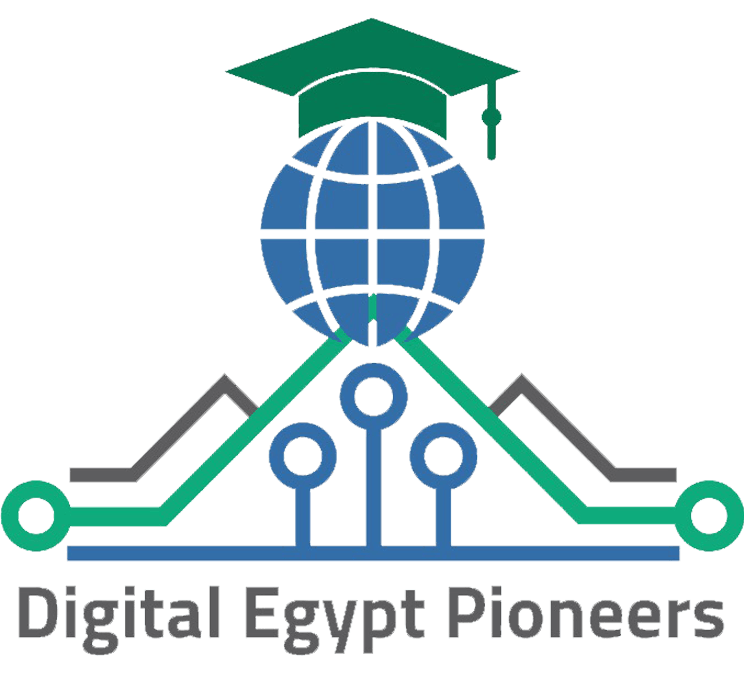
|  |
| --- |
| Close-up image showing the leaf-sides of two oversized books side-by-side on a bookshelf, with additional books in soft focus background |
| “ELK”  Log Management System |
| |  |  |  | | --- | --- | --- | | ELK Team | 4/1/25 | All About ELK | |



Cybersecurity Incident Response

Final Year Project

Implement a Centralized Log Management System Using ELK Stack

Presented By:

|  |  |
| --- | --- |
| *Mohamed Hesham* | *Ibrahem Mohamed* |
| *Khaled Mohamed*  *Mohamed Hassan* | *Ziyad Abbass* |

Supervised By:

*Eng.*

A P R I L – 2 0 2 5

# Contents

[Contents 2](#_Toc195610694)

[Chapter 1: 5](#_Toc195610695)

[1 Introduction 6](#_Toc195610696)

[1.1 Purpose of the Project 6](#_Toc195610697)

[1.2 Who We Are 6](#_Toc195610698)

[1.3 Tools and Techniques for the project 6](#_Toc195610699)

[1.3.1 Tools Used: 7](#_Toc195610700)

[1.3.2 Techniques: 7](#_Toc195610701)

[Chapter 2: 8](#_Toc195610702)

[2 Course Overview 9](#_Toc195610703)

[2.1 What is cybersecurity 9](#_Toc195610704)

[2.2 What is information security? 9](#_Toc195610705)

[2.3 Communications Security: CIA 9](#_Toc195610706)

[2.4 Threat, Vulnerability, and Risk 10](#_Toc195610707)

[2.5 Malware definition 11](#_Toc195610708)

[2.5.1 Malware types 12](#_Toc195610709)

[2.6 Ransomware 13](#_Toc195610710)

[2.6.1 WannaCry Ransomware 14](#_Toc195610711)

[2.6.2 Conti Ransomware 14](#_Toc195610712)

[2.7 Network 15](#_Toc195610713)

[2.7.1 Common Network Attacks 15](#_Toc195610714)

[2.7.2 Network Discovery 16](#_Toc195610715)

[2.7.3 Key Network Discovery Techniques 16](#_Toc195610716)

[2.7.4 Network Discovery Role in Incident Response 16](#_Toc195610717)

[2.7.5 Phases of Incident Response 17](#_Toc195610718)

[2.7.6 Cyber kill chain phases 18](#_Toc195610719)

[Chapter 3: 18](#_Toc195610720)

[3 ELK 19](#_Toc195610721)

[3.1 What Is the ELK Stack? 19](#_Toc195610722)

[3.1.1 A Short Recap: Why Is Log Management Important? 19](#_Toc195610723)

[3.1.2 Why Is the ELK Stack So Popular? 20](#_Toc195610724)

[3.2 ELK Logging: How to Use the Elastic Stack for Log Management, Analysis & Analytics 21](#_Toc195610725)

[3.3 What Is Elasticsearch? 23](#_Toc195610726)

[3.3.1 . Installing Elasticsearch 24](#_Toc195610727)

[3.4 Elasticsearch Queries 26](#_Toc195610728)

[3.4.1 Elasticsearch REST API 26](#_Toc195610729)

[3.4.2 Elasticsearch Plugins 26](#_Toc195610730)

[3.4.3 What Is Logstash? 26](#_Toc195610731)

[3.4.4 Installing Logstash 28](#_Toc195610732)

[3.4.5 What Is Kibana? 28](#_Toc195610733)

[3.4.6 Installing Kibana 29](#_Toc195610734)

[3.4.7 Installing Beats 30](#_Toc195610735)

