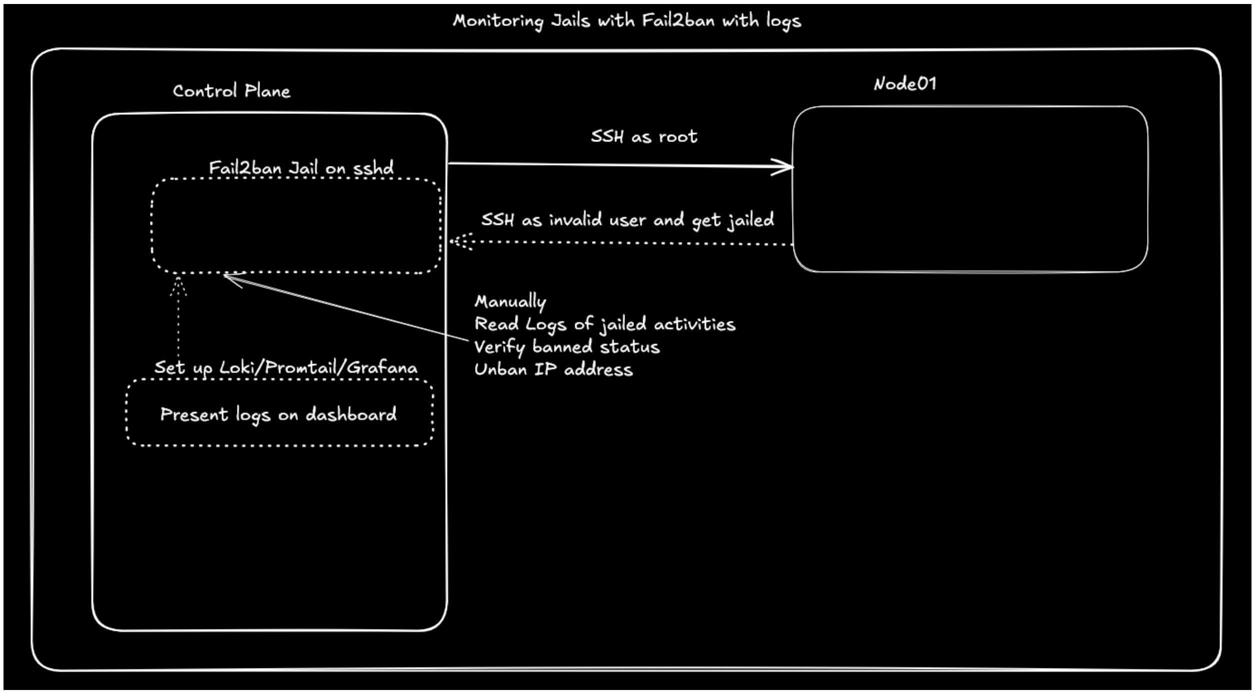
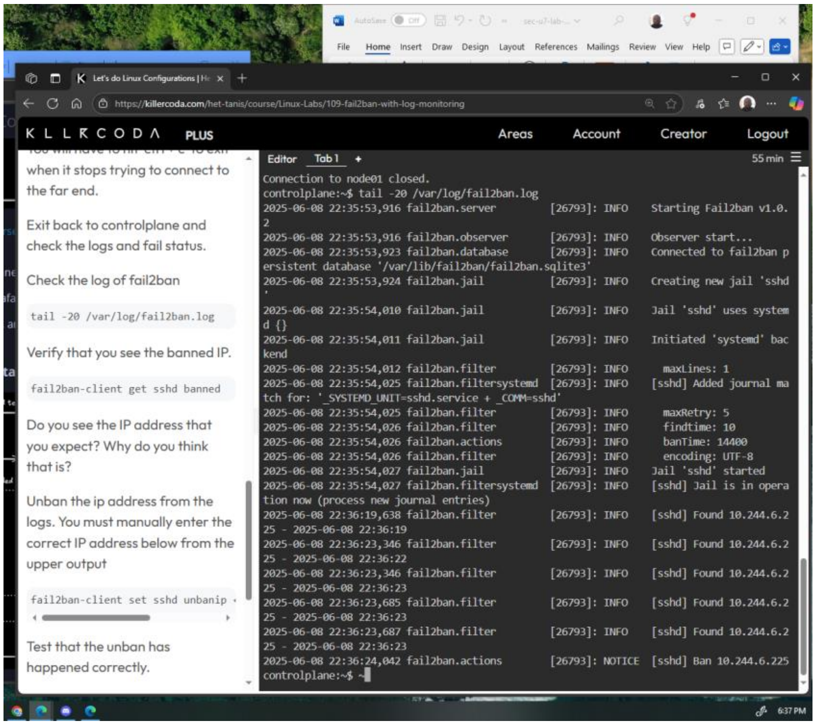
Unit 7 Lab - Monitoring and Alerting

Monitoring Jails with Fail2ban logs 1 of 2


Monitoring Jails with Fail2ban with logs
Control Plane
Node01
SSH as root
Fail2ban Jail on sshd
SSH as invalid user and get jailed
Manually
Read Logs of jailed activities
Verify banned status
Unban IP address
Set up Loki/Promtail/Grafana
Present logs on dashboard

Monitoring Jails with Fail2ban logs 2 of 2

Complete the lab: https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring


Let's do Linux Configurations | He
https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring
KLLRCODA PLUS
Areas
Account
Creator
Logout
Editor
Tab 1
55 min
6:37 PM

when it stops trying to connect to the far end.

Exit back to controlplane and check the logs and fail status.

Check the log of fail2ban

```
tail -20 /var/log/fail2ban.log
```

Verify that you see the banned IP.

```
fail2ban-client get sshd banned
```

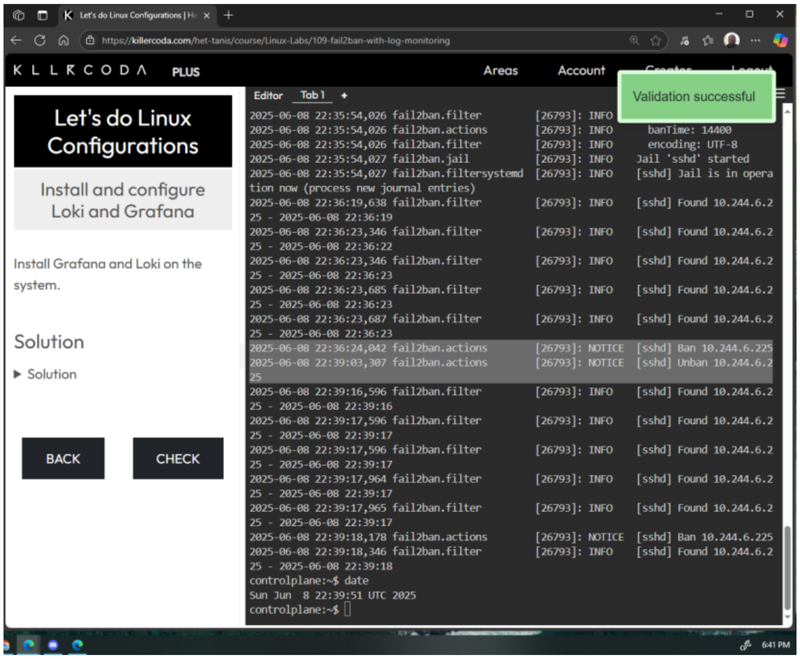
Do you see the IP address that you expect? Why do you think that is?

