owlh_documentation Documentation

Release 0.17.x

owlh team

Nov 29, 2020

Contents

CHAPTER 1

Install OwlH

1.1 Install all-in-one system (AIO)

- how to deploy an all-in-one system

CHAPTER 2

OwlH Scenarios and main configurations

2.1 Basic deployment - All-in-one deployment

- how to deploy an all-in-one system

2.2 Software TAP Scenario

- How-to configure Software TAP Scenario

2.3 Wazuh Integration

- Configure OwlH as NIDS for Wazuh

CHAPTER 3

User Manual

3.1 Open Rules

- Suricata ruleset management - 3rd party and custom rulesets

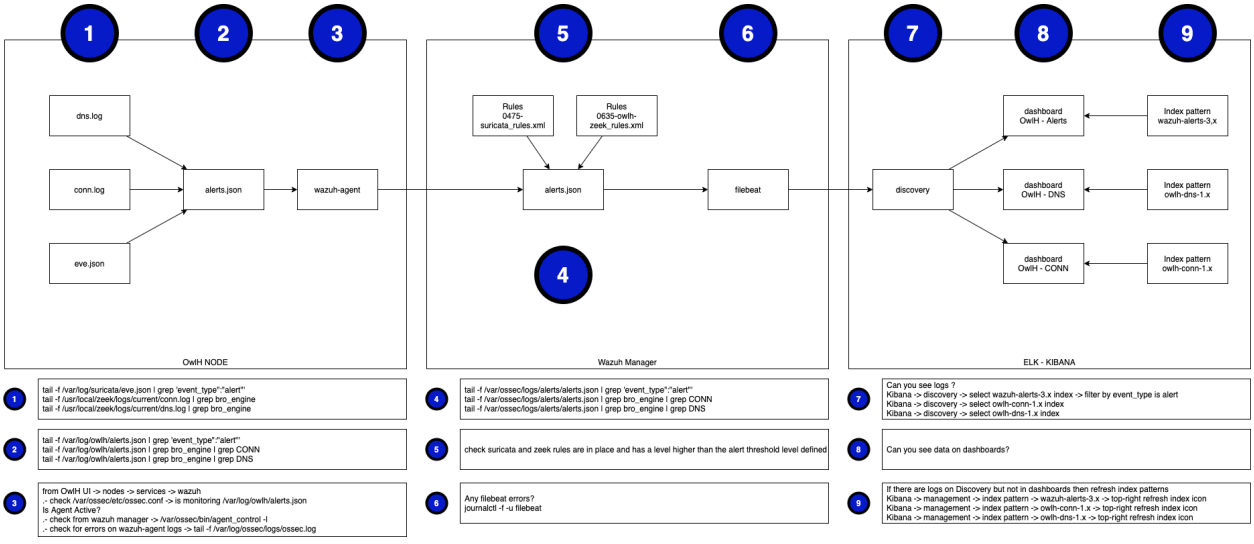
CHAPTER 4

Troubleshooting

Warning: work in progress. . .

Note: If you are missing something in this documentation, please say hello in our slack #doc channel and let us know what is missing or should be good to have.

- join OwlH slack - OwlH Slack workspace



4.1 OwlH Node

Suricata doesn't create alerts

4.2 OwlH Master

4.3 OwlH UI

4.4 OwlH Dashboards on Kibana

Can't see any alert on owlh-alert dashboard

- Check search owlh alert (discover -> open) is using wazuh-alerts-3.x, wazuh-alerts-4.x or wazuh-alerts-* depending on your Wazuh version. if you are running wazuh 3.x use wazuh-alerts-3.x. if running wazuh 4.x choose wazuh-alerts-*. Save, you should see now events in discovery, if any then your dashboard should work now.
- reload wazuh index pattern

CHAPTER 5

About OwlH

Current - v0.17.x

This picture will summarize the process we are working in.

5.1 If you need help

- email our support team - support@owlh.net
- join OwlH slack - OwlH Slack workspace
- ask for professional support and services - prohelp@owlh.net

OwlH - current v0.17.x

documentation last updated - Nov 29, 2020

- email our support team - support@owlh.net
- join OwlH slack - OwlH Slack workspace

documentation last updated - Nov 29, 2020