[3.4.8 Shipping some data 31](#_Toc195610736)

[3.5 ELK Stack Use Cases & Applications 33](#_Toc195610737)

[3.5.1 Development and troubleshooting 34](#_Toc195610738)

[3.5.2 Application Performance Monitoring (APM) 34](#_Toc195610739)

[3.5.3 Security and Compliance 34](#_Toc195610740)

[3.5.4 Cloud Operations 35](#_Toc195610741)

[3.5.5 Business Intelligence (BI) 35](#_Toc195610742)

[3.5.6 SEO 36](#_Toc195610743)

[3.5.7 Generic Search 36](#_Toc195610744)

[3.5.8 Using Sematext as a Hosted ELK Solution 36](#_Toc195610745)

[3.5.9 What Do You Choose: Open Source ELK Stack or Commercial Tools? 37](#_Toc195610746)

[Chapter 4: 38](#_Toc195610747)

[4 Install Ubuntu Server 39](#_Toc195610748)

[4.1 Install & Configure Elastic Stack v8 39](#_Toc195610749)

[4.1.1 Download & Install Elastic Stack : 39](#_Toc195610750)

[4.1.2 Check Elastic service & Reset Elastic password: 39](#_Toc195610751)

[4.1.3 Configure Elastic Configuration File: 39](#_Toc195610752)

[4.1.4 Connect To Elastic Search Port: 40](#_Toc195610753)

[4.1.5 Enabled elasticsearch Start on Boot 40](#_Toc195610754)

[4.1.6 Enable SSL 40](#_Toc195610755)

[4.2 Create Certificate For Elastic : 40](#_Toc195610756)

[4.3 Enable Certificate in Elastic Configuration File : 41](#_Toc195610757)

[4.4 Install Kibana 41](#_Toc195610758)

[4.5 Install & Configure Kibana On Ubuntu 41](#_Toc195610759)

[4.5.1 Install Kibana : 41](#_Toc195610760)

[4.5.2 Adjust Kibana Startup Time : 43](#_Toc195610761)

[4.6 Install Fleet Server & File Beat 43](#_Toc195610762)

[4.6.1 Installing Elastic Agent : 43](#_Toc195610763)

[4.7 Install Winlogbeat Agent On Windows 45](#_Toc195610764)

[4.7.1 Enable Power shell Logging : 45](#_Toc195610765)

[4.7.2 Install Winlog Beat On Windows Client: 45](#_Toc195610766)

[4.7.3 Install Packet Beat Agent On Windows 46](#_Toc195610767)

[4.7.4 Install Elastic Security Endpoint On Windows 47](#_Toc195610768)

[Chapter 5: 49](#_Toc195610769)

[5 Rules 50](#_Toc195610770)

[5.1 What does the Rules page do? 50](#_Toc195610771)

[5.1.1 New Roles 51](#_Toc195610772)

**Chapter 1:**

System Overview

# Introduction

## Purpose of the Project

The purpose of this project is to implement a centralized log management system using the ELK Stack (Elasticsearch, Logstash, and Kibana) in order to effectively collect, parse, analyze, and visualize logs from various network devices. This solution aims to enhance network visibility, support security monitoring, and improve incident detection and response through real-time dashboards and alerting

## Who We Are

We are a dedicated Security Operations Center (SOC) team specializing in the monitoring, analysis, and response to cybersecurity incidents. Our approach is rooted in industry best practices, with a strong emphasis on proactive threat detection and incident management.

We follow the Cyber Kill Chain framework, ensuring that each incident is handled through a structured process involving the four key phases:

Detection, Containment, Eradication, and Recovery.

This methodology enables us to minimize the impact of security threats and strengthen the organization’s overall cyber defense posture

## Tools and Techniques for the project

In this project, we employed a variety of tools and techniques to build an efficient and scalable Centralized Log Management System using the ELK Stack and additional log forwarding agents.

### Tools Used:

**ELK Stack:**

* Elasticsearch: used for indexing and storing large amounts of log data in a searchable format.
* Kibana: utilized to visualize the logs and create dashboards that help monitor security events in real-time.
* File beat: deployed on Kali Linux and Windows clients to collect logs and send them to Logstash for further processing.
* Packet beat: used to capture network traffic data and provide deeper insights into communication patterns.
* Wingbeat: installed on Windows clients to collect logs from Windows environments and forward them to the central logging system.
* Fleet Agent: configured to manage multiple Beats (File beat, Packet beat, win beat) efficiently for seamless log collection across different systems.
* Elastic Stack Setup: utilized to integrate all these tools effectively for end-to-end log management.

### Techniques:

* Log Collection and Forwarding: using Beats (Filebeat, Packetbeat, and Winbeat) to collect logs from various network devices (servers, firewalls, and routers) and forward them to Logstash.
* Custom Log Parsing and Transformation: developed custom parsing rules in Logstash to normalize and categorize the logs for meaningful analysis.
* Real-time Log Visualization: created interactive Kibana dashboards to visualize security events and track potential incidents in real-time.
* Security Event Correlation: configured Elasticsearch queries to identify patterns and correlate events for incident detection.
* Alerting: set up thresholds and alerts for critical security events (e.g., unauthorized access attempts or anomalies) to ensure quick response.