Unban the ip address from the logs. You must manually enter the correct IP address below from the upper output

```
fail2ban-client set sshd unbanip
```

Test that the unban has happened correctly.

```
Connection to node01 closed.
controlplane:~$ tail -20 /var/log/fail2ban.log
2025-06-08 22:35:53,916 fail2ban.server         [26793]: INFO    Starting Fail2ban v1.0.
2
2025-06-08 22:35:53,916 fail2ban.observer       [26793]: INFO    Observer start...
2025-06-08 22:35:53,923 fail2ban.database       [26793]: INFO    Connected to fail2ban p
ersistent database '/var/lib/fail2ban/fail2ban.sqlite3'
2025-06-08 22:35:53,924 fail2ban.jail           [26793]: INFO    Creating new jail 'sshd
'
2025-06-08 22:35:54,010 fail2ban.jail           [26793]: INFO    Jail 'sshd' uses system
d {}
2025-06-08 22:35:54,011 fail2ban.jail           [26793]: INFO    Initiated 'systemd' bac
kend
2025-06-08 22:35:54,012 fail2ban.filter         [26793]: INFO      maxLines: 1
2025-06-08 22:35:54,025 fail2ban.filtersystemd  [26793]: INFO    [sshd] Added journal ma
tch for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2025-06-08 22:35:54,025 fail2ban.filter         [26793]: INFO      maxRetry: 5
2025-06-08 22:35:54,026 fail2ban.filter         [26793]: INFO      findtime: 10
2025-06-08 22:35:54,026 fail2ban.actions        [26793]: INFO      banTime: 14400
2025-06-08 22:35:54,026 fail2ban.filter         [26793]: INFO      encoding: UTF-8
2025-06-08 22:35:54,027 fail2ban.jail           [26793]: INFO    Jail 'sshd' started
2025-06-08 22:35:54,027 fail2ban.filtersystemd  [26793]: INFO    [sshd] Jail is in opera
tion now (process new journal entries)
2025-06-08 22:36:19,638 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:19
2025-06-08 22:36:23,346 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:22
2025-06-08 22:36:23,346 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:23
2025-06-08 22:36:23,685 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:23
2025-06-08 22:36:23,687 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:23
2025-06-08 22:36:24,042 fail2ban.actions        [26793]: NOTICE  [sshd] Ban 10.244.6.225
controlplane:~$ ~
```


Let's do Linux Configurations | He
https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring
KLLRCODA PLUS
Areas
Account
Editor
Tab 1
BACK
CHECK
6:41 PM

Validation successful

Let's do Linux Configurations

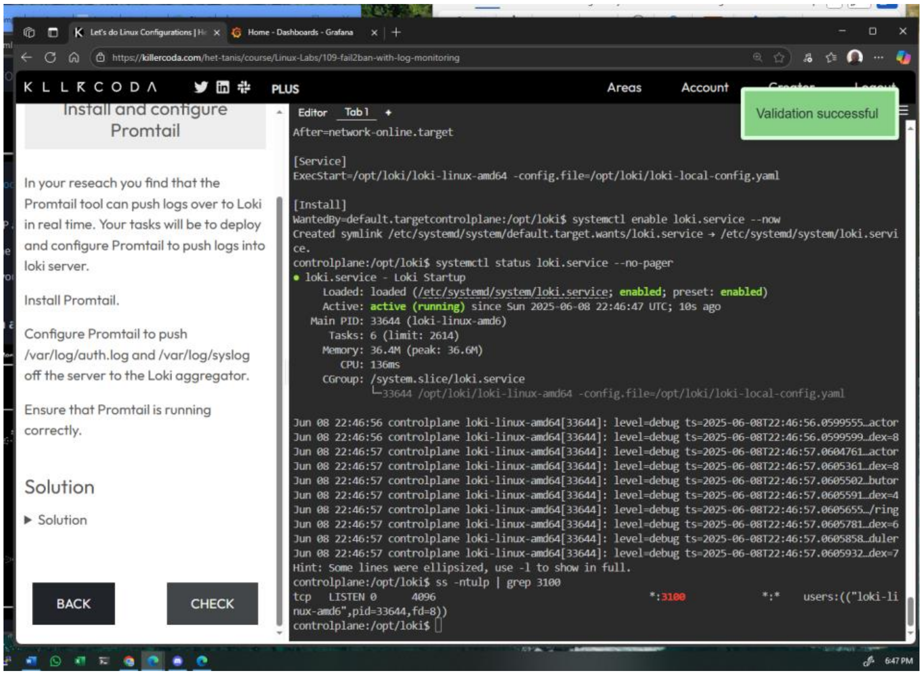
Install and configure Loki and Grafana

Install Grafana and Loki on the system.

Solution

▶ Solution

```
2025-06-08 22:35:54,026 fail2ban.filter         [26793]: INFO
2025-06-08 22:35:54,026 fail2ban.actions        [26793]: INFO      banTime: 14400
2025-06-08 22:35:54,026 fail2ban.filter         [26793]: INFO      encoding: UTF-8
2025-06-08 22:35:54,027 fail2ban.jail           [26793]: INFO    Jail 'sshd' started
2025-06-08 22:35:54,027 fail2ban.filtersystemd  [26793]: INFO    [sshd] Jail is in opera
tion now (process new journal entries)
2025-06-08 22:36:19,638 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:19
2025-06-08 22:36:23,346 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:22
2025-06-08 22:36:23,346 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:23
2025-06-08 22:36:23,685 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:23
2025-06-08 22:36:23,687 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:36:23
2025-06-08 22:36:24,042 fail2ban.actions        [26793]: NOTICE  [sshd] Ban 10.244.6.225
2025-06-08 22:39:03,307 fail2ban.actions        [26793]: NOTICE  [sshd] Unban 10.244.6.2
25
2025-06-08 22:39:16,596 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:39:16
2025-06-08 22:39:17,596 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:39:17
2025-06-08 22:39:17,596 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:39:17
2025-06-08 22:39:17,964 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:39:17
2025-06-08 22:39:17,965 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:39:17
2025-06-08 22:39:18,178 fail2ban.actions        [26793]: NOTICE  [sshd] Ban 10.244.6.225
2025-06-08 22:39:18,346 fail2ban.filter         [26793]: INFO    [sshd] Found 10.244.6.2
25 - 2025-06-08 22:39:18
controlplane:~$ date
Sun Jun  8 22:39:51 UTC 2025
controlplane:~$ 
```


Let's do Linux Configurations | Ho
Home - Dashboards - Grafana
https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring
KILLERCODA
PLUS
Areas
Account
Validation successful
Editor
Tab 1
BACK
CHECK
6:47 PM

Install and configure Promtail

In your reseach you find that the Promtail tool can push logs over to Loki in real time. Your tasks will be to deploy and configure Promtail to push logs into loki server.

Install Promtail.

