Setting up a secure logging and metrics platform

Werner Dijkerman

Setting up a secure logging and metrics platform

Building a secure platform for storing logging with Elasticsearch (incl. ECK Operator) and Prometheus with Thanos Query for metrics

Werner Dijkerman

This book is available at
https://leanpub.com/settingupasecureloggingandmetrics

This version was published on 2026-04-03

Tweet This Book!

Please help Werner Dijkerman by spreading the word about this book on Twitter!

The suggested tweet for this book is:

I now have a secure logging and/or metrics platform, by following the book "Setting up a secure logging and metrics platform" https://leanpub.com/settingupasecureloggingandmetrics via @leanpub

The suggested hashtag for this book is #Monitoring.

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

#Monitoring

Contents

Chapter 1: Introduction

Welcome and Guide Overview

Welcome to the "Setting up a secure logging and metrics platform" guide. In this guide we will build a secure and production-grade monitoring stack in Kubernetes. We will be using `Kind` as our Kubernetes platform, but you can use any other (cloud or on-premises) platform that you have access to. In Chapters 2 and 3 we will be using AWS, specifically an S3 bucket. If you do not have (or do not want to use) an AWS account, you can use MinIO instead. We will use Kind throughout this guide. Kind allows you to create a Kubernetes cluster locally on your machine. With Kind you can create and test the setup before applying it to a production environment, as you can remove the setup and rebuild it. This will help you gain experience with the solution, as you can also easily break it and practice fixing it.

What you will achieve

By the end of this guide you will have a fully secure, highly available logging and metrics platform with:

- Elasticsearch (ECK) + Logstash + Filebeat/Metricbeat for logs
- Prometheus + Thanos Query + Alertmanager for metrics
- Falco feeding runtime-security events into Elasticsearch and exposing metrics to Prometheus
- End-to-end TLS and mTLS between all components
- Network policies, persistent storage, and multi-AZ readiness patterns
- Ready-to-use Grafana dashboards and alerts
- A GitOps-ready repository with all YAML and Helm values

In this guide we will cover the following:

- Chapter 1: Introduction (this chapter)

- Chapter 2: Building a secure logging solution with the ECK operator
- Chapter 3: Metrics setup with Prometheus and Thanos Query
- Chapter 4: Alerts and visualizations

The main focus of this guide is security. We will configure all applications with TLS so that all communication is secure. In components that support it, we will also configure mTLS to enhance security. Where possible, we focus on automation by providing all configurations as YAML files. A Git repository containing all of the code used in this guide is available.

The code can be found here: https://github.com/dj-wasabi/setting-up-secure-logging-and-metrics-platform-guide I will keep this GIT repository up2date. I like code in GIT, thats why I use: If your sh*it isn't in GIt, it doest't exist!

In Chapter 2 we rely on some manual actions due to the lack of an Elasticsearch license. In Chapter 4 we will be using the data in our logging and/or metrics solution to create dashboards in Grafana and alerts.

Tooling

In this guide we will be using open-source tooling. In Chapter 2 we will build a logging platform using the ECK operator to deploy an Elasticsearch cluster, along with Logstash and Filebeat/Metricbeat. Even though these components are open source, configuring an Index Lifecycle Policy requires a license. We will therefore perform this step manually. If you have an Elasticsearch license, Appendix 2 shows how this can be achieved with full automation.

In Chapter 3 we will use Prometheus and its components, including Alertmanager, Node Exporter, and kube-state-metrics, to build our metrics solution. We will deploy Grafana as our dashboard tool, which we will also use in Chapter 4 when we talk about dashboards.

In both chapters we will deploy Falco as a runtime security tool. This allows us to gather security events as logs and store them in Elasticsearch. We will also configure Falco to expose metrics so they can be collected by our metrics solution. To achieve a fully secure setup, we will create and manage a large number of certificates using the cert-manager application.

Who and why

Why is this guide important? Much of the content available on the internet provides examples of how to set up a solution. It includes some basic explanations and examples of how to quickly achieve a working solution. However, for many people, and especially organisations, this is not enough. Security is more important than ever, and simply configuring a certificate in an Ingress and calling it secure is no longer sufficient. We want all connections to be secure, and that is what we will do in this guide.

When you are an ops, observability, or platform engineer tasked with building a secure logging and/or metrics solution, this guide is for you. I do assume you have a basic understanding of Kubernetes and the `kubectl` and Helm commands. We will first deploy our applications as you would normally see in blogs on the internet, with a certificate on the Ingress (or in our case the Gateway API). Then we will focus on configuring (m)TLS to have secure communication between the components so we go one step further. We will also apply network policies to make sure that not every tool can just access our solution. Once it is configured fully with (m)TLS, we apply some other security and availability configurations so our solution is highly available and spread over multiple zones.

I am not here to sell you a full-blown solution. I am a freelancer. The only thing I am selling is my knowledge and time (as you can hire me in case you are looking for someone ;-)). I am not trying to sell you an Elasticsearch solution or license or anything related to Prometheus. I am not sponsored in any way. I am writing about these tools because I have experience working with them. And I like these tools too, so I really don't mind working with them.