This comprehensive approach using the ELK Stack, Beats agents, and various parsing techniques enabled us to effectively monitor, analyze, and visualize network security logs, enhancing the overall security posture

**Chapter 2:**

Course Overview

# Course Overview

## What is cybersecurity

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

## What is information security?

Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information.

This includes policy settings that prevent unauthorized people from accessing business or personal information it also protect data at rest , motion and use.

## Communications Security: CIA

Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

**CIA Triad**

The CIA triad consists of three components of information security:

* **Confidentiality -** Only authorized individuals, entities, or processes can access sensitive information.
* **Integrity -** This refers to the protection of data from unauthorized alteration.
* **Availability -** Authorized users must have uninterrupted access to the network resources and data that they require.

## Threat, Vulnerability, and Risk

Attackers wants to access our assets such as data and other intellectual property, servers, computers, smart phones, tablets, and so on.

|  |  |
| --- | --- |
| **TERM** | **EXPLANATION** |
| Threat | A potential danger to an asset such as data or the network itself. |
| Vulnerability | A weakness in a system or its design that could be exploited by a threat. |
| Attack Surface | An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system. |
| Exploit | The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local.A remote exploit is one that works over the network without any prior access to the target system. In a local exploit, the threat actor has some type of user or administrative access to the end system. It does not necessarily mean that the attacker has physical access to the end system. |
| Risk | The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence. |



## Malware definition

* Malware is a code or software designed to damage, disrupt, steal, or do illegitimate action on data, hosts, or networks.
* A diagram of a computer

  AI-generated content may be incorrect.The three most common types of malware are **Virus**, **Worm**, and **Trojan horse**.

### Malware types

|  |  |
| --- | --- |
| **Malware Type** | **Description** |
| Virus | Attaches to legitimate programs or files and spreads when the infected file is executed. |
| Worm | Self-replicates and spreads across networks without user interaction. |
| Trojan | Disguises itself as legitimate software but contains malicious code to perform unauthorized actions. |
| Spyware | Secretly monitors and collects user information, often for surveillance or data theft. |
| Adware | Displays unwanted advertisements on the user's device, often slowing down performance. |
| Ransomware | Encrypts files or locks users out of their system until a ransom is paid. |
| Rootkit | Grants attackers administrative-level control over a system while remaining hidden. |

## Ransomware

* Ransomware is a malware that denies access to the infected computer system or its data.
* Ransomware frequently uses an encryption algorithm to encrypt system files and data.
* Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
* Social engineering is also used, when cybercriminals pretending to be security technicians
* make random calls at homes and persuade users to connect to a website that downloads ransomware to the user’s computer



### WannaCry Ransomware

### Conti Ransomware

* **What is Conti Ransomware?**

Conti is a highly sophisticated ransomware strain first identified in early 2020, known for its rapid deployment and extensive use of double extortion tactics, where data is both encrypted and threatened with public release.

* **Key Characteristics:**

**Targeted Attacks:** Primarily focuses on high-value targets, including enterprises and critical infrastructure.

**Speed and Efficiency:** Capable of encrypting thousands of files in a matter of minutes.

**Communication:** Operates as a Ransomware-as-a-Service (RaaS), allowing affiliates to conduct attacks while the Conti group manages the backend.

**Notable Incidents:** in 2021, Conti attacked the Irish Health Service, disrupting healthcare services and leading to significant financial losses.

* **Attack Vector:**

Often gains initial access through phishing emails, exploiting vulnerabilities, or using Remote Desktop Protocol (RDP).

## Network

### Common Network Attacks

|  |  |
| --- | --- |
| **Attack Type** | **Description** |
| Man-in-the-Middle Attack | Attacker intercepts and potentially alters communication between two parties. |
| Buffer Overflow Attack | Exploits a system by overloading a buffer to execute malicious code. |
| DoS Attack | Denies legitimate users access to a resource by overwhelming the system with traffic. |
| DDoS Attack | Similar to DoS but launched from multiple compromised devices to flood a target. |
| ICMP Attack | Exploits ICMP protocol (Ping) to overwhelm the target with echo requests. |

### Network Discovery

Definition: Network discovery is the process of identifying devices, services, resources, and vulnerabilities on a network.

Importance: Provides visibility into network assets and vulnerabilities. Essential for security assessments, vulnerability management, and compliance.

Helps in network planning, management, and optimization.

### Key Network Discovery Techniques

#### Active Scanning

Description: Sends packets to various IP addresses to discover devices and open ports.

Tools: Nmap, Angry IP Scanner

#### Passive Scanning

Description: Monitors network traffic to identify devices and services without active probing.

Tools: Wireshark, PRTG Network Monitor

#### Network Mapping

Description: Creates a visual representation of the network topology to identify potential vulnerabilities.