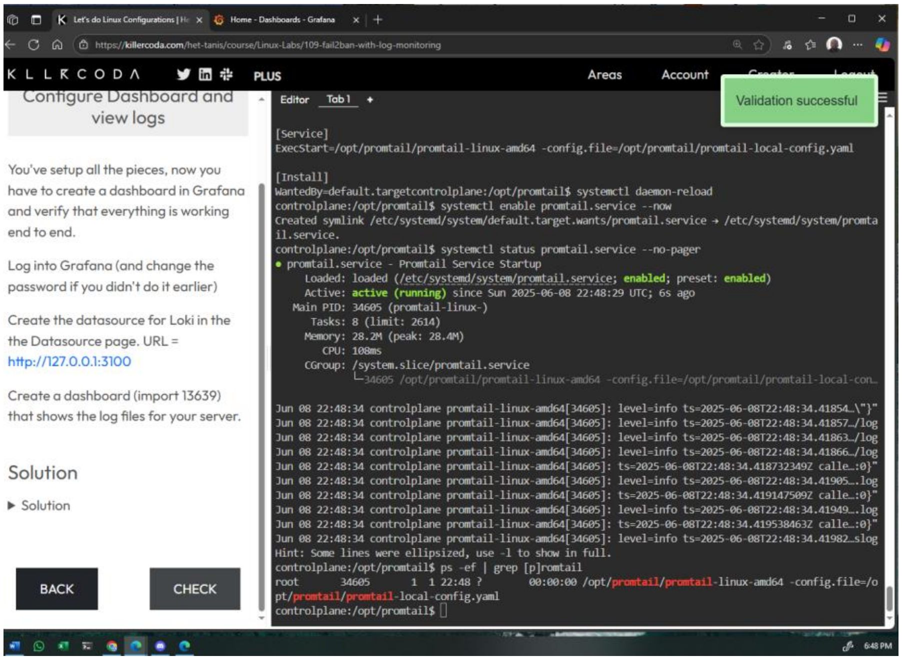
Configure Promtail to push /var/log/auth.log and /var/log/syslog off the server to the Loki aggregator.

Ensure that Promtail is running correctly.

Solution

▶ Solution

```
After=network-online.target

[Service]
ExecStart=/opt/loki/loki-linux-amd64 -config.file=/opt/loki/loki-local-config.yaml

[Install]
WantedBy=default.targetcontrolplane:/opt/loki$ systemctl enable loki.service --now
Created symlink /etc/systemd/system/default.target.wants/loki.service → /etc/systemd/system/loki.servi
ce.
controlplane:/opt/loki$ systemctl status loki.service --no-pager
● loki.service - Loki Startup
     Loaded: loaded (/etc/systemd/system/loki.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-06-08 22:46:47 UTC; 10s ago
   Main PID: 33644 (loki-linux-amd6)
      Tasks: 6 (limit: 2614)
     Memory: 36.4M (peak: 36.6M)
        CPU: 136ms
     CGroup: /system.slice/loki.service
             └─33644 /opt/loki/loki-linux-amd64 -config.file=/opt/loki/loki-local-config.yaml

Jun 08 22:46:56 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:56.0599555…actor
Jun 08 22:46:56 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:56.0599599…dex=8
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0604761…actor
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605361…dex=8
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605502…butor
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605591…dex=4
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605655…/ring
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605781…dex=6
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605858…duler
Jun 08 22:46:57 controlplane loki-linux-amd64[33644]: level=debug ts=2025-06-08T22:46:57.0605932…dex=7
Hint: Some lines were ellipsized, use -l to show in full.
controlplane:/opt/loki$ ss -ntulp | grep 3100
tcp   LISTEN 0      4096                              *:3100           *:*    users:(("loki-li
nux-amd6",pid=33644,fd=8))
controlplane:/opt/loki$ 
```


Let's do Linux Configurations | Ho
Home - Dashboards - Grafana
https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring
KILLERCODA
PLUS
Areas
Account
Validation successful
Editor
Tab 1
BACK
CHECK
6:48 PM

Configure Dashboard and view logs

You've setup all the pieces, now you have to create a dashboard in Grafana and verify that everything is working end to end.

Log into Grafana (and change the password if you didn't do it earlier)

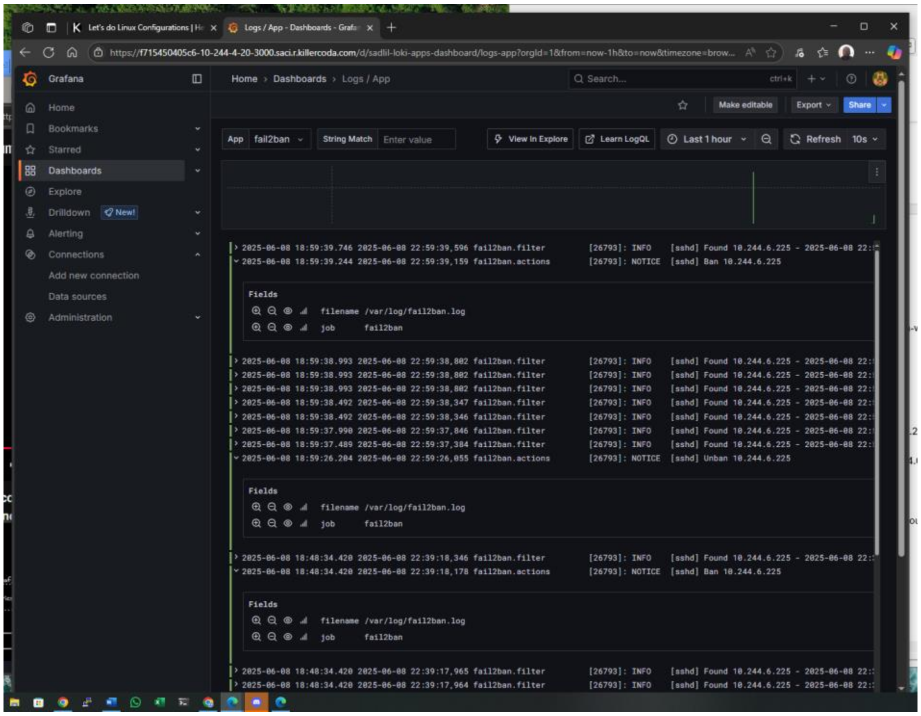
Create the datasource for Loki in the the Datasource page. URL = http://127.0.0.1:3100

Create a dashboard (import 13639) that shows the log files for your server.

