Unit 7 Lab – Monitoring and Alerting

Required Materials

Putty or other connection tool

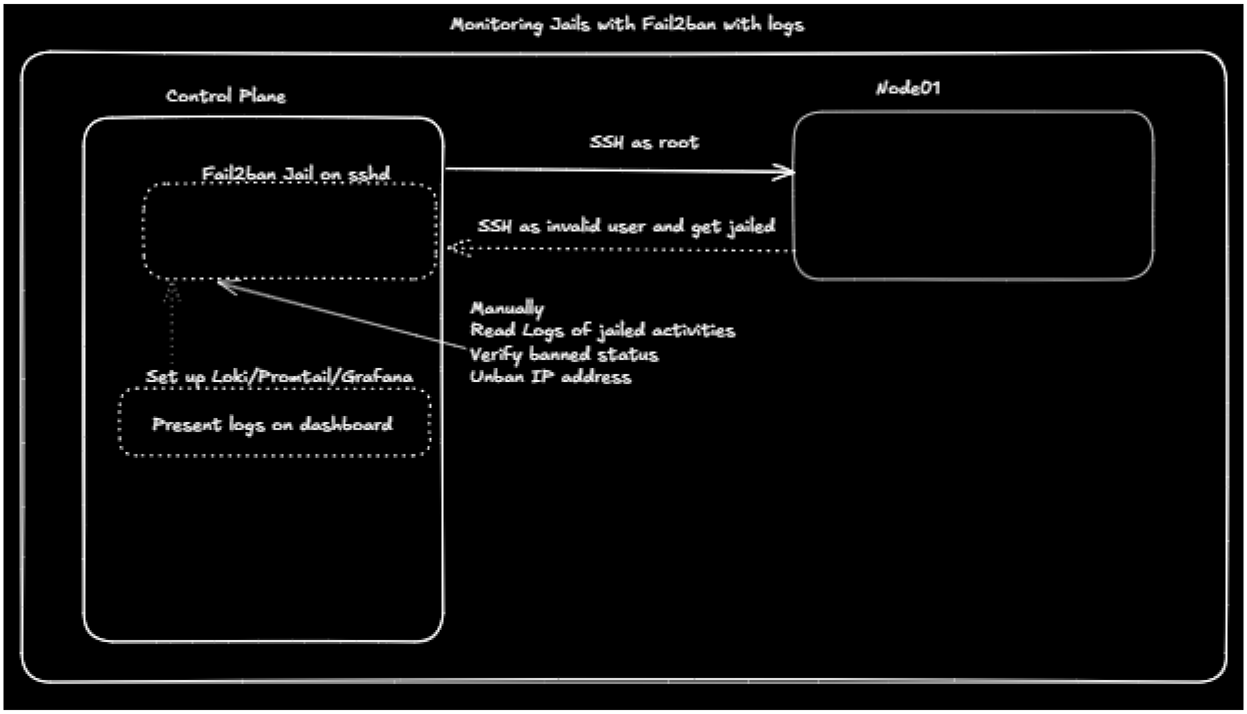
Lab Server

Root or sudo command access

LAB

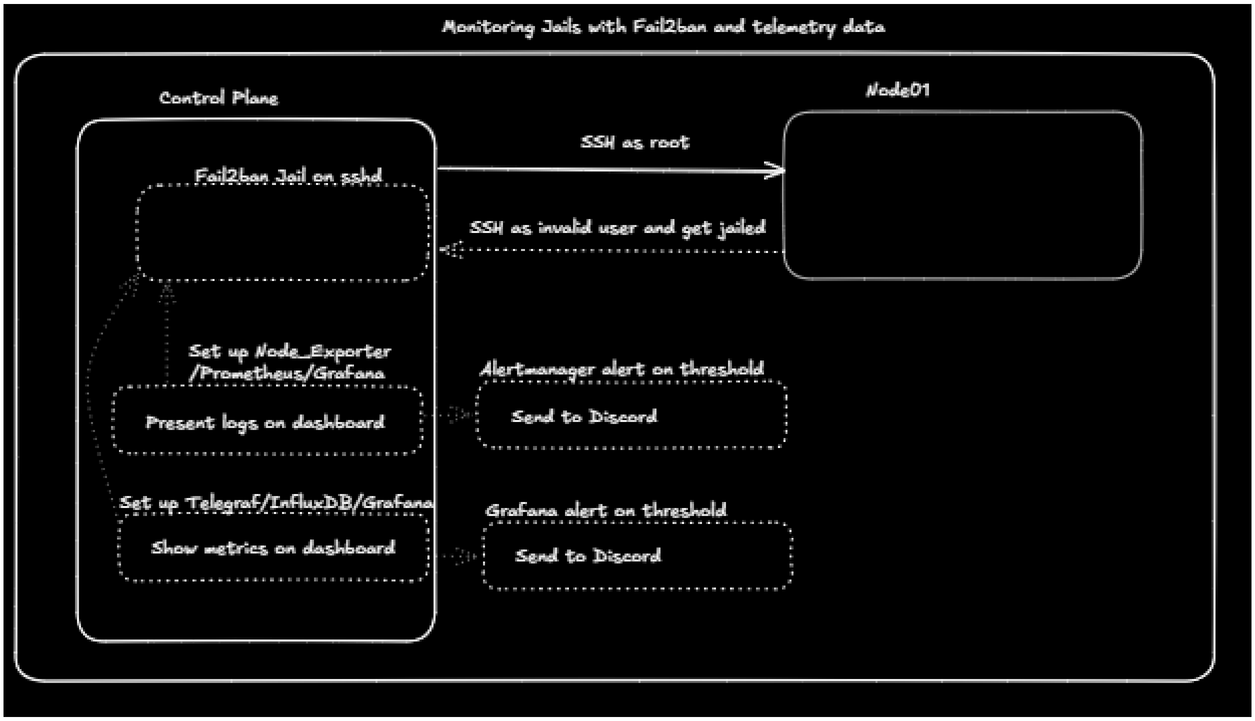
These labs focus on pulling metric information and then visualizing that data quickly on dashboards for real time analysis.

Monitoring Jails with Fail2ban logs


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

1. Complete the lab: https://killercoda.com/het-tanis/course/Linux-Labs/109-fail2ban-with-log-monitoring
    a. Were you able to see the IP address that was banned and unban it?
    b. Were you able to see all the NOTICE events in Grafana?
    c. What other questions do you have about this lab, and how might you go figure them out?

Monitoring Jails with Fail2ban and telemetry data


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 Node_Exporter /Prometheus/Grafana
Alertmanager alert on threshold
Present logs on dashboard
Send to Discord
Set up Telegraf/InfluxDB/Grafana
Grafana alert on threshold
Show metrics on dashboard
Send to Discord

1. Complete the lab here: https://killercoda.com/het-tanis/course/Linux-Labs/110-fail2ban-with-metric-alerting
    a. Do you see fail2ban in the Grafana Dashboard? If not, how are you going to troubleshoot it?
    b. Did you get your test alert and then real alert to trigger into the Discord channel?
    c. What other applications or uses for this could you think of? Do you have other places you could send alerts that would help you professionally?

Digging Deeper challenge (not required for finishing lab)

1. Review the alert manager documentation: https://prometheus.io/docs/alerting/latest/configuration/
    a. What are all the types of receivers you see?
    b. Which of the receivers do you have experience with?
2. Review the Grafana alert thresholds: https://grafana.com/docs/grafana/latest/panels-visualizations/configure-thresholds/
    a. Can you modify one of the thresholds from the lab to trigger into the discord?
        i. What is the relationship between critical and warning by default?