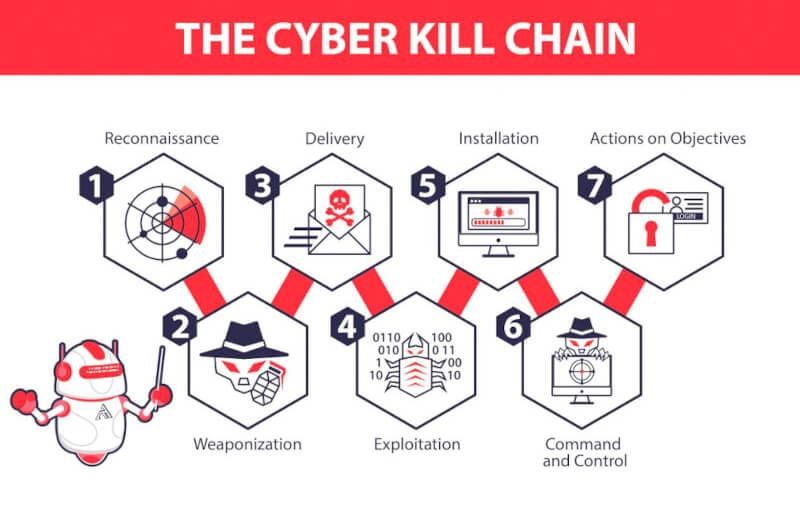
Tools: SolarWinds Network Topology Mapper

### Network Discovery Role in Incident Response

* **Initial Assessment**: Quickly identifies affected devices and the scope of the incident.
* **Forensic Analysis**: Helps trace back the attack path and understand the impact.
* **Vulnerability Assessment**: Facilitates identifying unpatched systems and vulnerable services during a response.
* **Continuous Monitoring:** Regularly use network discovery techniques to stay ahead of threats.
* Integration with SIEM: Incorporate findings into Security Information and Event Management (SIEM) systems for better incident response.
* **Documentation:** Keep detailed records of network configurations and changes for forensic readiness.

### Phases of Incident Response

### Cyber kill chain phases



**Chapter 3:**

**ELK**

# ELK

## What Is the ELK Stack?

The ELK stack is an acronym used to describe a collection of three open-source projects – Elasticsearch, Logstash, and Kibana. Elasticsearch is a full-text search and analytics engine. Logstash is a log aggregator that collects and processes data from multiple sources, converts, and ships it to various destinations, such as Elasticsearch. And finally, Kibana provides a user interface, allowing users to visualize, query, and analyze their data via graphs and charts.

Recently, however, a fourth project was added to the mix – Beats – which led to the stack being rebranded as the Elastic Stack. Beats is a family of lightweight data shippers that collect and send data from different machines and systems to the stack, in this case, to Logstash or Elasticsearch.

Although all four are independent projects run by Elastic, they were designed to complete each other into an end-to-end log analysis solution.

Thus, ELK is a log management platform that works by enabling you to gather massive amounts of log data from anywhere across your infrastructure into a single place, then search, analyze and visualize it in real time. Among the most common ELK use cases, we can name monitoring, troubleshooting, web analytics, risk management, business intelligence, compliance, fraud detection and security analysis.

### A Short Recap: Why Is Log Management Important?

Competitors are always ready to grab one of your unhappy customers. On the other hand, while it’s easy to lose clients, it’s getting harder and harder to make sure apps are available, performant, and secure at all times.

You can get the necessary information by analyzing logs. However, the architecture of the environments generating these logs has evolved into microservices, containers, and orchestration infrastructure deployed on the cloud, across clouds or in hybrid clouds. As you move more and more of your IT infrastructure to the cloud, you build highly distributed and dynamic environments that are more difficult to monitor. Data is everywhere across your infrastructure, in different formats and sometimes, even difficult to locate and manage.

That’s where log management tools such as the ELK stack come in. Their main capabilities – collection, aggregation, search and analysis, monitoring and alerting, and visualization and reporting – that help SREs, IT Operations, or DevOps keep an eye on application and infrastructure performance, gather meaningful insights and make better data-driven decisions.

Further reading:

• 10+ Best Practices for efficient logging and monitoring

• 5 Benefits to run Elastic Stack in the Cloud

### Why Is the ELK Stack So Popular?

The ELK stack is popular because it fulfills a need in the log management and analytics space. In cloud-based environments, performance isolation is extremely difficult to reach. Specific loads, infrastructure servers, environments and the number of active users are just a few of the factors that influence the performance of virtual machines in the cloud. However, ELK and other similar platforms can help with such infrastructure problems, as well as Linux log files or other operating system logs, NGINX and IIS server logs.

ELK has definitely set itself apart as one of the best log management solutions by constantly improving the stack to meet customers’ demands, as evidenced by the recent addition of Beats. ELK is open-source and, as one of the oldest tools available, it has gathered a large community of enthusiasts that drive innovation and new features and offer help when needed. Not to mention, with an open-source tool, you don’t depend on a vendor.

