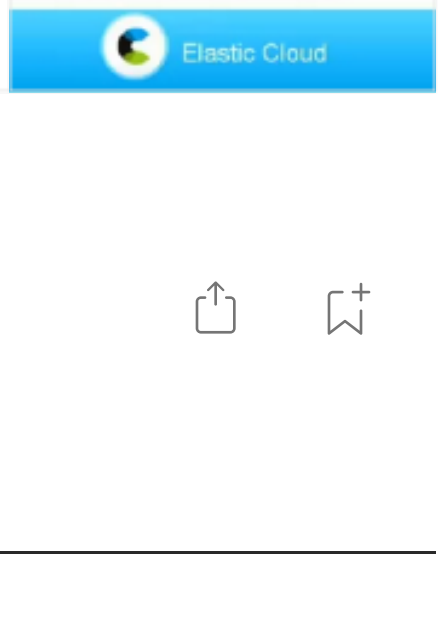
D-day is just one day away and finally, this is a continuation of the post(I posted a month earlier)


medium.com


100 Days of DevOps — Day 84-Introduction to ElasticSearch


Welcome to Day 84 of 100 Days of DevOps, Focus for today is Introduction to ElasticSearch


medium.com





 54




 54





Get an email whenever Prashant Lakhera publishes.

Your email

 Subscribe

By signing up, you will create a Medium account if you don't already have one. Review our [Privacy Policy](#) for more information about our privacy practices.

More from Prashant Lakhera

Follow




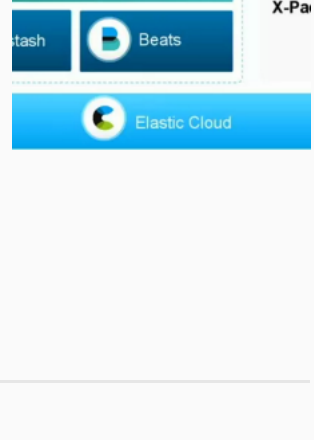
AWS Community Builder, Ex-Redhat, Author, Blogger, YouTuber, RHCA, RHCHS, RHCE, Docker Certified,4XAWS, CCNA, MCP, Certified Jenkins, Terraform Certified, 1XGCP

100 Days of DevOps — Day 84-Introduction to ElasticSearch

To view the updated DevOps course(101DaysofDevOps) Course Registration link: <https://www.101daysofdevops.com/register/> Course...

Elasticsearch 7 min read






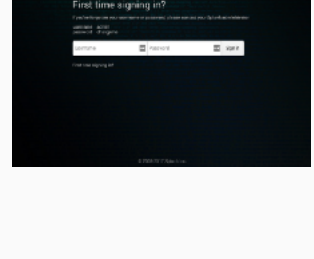
Share your ideas with millions of readers. [Write on Medium](#)

100 Days of DevOps — Day 83-Introduction to Splunk

To view the updated DevOps course(101DaysofDevOps) Course Registration link: <https://www.101daysofdevops.com/register/> Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>...

Dev Ops 6 min read




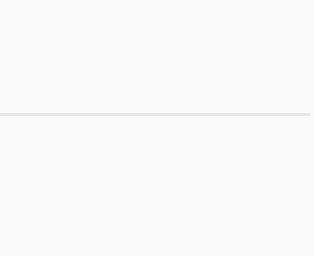


100 Days of DevOps — Day 82- Python Object Oriented Programming(OOP)

To view the updated DevOps course(101DaysofDevOps) Course Registration link: <https://www.101daysofdevops.com/register/> Course...

Programming 6 min read




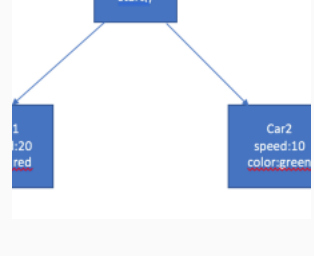


100 Days of DevOps — Day 81-Debugging Python Code

To view the updated DevOps course(101DaysofDevOps) Course Registration link: <https://www.101daysofdevops.com/register/> Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/>...

Debugging 5 min read

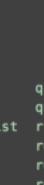




100 Days of DevOps — Day 80-Python Unit Testing(Pytest)

To view the updated DevOps course(101DaysofDevOps) Course Registration link: <https://www.101daysofdevops.com/register/> Course Link: <https://www.101daysofdevops.com/courses/101-days-of-devops/> YouTube link:...

Python 5 min read



Love podcasts or audiobooks? Learn on the go with our new app. [Try Knowable](#)