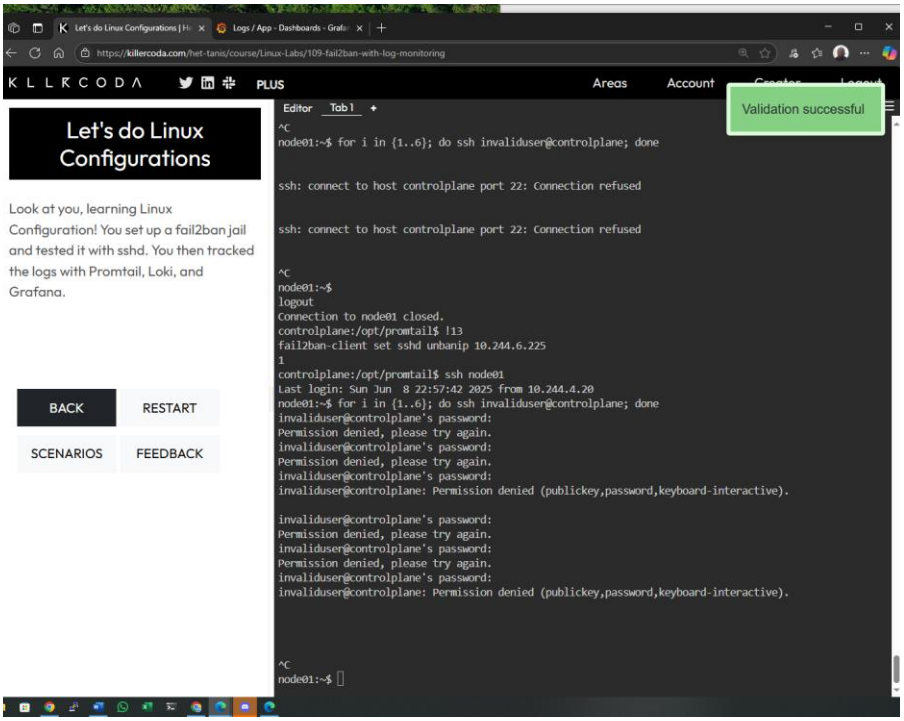
Solution

▶ Solution

```
[Service]
ExecStart=/opt/promtail/promtail-linux-amd64 -config.file=/opt/promtail/promtail-local-config.yaml

[Install]
WantedBy=default.targetcontrolplane:/opt/promtail$ systemctl daemon-reload
controlplane:/opt/promtail$ systemctl enable promtail.service --now
Created symlink /etc/systemd/system/default.target.wants/promtail.service → /etc/systemd/system/promta
il.service.
controlplane:/opt/promtail$ systemctl status promtail.service --no-pager
● promtail.service - Promtail Service Startup
     Loaded: loaded (/etc/systemd/system/promtail.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-06-08 22:48:29 UTC; 6s ago
   Main PID: 34605 (promtail-linux-)
      Tasks: 8 (limit: 2614)
     Memory: 28.2M (peak: 28.4M)
        CPU: 108ms
     CGroup: /system.slice/promtail.service
             └─34605 /opt/promtail/promtail-linux-amd64 -config.file=/opt/promtail/promtail-local-con…

Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41854…\"}"
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41857…/log
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41863…/log
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41866…/log
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: ts=2025-06-08T22:48:34.418732349Z calle…:0}"
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41905….log
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: ts=2025-06-08T22:48:34.419147509Z calle…:0}"
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41949….log
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: ts=2025-06-08T22:48:34.419538463Z calle…:0}"
Jun 08 22:48:34 controlplane promtail-linux-amd64[34605]: level=info ts=2025-06-08T22:48:34.41982…slog
Hint: Some lines were ellipsized, use -l to show in full.
controlplane:/opt/promtail$ ps -ef | grep [p]romtail
root       34605       1  1 22:48 ?        00:00:00 /opt/promtail/promtail-linux-amd64 -config.file=/o
pt/promtail/promtail-local-config.yaml
controlplane:/opt/promtail$ 
```



```
> 2025-06-08 18:59:39.746 2025-06-08 22:59:39,596 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
˅ 2025-06-08 18:59:39.244 2025-06-08 22:59:39,159 fail2ban.actions    [26793]: NOTICE [sshd] Ban 10.244.6.225

    Fields
      filename /var/log/fail2ban.log
      job      fail2ban

> 2025-06-08 18:59:38.993 2025-06-08 22:59:38,802 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:59:38.993 2025-06-08 22:59:38,802 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:59:38.993 2025-06-08 22:59:38,802 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:59:38.492 2025-06-08 22:59:38,347 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:59:38.492 2025-06-08 22:59:38,346 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:59:37.990 2025-06-08 22:59:37,846 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:59:37.489 2025-06-08 22:59:37,384 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
˅ 2025-06-08 18:59:26.204 2025-06-08 22:59:26,055 fail2ban.actions    [26793]: NOTICE [sshd] Unban 10.244.6.225

    Fields
      filename /var/log/fail2ban.log
      job      fail2ban

> 2025-06-08 18:48:34.420 2025-06-08 22:39:18,346 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
˅ 2025-06-08 18:48:34.420 2025-06-08 22:39:18,178 fail2ban.actions    [26793]: NOTICE [sshd] Ban 10.244.6.225

    Fields
      filename /var/log/fail2ban.log
      job      fail2ban

> 2025-06-08 18:48:34.420 2025-06-08 22:39:17,965 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
> 2025-06-08 18:48:34.420 2025-06-08 22:39:17,964 fail2ban.filter     [26793]: INFO   [sshd] Found 10.244.6.225 - 2025-06-08 22::
```


Let's do Linux Configurations | H
Logs / App - Dashboards - Grafa
https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring
KILLERCODA
PLUS
Areas
Account
Creator
Logout
Validation successful
Editor
Tab 1
BACK
RESTART
SCENARIOS
FEEDBACK

Let's do Linux Configurations

Look at you, learning Linux Configuration! You set up a fail2ban jail and tested it with sshd. You then tracked the logs with Promtail, Loki, and Grafana.

```
^C
node01:~$ for i in {1..6}; do ssh invaliduser@controlplane; done


ssh: connect to host controlplane port 22: Connection refused


ssh: connect to host controlplane port 22: Connection refused


^C
node01:~$
logout
Connection to node01 closed.
controlplane:/opt/promtail$ !13
fail2ban-client set sshd unbanip 10.244.6.225
1
controlplane:/opt/promtail$ ssh node01
Last login: Sun Jun  8 22:57:42 2025 from 10.244.4.20
node01:~$ for i in {1..6}; do ssh invaliduser@controlplane; done
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
invaliduser@controlplane: Permission denied (publickey,password,keyboard-interactive).

invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
invaliduser@controlplane: Permission denied (publickey,password,keyboard-interactive).



^C
node01:~$
```

Were you able to see the IP address that was banned and unban it?

2025-06-08 22:36:24,042 fail2ban.actions [26793]: NOTICE [sshd] Ban 10.244.6.225

2025-06-08 22:39:03,307 fail2ban.actions [26793]: NOTICE [sshd] Unban 10.244.6.225

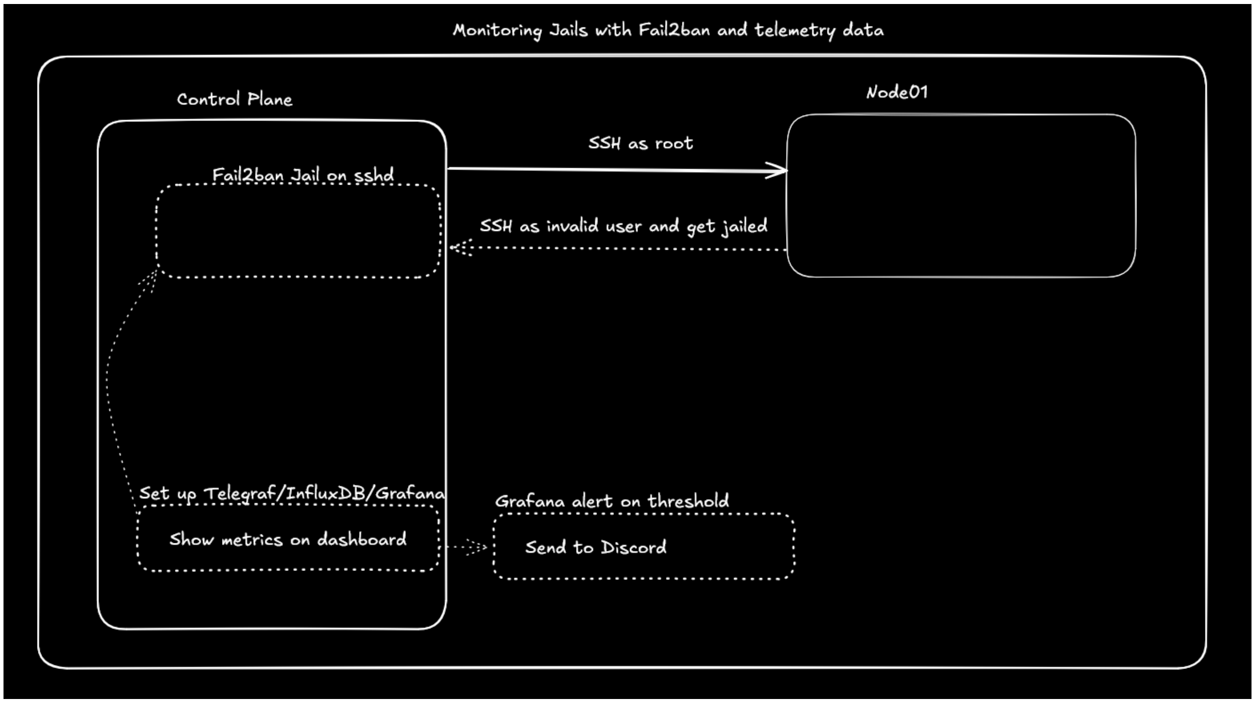
Were you able to see all the NOTICE events in Grafana?