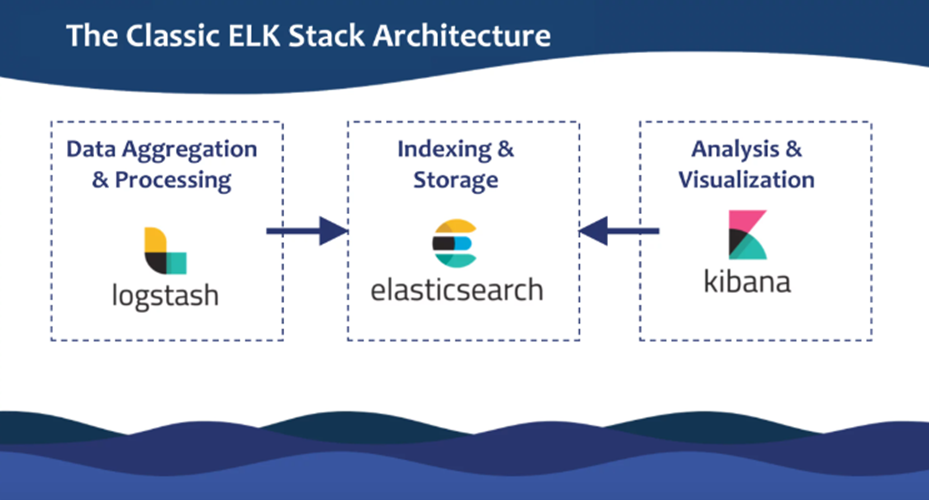
And lastly, ELK is just that of a powerful platform. Simple and robust, it can manage large volumes of data and it can further scale as data grows without any bumps in performance. Compared to Splunk, it has fewer functionalities, but you don’t need all the analytical capabilities offered by Splunk to do your job. You can do just as well with ELK.

On the other hand, you can update from free and open-source to a paid version of ELK that makes it just as pricey. It’s called Elastic Stack Features (formerly X-Pack) and extends the basic setup with ELK has the option of extending its capabilities. However, just as ELK is a great Splunk alternative, there are some great alternatives for each “Elastic Stack Features” component.

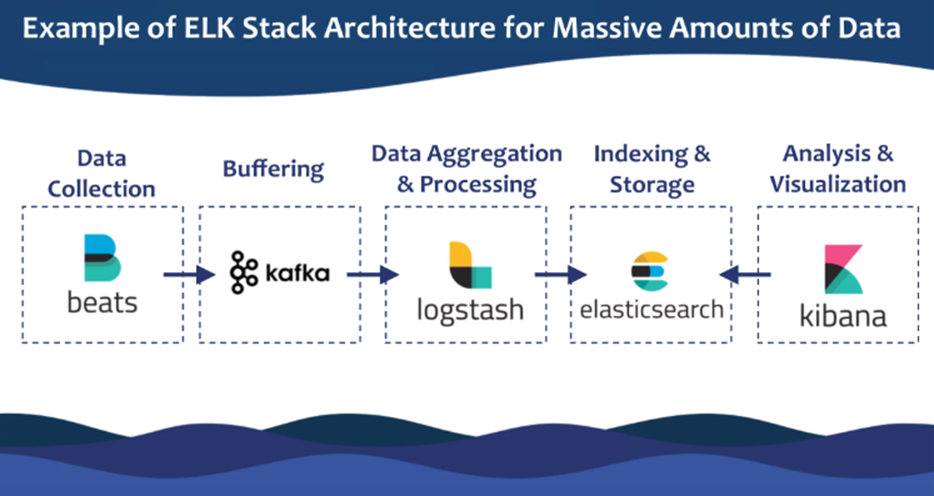
## **ELK Logging: How to Use the Elastic Stack for Log Management, Analysis & Analytics**

Depending on the use case and environment, businesses require different logging architectures.

For small environments, the classic ELK stack architecture is more than enough. It would look as follows:



On the other hand, when you work with massive amounts of data, you will, more than likely, need additional components. For example, you may want to use Apache Kafka for buffering:



A full-production grade architecture will more than likely, have multiple Elasticsearch nodes, maybe even multiple Logstash instances, an alerting plugin, and an archiving mechanism.  
That is why, before setting up your stack, you should be clear about your use case. This will influence where and how you install the stack, how you configure your Elasticsearch cluster, how you allocate resources, and many more.

Now that you know how your ELK logging stack should look like, let’s start with the basics and see in detail what each of the ELK components – Elasticsearch, Logstash, Kibana, and Beats – do:

## What Is Elasticsearch?

You’ve probably heard of Elasticsearch before the ELK, right? That’s because Elasticsearch is the most popular search engine available today and, practically, the heart of the Elastic Stack; so much so, that people use it as a synonym for the name of the stack itself.

Elasticsearch is a free and open-source search and analytics engine based on the Apache Lucene library that was first released in 2010. It’s equipped with a rich and powerful HTTP RESTful API that enables you to perform fast searches in near real-time. Elasticsearch is developed in Java, supporting clients in many different languages, such as PHP, Python, C#, and Ruby.

In the context of using ELK as a tool for log management and analytics, Elasticsearch oversees indexing and storing data. You can read more about Elasticsearch in our Elasticsearch tutorial, from basic concepts to how it works, the benefits of using Elasticsearch, and use cases.

And since you’re starting with the ELK, check out this presentation where our colleagues cover how to do log analysis with Elasticsearch and what you shouldn’t do when working with Elasticsearch in Top 10 Elasticsearch mistakes

### . Installing Elasticsearch

First, you need to add Elastic’s signing key so that the downloaded package can be verified (skip this step if you’ve already installed packages from Elastic):

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add –

For Debian, we need to then install the apt-transport-https package:

sudo apt-get update sudo apt-get install apt-transport-https

The next step is to add the repository definition to your system:

echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

To install a version of Elasticsearch that contains only features licensed under Apache 2.0 (aka OSS Elasticsearch):

echo "deb https://artifacts.elastic.co/packages/oss-7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list

All that’s left to do is to update your repositories and install Elasticsearch:

sudo apt-get update sudo apt-get install elasticsearch

Elasticsearch configurations are done using a configuration file that allows you to configure general settings (e.g. node name), as well as network settings (e.g. host and port), where data is stored, memory, log files, and more.