I have been working in IT for more than 20 years. I am a huge fan of automation, containerisation, monitoring, and cloud technologies. I strongly prefer not to perform tasks manually; ideally, I want to automate myself out of a job. My monitoring journey began with Nagios, which was very, lets say, interesting. I then moved on to Zabbix, where I created the Puppet module `wdijkerman/zabbix`, which gained significant traction and was later transferred to `voxpopli/zabbix` as I stopped working with Puppet. I also developed several Ansible roles for Zabbix under my `dj-wasabi` GitHub account, which were later moved into the `community.zabbix` collection and for a few years I helped maintaining it. I also gained hands-on experience building Elasticsearch clusters (initially small-scale setups for storing and viewing log events with

multiple clients) and gradually adopted Prometheus and Grafana as defacto standard monitoring tool. I might have used InfluxDB and Telegraf on a blue Monday, for which the later I created an Ansible role too.

I also use this as a learning opportunity to write a guide like this and maybe, in the future, a full book. I have been a technical reviewer for publishers like Packt, BPB Online, Manning, and O'Reilly on books about Terraform, Ansible, Zabbix, and the majority about Kubernetes. Instead of contacting one of these publishers, I am trying to see if I can write a bit about a topic. That is why I am writing this guide and publishing it on Leanpub. Who knows what might follow after this? :)

What is equally important as what we will do in this guide is what we will not be doing. This guide helps you reach a specific situation: building a secure, highly available logging and metrics solution. We will execute various commands and show code for resources and configurations to achieve that goal. We will not go into depth on f.e. what Elasticsearch or Prometheus is, how the internals work, or, in the case of Elasticsearch, how indexes work. This kind of depth is something that other books provide (better), and I recommend reading those books if you want to know the inner details.

AI

AI is booming at the moment. It can do a lot for us, and some may even think we will lose our jobs because of it. We already see a rise in content on the various platforms like Medium or Youtube that contains AI-generated information. **Not** this guide. All of the content in this guide is written by me, myself and I. However, as English is not my mother tongue, I have used AI to help me proofread and fix my typos and grammar. I am doing this all alone and do not have any department that can focus on this, so I have used AI for this.

But I also have used AI for my book cover. I had 2 screenshots, 1 from Grafana with Falco metrics and 1 from Kibana also with Falco events and asked to generate a book cover with these 2 screenshots. Maybe in a near future I will try to polish my Photoshop skills...

Why monitoring is important

You want to know how your infrastructure is performing, right? You want to know how your application is running, if it produces any errors, or provides any

other useful information to you or another team in your organisation. What if a Pod is started with incorrect settings and causes havoc in your cluster, you want to know that is happening. And that is what monitoring is. It is about getting the current state of your platform: are things "still okay"? Having one or more dashboards that tell you how much load there is on your platform, or seeing database connection errors and being able to relate that to your database consuming CPU resources. You want to know what is going on, at any moment of the day. You can only do that when you have a platform that you can rely on.

But what about observability? That is the same as monitoring, right? No. As said earlier, monitoring is about knowing how everything currently works and how it performs. It is based on the things we know in advance, like wanting to know about database connection errors. In our application we provided for example a `log.Error("database connection error")` in the code, so we get an error log when there is a database connection error. Or we create alerts in our system for situations that we can think of in advance when we should receive an alert.

Observability is the next step after monitoring. It is being able to understand any unexpected problem in the system, even if you did not plan for it in advance. You still need the logging and metrics information in your platform, but you need to be able to explore the data. Something that can help is adding traces in your application, which add telemetry. Telemetry (the combination of logs, metrics, and traces) lets you connect information across services and quickly understand issues that you could not have predicted. Even though it is a very interesting topic, this is outside of the scope for this guide. But the platform we are creating, will make observability possible if you want to add tracing or deeper analysis later on.

todo

Chapter 2: Building a secure logging solution with the ECK operator

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Introduction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Prerequisites & Architecture Overview

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

What You Need

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Architecture Overview

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Installing the ECK Operator

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Deploying the Core Elastic Stack

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Elasticsearch

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Kibana

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Logstash

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Data Collection Layer

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Security Foundations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Client TLS Authentication (Mutual TLS)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Elasticsearch

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Kibana

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Logstash

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Filebeat

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Enabling Network policies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Reflector

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

eck-operator

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Elasticsearch

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Kibana

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Logstash

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Filebeat

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Extending with Runtime Security Events

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Configuring Automated Snapshots & Backups

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Production ready

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Elasticsearch Prod

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Kibana Prod

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Logstash

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Filebeat prod

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Metricbeat prod

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

What We Deliberately Left Out

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Chapter 3: Metrics setup with Prometheus and Thanos Query

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Basic setup for metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Prometheus

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Thanos

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Network policies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Configuring TLS

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Small requirements for TLS

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

TLS For Prometheus

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Thanos TLS

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Adding Metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Cilium Metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Falco

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Configure for Production

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

What did we not do?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Central Thanos

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Scaling based on metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Authentication/Authorization

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Chapter 4: Alerts and visualizations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Appendix 1 Setting up Kind cluster

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Introduction

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Setup

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Kind

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Gateway API CRDs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Cilium

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Cert Manager

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Cert Manager CSI Driver

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Reflector

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Configuration

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

CA Certificate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Gateway

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.

Appendix 2 ILM

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/settingupasecureloggingandmetrics.