Yes

What other questions do you have about this lab, and how might you go figure them out?

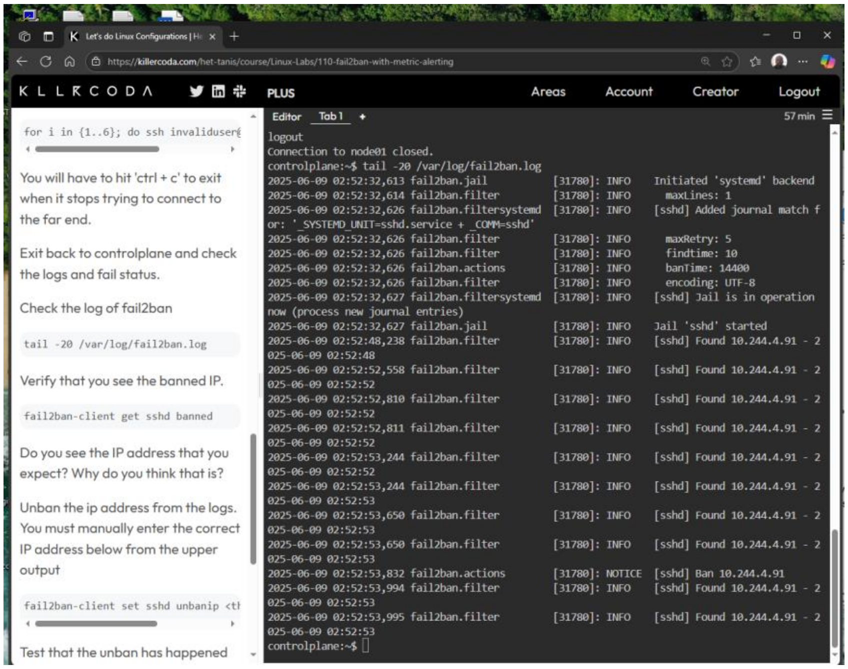
I would like to repeat this lab

Monitoring Jails with Fail2ban and telemetry data 1 of 2


Monitoring Jails with Fail2ban and telemetry data
Control Plane
Node01
SSH as root
Fail2ban Jail on sshd
SSH as invalid user and get jailed
Set up Telegraf/InfluxDB/Grafana
Show metrics on dashboard
Grafana alert on threshold
Send to Discord

Monitoring Jails with Fail2ban and telemetry data 2 of 2

Complete the lab here: https://killercoda.com/het-tanis/course/Linux-Labs/110-fail2ban-with-metric-alerting


Let's do Linux Configurations | He
https://killercoda.com/het-tanis/course/Linux-Labs/110-fail2ban-with-metric-alerting
KLLRCODA
PLUS
Areas
Account
Creator
Logout
Editor
Tab 1
57 min

```
for i in {1..6}; do ssh invaliduser@
```

You will have to hit 'ctrl + c' to exit when it stops trying to connect to the far end.

Exit back to controlplane and check the logs and fail status.

Check the log of fail2ban

```
tail -20 /var/log/fail2ban.log
```

Verify that you see the banned IP.

```
fail2ban-client get sshd banned
```

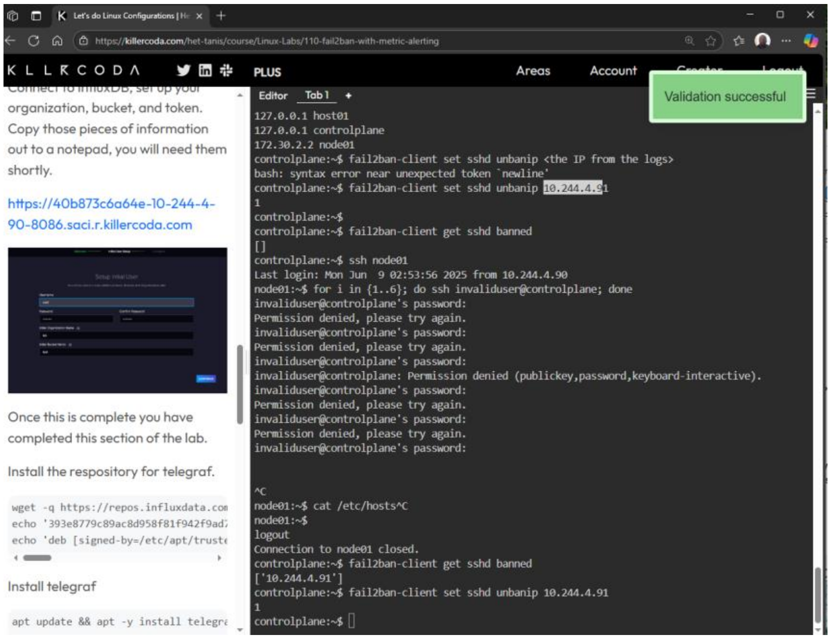
Do you see the IP address that you expect? Why do you think that is?

Unban the ip address from the logs. You must manually enter the correct IP address below from the upper output

```
fail2ban-client set sshd unbanip <th
```

Test that the unban has happened

```
logout
Connection to node01 closed.
controlplane:~$ tail -20 /var/log/fail2ban.log
2025-06-09 02:52:32,613 fail2ban.jail           [31780]: INFO    Initiated 'systemd' backend
2025-06-09 02:52:32,614 fail2ban.filter         [31780]: INFO      maxLines: 1
2025-06-09 02:52:32,626 fail2ban.filtersystemd  [31780]: INFO    [sshd] Added journal match f
or: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd'
2025-06-09 02:52:32,626 fail2ban.filter         [31780]: INFO      maxRetry: 5
2025-06-09 02:52:32,626 fail2ban.filter         [31780]: INFO      findtime: 10
2025-06-09 02:52:32,626 fail2ban.actions        [31780]: INFO      banTime: 14400
2025-06-09 02:52:32,626 fail2ban.filter         [31780]: INFO      encoding: UTF-8
2025-06-09 02:52:32,627 fail2ban.filtersystemd  [31780]: INFO    [sshd] Jail is in operation
now (process new journal entries)
2025-06-09 02:52:32,627 fail2ban.jail           [31780]: INFO    Jail 'sshd' started
2025-06-09 02:52:48,238 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:48
2025-06-09 02:52:52,558 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:52
2025-06-09 02:52:52,810 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:52
2025-06-09 02:52:52,811 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:52
2025-06-09 02:52:53,244 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:52
2025-06-09 02:52:53,244 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:53
2025-06-09 02:52:53,650 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:53
2025-06-09 02:52:53,650 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:53
2025-06-09 02:52:53,832 fail2ban.actions        [31780]: NOTICE  [sshd] Ban 10.244.4.91
2025-06-09 02:52:53,994 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:53
2025-06-09 02:52:53,995 fail2ban.filter         [31780]: INFO    [sshd] Found 10.244.4.91 - 2
025-06-09 02:52:53
controlplane:~$
```


Let's do Linux Configurations | He
https://killercoda.com/het-tanis/course/Linux-Labs/110-fail2ban-with-metric-alerting
KLLRCODA
PLUS
Areas
Account
Creator
Logout
Editor
Tab 1
Validation successful

Connect to InfluxDB, set up your organization, bucket, and token. Copy those pieces of information out to a notepad, you will need them shortly.

https://40b873c6a64e-10-244-4-90-8086.saci.r.killercoda.com

Once this is complete you have completed this section of the lab.