For our example, since we are installing Elasticsearch on AWS, it is a good best practice to bind Elasticsearch to either a private IP or localhost:

sudo vim /etc/elasticsearch/elasticsearch.yml network.host: "localhost" http.port:9200 cluster.initial\_master\_nodes: ["<PrivateIP"]

To run Elasticsearch, use:

sudo service elasticsearch start

To confirm that everything is working as expected, point curl or your browser to http://localhost:9200, and you should see something like the following output:

{ "name" : "ip-172-31-10-207", "cluster\_name" : "elasticsearch", "cluster\_uuid" : "bzFHfhcoTAKCH-Niq6\_GEA", "version" : { "number" : "7.1.1", "build\_flavor" : "default", "build\_type" : "deb", "build\_hash" : "7a013de", "build\_date" : "2019-05-23T14:04:00.380842Z", "build\_snapshot" : false, "lucene\_version" : "8.0.0", "minimum\_wire\_compatibility\_version" : "6.8.0", "minimum\_index\_compatibility\_version" : "6.0.0-beta1" }, "tagline" : "You Know, for Search" }

Installing an Elasticsearch cluster requires a different type of setup. Read our Elasticsearch Cluster tutorial for more information on that.

## Elasticsearch Queries

When getting started with Elasticsearch, one of the first things you should dive into is the query syntax as it will be of great help along the way. Learn more about queries in our Elasticsearch cheat sheet, as well as other core Elasticsearch operations such as index creation, deletion, mapping manipulation, and more.

### Elasticsearch REST API

Since you’re getting started with Elasticsearch, you should be familiar with the most common APIs – Document API, Search API, Indices API, Cluster API, and cat API.

### Elasticsearch Plugins

Last but not least, Elasticsearch functionality can be extended with plugins to better suit your needs. There are many types of plugins you may care about, such as alerting, analysis, API extension, discovery, ingest, management, mapper, security, snapshot/restore, and store plugins. You can learn how to install them here.

Read more on Elasticsearch:

• Top 10 Elasticsearch metrics to monitor

• Elasticsearch security: Authentication, encryption, backup

Now you know what Elasticsearch does, but not how you get data to Elasticsearch. Enter Logstash.

### What Is Logstash?

You can’t do log analysis on unstructured logs. Or better said, you can but with great expense of time and energy. That’s why tools like Logstash are indispensable in the space of log management and analytics.

Logstash is a free and open-source log aggregator and processor that works by reading data from many sources and sending it to one or more destinations for storage or stashing – in this case, when using ELK for data analytics, to Elasticsearch. However, along the way, data is processed by filtering, massaging and shaping it to reach a uniform and structured view. Logstash is equipped with ready-made inputs, filters, codecs, and outputs, to help you extract relevant, high-value data from your logs.

Similar to Elasticsearch, Logstash too has a rich library of plugins, allowing it to collect, convert, and enrich various log types, from system logs to web server logs, error logs, and app logs.

Learn more about how to install and use Logstash from our Logstash tutorial, where we also talk about Logstash monitoring, best practices, and walk you through a Logstash configuration example to help you understand the basics in under 5 minutes!

Logstash is one of the best and easy to use logging tools, but there are some other good options available too, such as Fluentd, rsyslog, syslog-ng, or Filebeat, which we discuss in our article about Logstash alternatives. Logagent is our own modern, open-source, lightweight data shipper that allows you to ship logs to Elasticsearch – you can see how Logagent compares to other log shippers.

If you want to learn more about Logstash and how it works, you might also be interested in:

• Parsing and centralizing Elasticsearch logs with Logstash

• How to: Logstash to Kafka to rsyslog

• Sending your Windows event logs to Sematext using NxLog and Logstash

• Handling multiline stack traces with Logstash

• Elasticsearch ingest node vs. Logstash performance

• Recipe: Reindexing Elasticsearch documents with Logstash

At this point, your log data is collected and stored in a single location, but you can’t use it since you can’t see it, much less monitor or query it. At least, not without Kibana.

### Installing Logstash

Logstash requires Java 8 or Java 11 to run so we will start the process of setting up Logstash with:

sudo apt-get install default-jre

Verify java is installed:

java -version openjdk version "1.8.0\_191" OpenJDK Runtime Environment (build 1.8.0\_191-8u191-b12-2ubuntu0.16.04.1-b12) OpenJDK 64-Bit Server VM (build 25.191-b12, mixed mode)

Since we already defined the repository in the system, all we have to do to install Logstash is run:

Before you run Logstash, you will need to configure a data pipeline. We will get back to that once we’ve installed and started Kibana.

### **What Is Kibana?**

Kibana is a free and open-source analysis and visualization layer that works on top of Elasticsearch and Logstash. It’s actually the preferred choice for visualizing logs stored in Elasticsearch. Kibana makes it really easy to search, analyze, and visualize large volumes of data, as well as to detect trends and patterns. The dashboard features various interactive charts and allows for customization, depending on what team in your company uses it – yes, ELK logging is useful for BizOps as well!