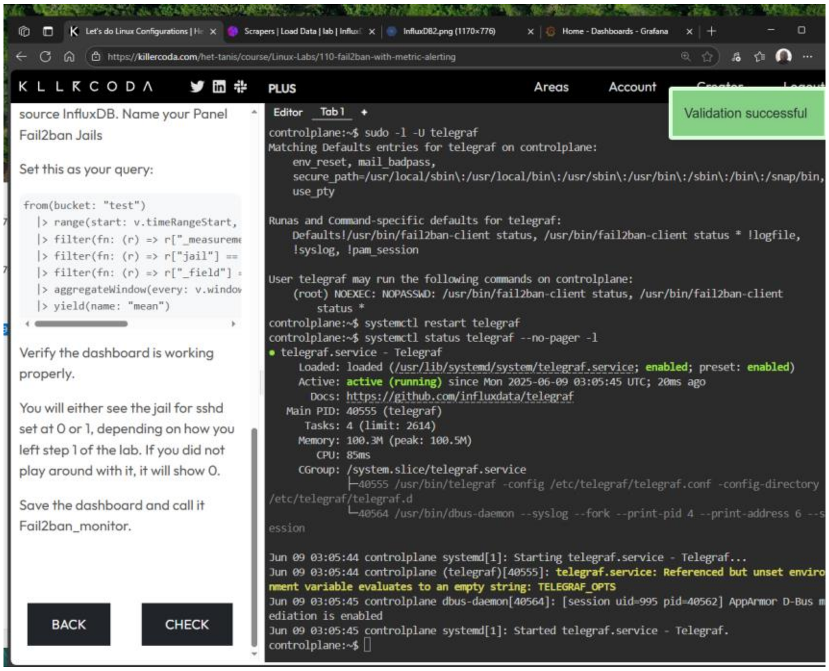
Install the respository for telegraf.

```
wget -q https://repos.influxdata.com
echo '393e8779c89ac8d958f81f942f9ad
echo 'deb [signed-by=/etc/apt/truste
```

Install telegraf

```
apt update && apt -y install telegra
```

```
127.0.0.1 host01
127.0.0.1 controlplane
172.30.2.2 node01
controlplane:~$ fail2ban-client set sshd unbanip <the IP from the logs>
bash: syntax error near unexpected token `newline'
controlplane:~$ fail2ban-client set sshd unbanip 10.244.4.91
1
controlplane:~$
controlplane:~$ fail2ban-client get sshd banned
[]
controlplane:~$ ssh node01
Last login: Mon Jun  9 02:53:56 2025 from 10.244.4.90
node01:~$ for i in {1..6}; do ssh invaliduser@controlplane; done
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
invaliduser@controlplane: Permission denied (publickey,password,keyboard-interactive).
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:


^C
node01:~$ cat /etc/hosts^C
node01:~$
logout
Connection to node01 closed.
controlplane:~$ fail2ban-client get sshd banned
['10.244.4.91']
controlplane:~$ fail2ban-client set sshd unbanip 10.244.4.91
1
controlplane:~$
```



Let's do Linux Configurations | H
Scrapers | Load Data | lab | Influx
InfluxDB2.png (1170×776)
Home - Dashboards - Grafana
https://killercoda.com/het-tanis/course/Linux-Labs/110-fail2ban-with-metric-alerting
KLLRCODA
PLUS
Areas
Account
Editor
Tab 1
BACK
CHECK

Validation successful

source InfluxDB. Name your Panel Fail2ban Jails

Set this as your query:

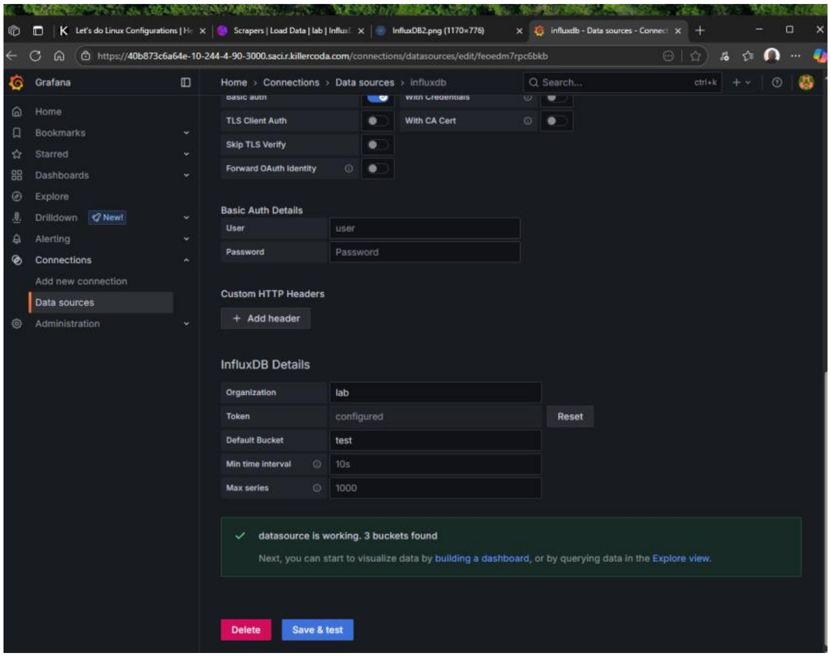
```
from(bucket: "test")
  |> range(start: v.timeRangeStart,
  |> filter(fn: (r) => r["_measureme
  |> filter(fn: (r) => r["jail"] ==
  |> filter(fn: (r) => r["_field"] =
  |> aggregateWindow(every: v.windov
  |> yield(name: "mean")
```

Verify the dashboard is working properly.

You will either see the jail for sshd set at 0 or 1, depending on how you left step 1 of the lab. If you did not play around with it, it will show 0.

Save the dashboard and call it Fail2ban_monitor.

```
controlplane:~$ sudo -l -U telegraf
Matching Defaults entries for telegraf on controlplane:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

Runas and Command-specific defaults for telegraf:
    Defaults!/usr/bin/fail2ban-client status, /usr/bin/fail2ban-client status * !logfile,
    !syslog, !pam_session

User telegraf may run the following commands on controlplane:
    (root) NOEXEC: NOPASSWD: /usr/bin/fail2ban-client status, /usr/bin/fail2ban-client
        status *
controlplane:~$ systemctl restart telegraf
controlplane:~$ systemctl status telegraf --no-pager -l
● telegraf.service - Telegraf
     Loaded: loaded (/usr/lib/systemd/system/telegraf.service; enabled; preset: enabled)
     Active: active (running) since Mon 2025-06-09 03:05:45 UTC; 20ms ago
       Docs: https://github.com/influxdata/telegraf
   Main PID: 40555 (telegraf)
      Tasks: 4 (limit: 2614)
     Memory: 100.3M (peak: 100.5M)
        CPU: 85ms
     CGroup: /system.slice/telegraf.service
             ├─40555 /usr/bin/telegraf -config /etc/telegraf/telegraf.conf -config-directory
/etc/telegraf/telegraf.d
             └─40564 /usr/bin/dbus-daemon --syslog --fork --print-pid 4 --print-address 6 --s
ession

Jun 09 03:05:44 controlplane systemd[1]: Starting telegraf.service - Telegraf...
Jun 09 03:05:44 controlplane (telegraf)[40555]: telegraf.service: Referenced but unset enviro
nment variable evaluates to an empty string: TELEGRAF_OPTS
Jun 09 03:05:45 controlplane dbus-daemon[40564]: [session uid=995 pid=40562] AppArmor D-Bus m
ediation is enabled
Jun 09 03:05:45 controlplane systemd[1]: Started telegraf.service - Telegraf.
controlplane:~$ 
```



Let's do Linux Configurations | H
Scrapers | Load Data | lab | Influx
InfluxDB2.png (1170×776)
influxdb - Data sources - Connect
https://40b873c6a64e-10-244-4-90-3000.saci.r.killercoda.com/connections/datasources/edit/feoedm7rpc6bkb
Grafana
Home › Connections › Data sources › influxdb
Search... ctrl+k
Home
Bookmarks
Starred
Dashboards
Explore
Drilldown
New!
Alerting
Connections
Add new connection
Data sources
Administration
Add header
Reset
Delete
Save & test

Basic auth
With Credentials
TLS Client Auth
With CA Cert
Skip TLS Verify
Forward OAuth Identity

Basic Auth Details

User	user
Password	Password

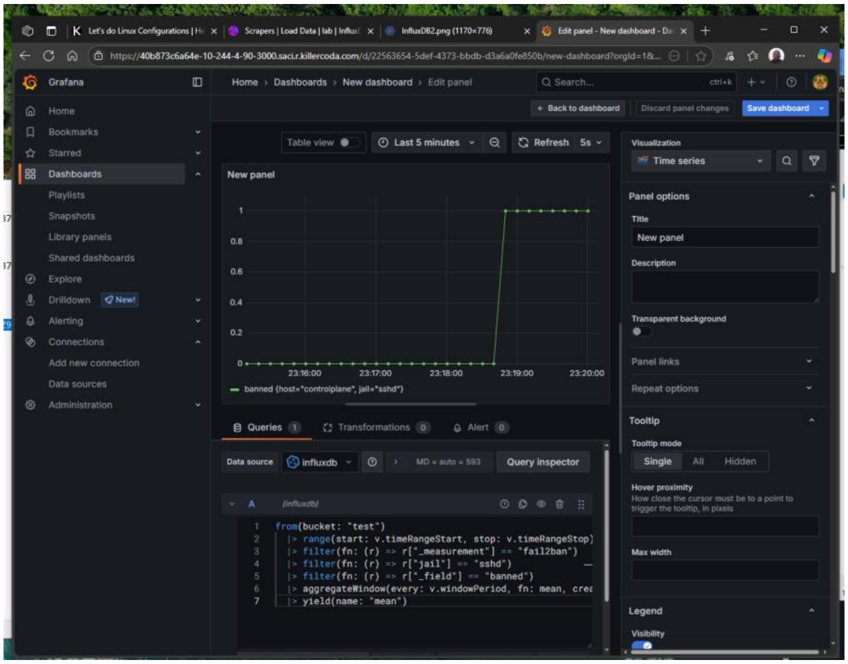
Custom HTTP Headers

InfluxDB Details

Organization	lab
Token	configured
Default Bucket	test
Min time interval	10s
Max series	1000

✓ datasource is working. 3 buckets found

Next, you can start to visualize data by building a dashboard, or by querying data in the Explore view.



https://40b873c6a64e-10-244-4-90-3000.saci.r.killercoda.com/d/22563654-5def-4373-bbdb-d3a6a0fe850b/new-dashboard?orgId=1&...

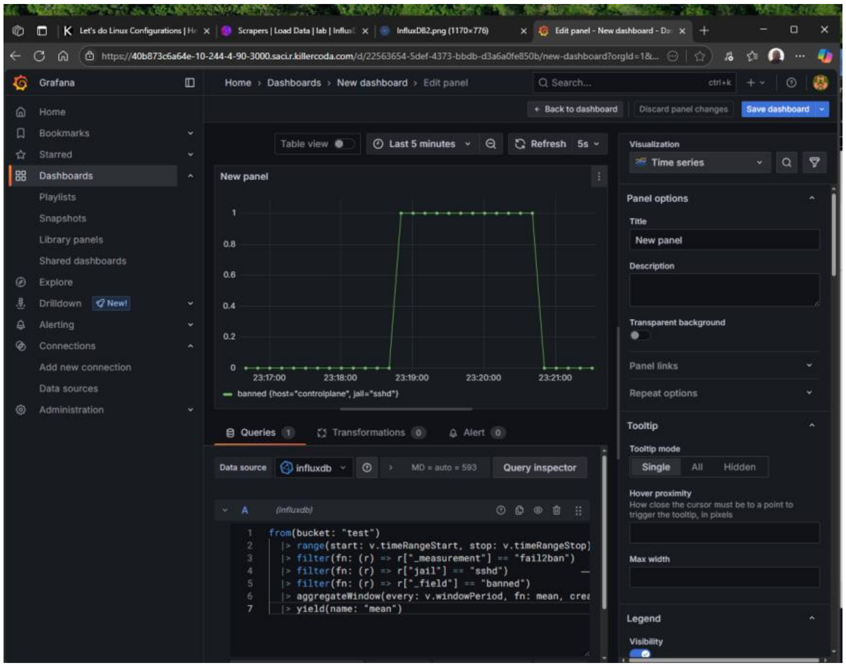
Title: New panel

Tooltip mode: Single

Data source: influxdb

MD = auto = 593

```
from(bucket: "test")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["_measurement"] == "fail2ban")
  |> filter(fn: (r) => r["jail"] == "sshd")
  |> filter(fn: (r) => r["_field"] == "banned")
  |> aggregateWindow(every: v.windowPeriod, fn: mean, crea
  |> yield(name: "mean")
```



https://40b873c6a64e-10-244-4-90-3000.saci.r.killercoda.com/d/22563654-5def-4373-bbdb-d3a6a0fe850b/new-dashboard?orgId=1&...

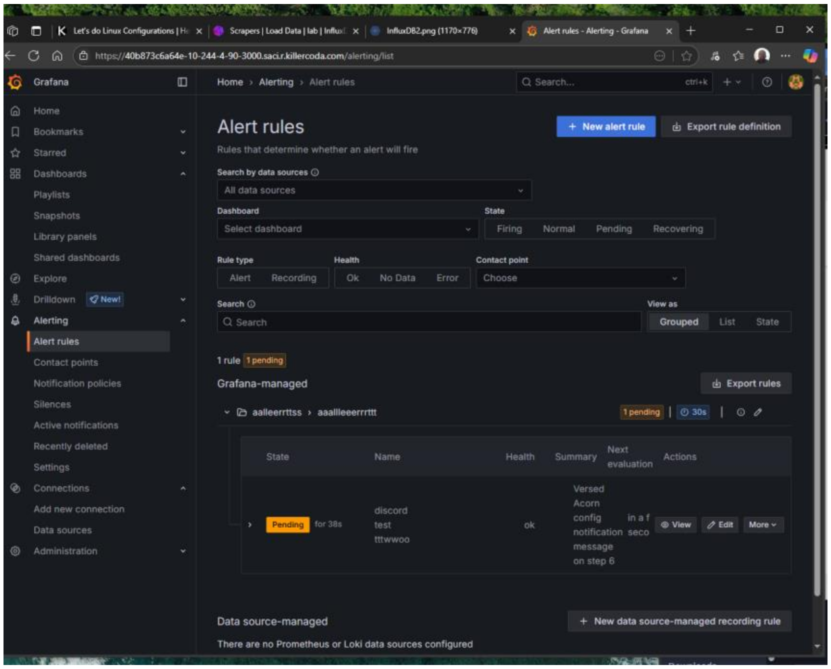
Title: New panel

Tooltip mode: Single

Data source: influxdb

MD = auto = 593

```
from(bucket: "test")
  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)
  |> filter(fn: (r) => r["_measurement"] == "fail2ban")
  |> filter(fn: (r) => r["jail"] == "sshd")
  |> filter(fn: (r) => r["_field"] == "banned")
  |> aggregateWindow(every: v.windowPeriod, fn: mean, crea
  |> yield(name: "mean")
```