### Installing Kibana

As before, we will use a simple apt command to install Kibana:

sudo apt-get install kibana

Open the Kibana configuration file at: /etc/kibana/kibana.yml, and make sure you have the following configurations defined:

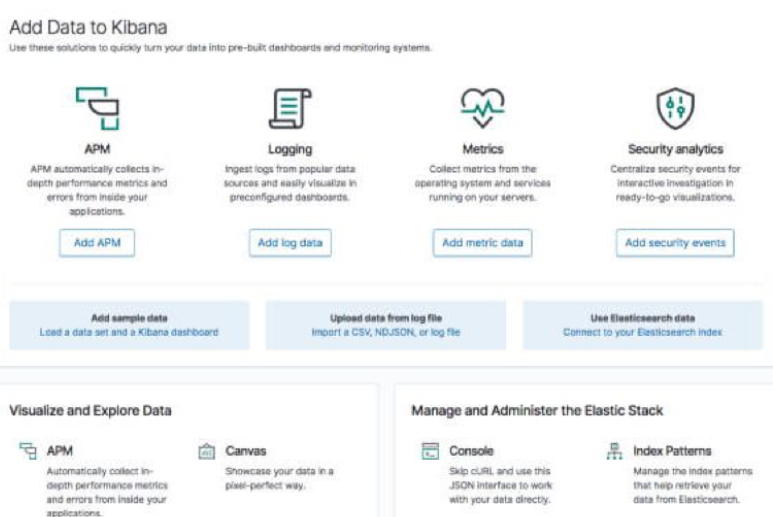
server.port: 5601 elasticsearch.url: "http://localhost:9200"

These specific configurations tell Kibana which Elasticsearch to connect to and which port to use.

Now, start Kibana with:

sudo service kibana start

Open up Kibana in your browser with: http://localhost:5601. You will be presented with the Kibana home page.



### Installing Beats

The various shippers belonging to the Beats family can be installed in exactly the same way as we installed the other components.

As an example, let’s install Metricbeat:

sudo apt-get install metricbeat

To start Metricbeat, enter:

sudo service metricbeat start

Metricbeat will begin monitoring your server and create an Elasticsearch index which you can define in Kibana. In the next step, however, we will describe how to set up a data pipeline using Logstash.

### Shipping some data

For the purpose of this tutorial, we’ve prepared some sample data containing Apache access logs that is refreshed daily.

Next, create a new Logstash configuration file at: /etc/logstash/conf.d/apache-01.conf:

sudo vim /etc/logstash/conf.d/apache-01.conf

Enter the following Logstash configuration (change the path to the file you downloaded accordingly):

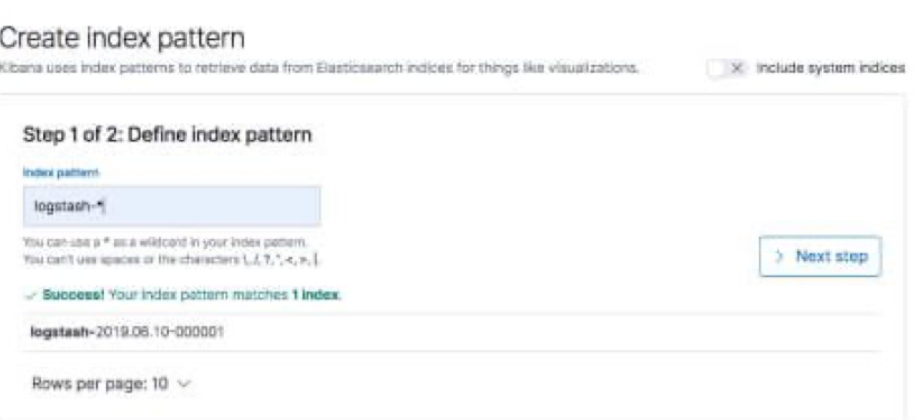
input { file { path => "/home/ubuntu/apache-daily-access.log" start\_position => "beginning" sincedb\_path => "/dev/null" } } filter { grok { match => { "message" => "%{COMBINEDAPACHELOG}" } } date { match => [ "timestamp" , "dd/MMM/yyyy:HH:mm:ss Z" ] } geoip { source => "clientip" } } output { elasticsearch { hosts => ["localhost:9200"] } }

Start Logstash with:

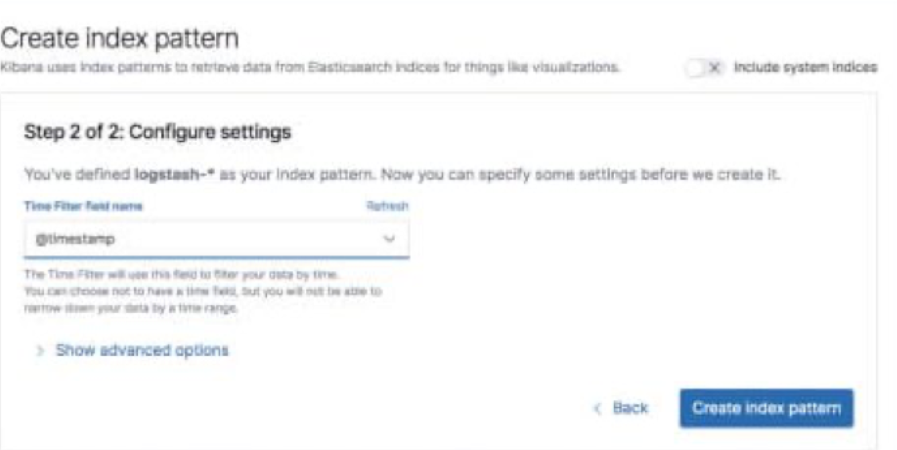
sudo service logstash start

If all goes well, a new Logstash index will be created in Elasticsearch, the pattern of which can now be defined in Kibana.