Alert rules

Rules that determine whether an alert will fire

Search by data sources: All data sources

Dashboard: Select dashboard

State: Firing | Normal | Pending | Recovering

Rule type: Alert | Recording

Health: Ok | No Data | Error

Contact point: Choose

Search: Search

View as: Grouped | List | State

1 rule 1 pending

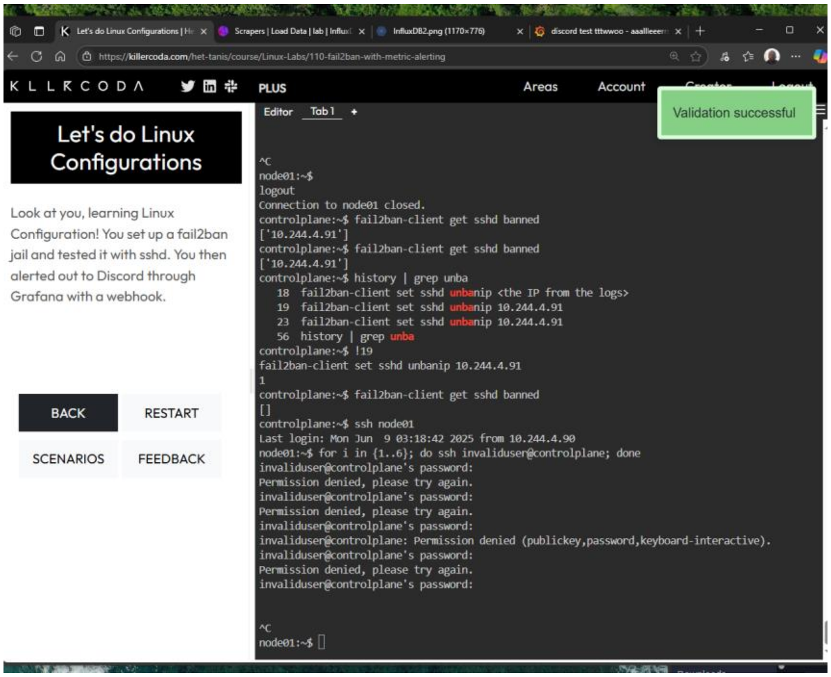
Grafana-managed

aalleerrttss › aaallleeerrrttt 1 pending | 30s

State	Name	Health	Summary	Next evaluation	Actions
Pending for 38s	discord test tttwwoo	ok	Versed Acorn config notification message on step 6	in a f seco	View Edit More

Data source-managed

There are no Prometheus or Loki data sources configured

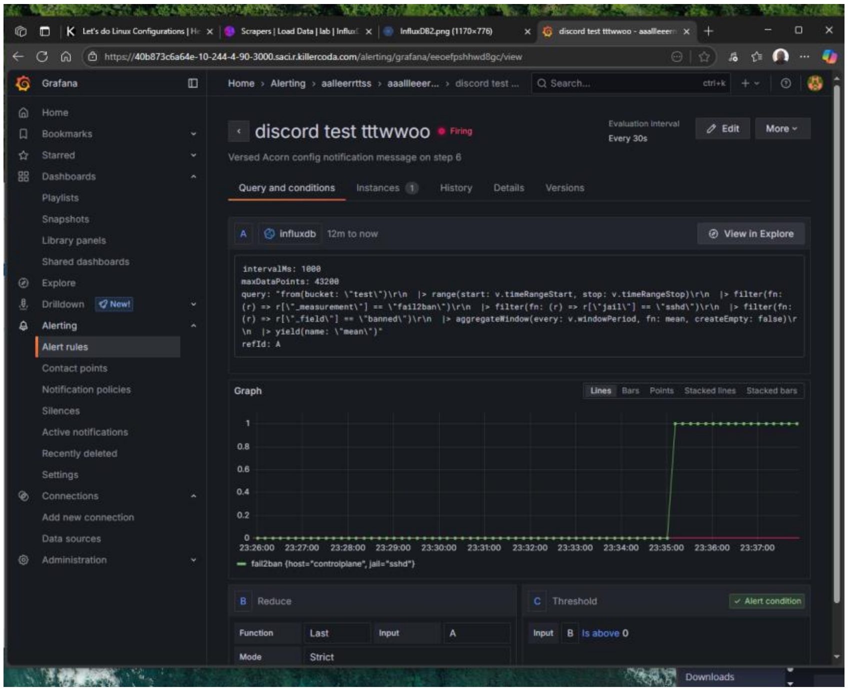

Let's do Linux Configurations | He
Scrapers | Load Data | lab | Influx
InfluxDB2.png (1170×776)
discord test tttwwoo - aaallleeerr
https://killercoda.com/het-tanis/course/Linux-Labs/110-fail2ban-with-metric-alerting
KILLERCODA
PLUS
Areas
Account
Creator
Logout
Editor
Tab 1
BACK
RESTART
SCENARIOS
FEEDBACK

Validation successful

Let's do Linux Configurations

Look at you, learning Linux Configuration! You set up a fail2ban jail and tested it with sshd. You then alerted out to Discord through Grafana with a webhook.

```
^C
node01:~$
logout
Connection to node01 closed.
controlplane:~$ fail2ban-client get sshd banned
['10.244.4.91']
controlplane:~$ fail2ban-client get sshd banned
['10.244.4.91']
controlplane:~$ history | grep unba
   18  fail2ban-client set sshd unbanip <the IP from the logs>
   19  fail2ban-client set sshd unbanip 10.244.4.91
   23  fail2ban-client set sshd unbanip 10.244.4.91
   56  history | grep unba
controlplane:~$ !19
fail2ban-client set sshd unbanip 10.244.4.91
1
controlplane:~$ fail2ban-client get sshd banned
[]
controlplane:~$ ssh node01
Last login: Mon Jun  9 03:18:42 2025 from 10.244.4.90
node01:~$ for i in {1..6}; do ssh invaliduser@controlplane; done
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:
invaliduser@controlplane: Permission denied (publickey,password,keyboard-interactive).
invaliduser@controlplane's password:
Permission denied, please try again.
invaliduser@controlplane's password:


^C
node01:~$ 
```



discord test tttwwoo ● Firing

Evaluation interval
Every 30s

Versed Acorn config notification message on step 6

A influxdb 12m to now

```
intervalMs: 1000
maxDataPoints: 43200
query: "from(bucket: \"test\")\r\n  |> range(start: v.timeRangeStart, stop: v.timeRangeStop)\r\n  |> filter(fn:
(r) => r[\"_measurement\"] == \"fail2ban\")\r\n  |> filter(fn: (r) => r[\"jail\"] == \"sshd\")\r\n  |> filter(fn:
(r) => r[\"_field\"] == \"banned\")\r\n  |> aggregateWindow(every: v.windowPeriod, fn: mean, createEmpty: false)\r
\n  |> yield(name: \"mean\")"
refId: A
```

— fail2ban {host="controlplane", jail="sshd"}

B Reduce

Function: Last Input: A
Mode: Strict

C Threshold

Input: B Is above 0

Do you see fail2ban in the Grafana Dashboard?

Yes

If not, how are you going to troubleshoot it?

Did you get your test alert and then real alert to trigger into the Discord channel?

Yes

https://discord.com/channels/611027490848374811/746588442603028546/1381475036862353591
https://discord.com/channels/611027490848374811/746588442603028546/1381477154520563873

What other applications or uses for this could you think of?

Batch jobs completion...

Do you have other places where you could send alerts that would help you professionally?

> **A group email thread that just records various output for occasional historical review.**