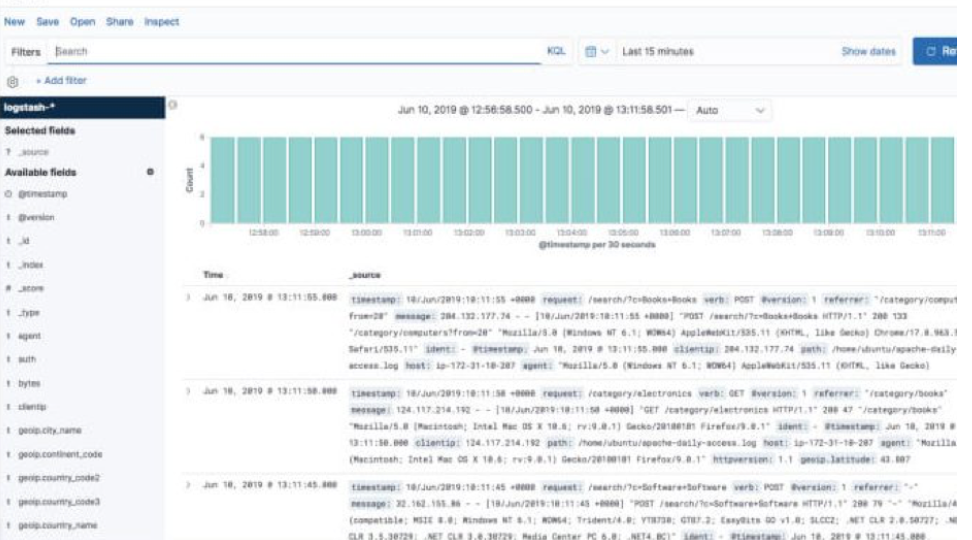
In Kibana, go to Management → Kibana Index Patterns. Kibana should display the Logstash index and along with the Metricbeat index if you followed the steps for installing and running Metricbeat).



Enter “logstash-\*” as the index pattern, and in the next step select @timestamp as your Time Filter field.



Hit Create index pattern, and you are ready to analyze the data. Go to the Discover tab in Kibana to take a look at the data (look at today’s data instead of the default last 15 mins).



Congratulations! You have set up your first ELK data pipeline using Elasticsearch, Logstash, and Kibana.

## ELK Stack Use Cases & Applications

You’ve probably caught on that the ELK stack is most commonly used as a log analysis tool for various use cases and purposes – from monitoring and troubleshooting to security and compliance, SEO and business intelligence.

As already mentioned, make sure you have a very good understanding of your use case before setting up your ELK stack. Here are a few ideas of what is the ELK stack most used for:

### Development and troubleshooting

While log management is great for monitoring performance and troubleshooting, you can actually leverage itearlier than that, in the development phase of the application’s lifecycle.

When implementing logging in the code, developers can correlate, identify and solve errors and exceptions – in testing or staging. You collect logs into the ELK, ship them to a centralized location then push them to production. Once there, the Kibana dashboards make it easier and faster for you to monitor, analyze and troubleshoot.

Medium, a platform that receives 25 million unique readers and thousands of published posts per week, uses the ELK stack to debug their production issues.

### Application Performance Monitoring (APM)

With modern apps, it’s critical to monitor performance metrics for each component in your architecture. How does the ELK fit into the picture?

Although it wasn’t designed to store metrics, Elasticsearch is used by many for that specific purpose. You can ship such data to Elasticsearch or Logstash with Metricbeat, thus making ELK an alternative to other basic APM tools. If you need to look even deeper into application performance, you can use open source distributed tracing tools such as Jaeger and Zipkin or commercial ones like Sematext Tracing.

Linkedin is one of the big names that use ELK to monitor performance. Moreover, they integrated with Kafka to support their load in real-time.

### Security and Compliance

With the number of cyberattacks increasing, companies are forced to meet more and more compliance regulations such as HIPAA, FISMA, SOC, or PCI. As such, they need to have a reliable security mechanism in place.

The ELK stack brings together the data that paints a clear picture of your overall IT security, more specifically, who does what with your app or system in real time. For example, you can aggregate Linux audit logs in Elasticsearch to monitor systems for suspicious activity. This makes ELK great for SIEM.

Netflix uses ELK for security purposes, as well as for monitoring and analyzing customer service-related operations.

### Cloud Operations

Unlike conventional environments, cloud and hybrid environments are multilayered and distributed, making them much more difficult to manage. This raises questions such as how to access each machine, how to collect and process it, where to store it and for how long, how to analyze, secure, and backup the data.

ELK, with all its four components, can cover all of them. Beats is installed on each machine to forward data to Logstash. Logstash normalizes it and ships it to Elasticsearch where is indexed and stored. And, finally, Kibana’s dashboards and visualizations help you analyze, detect anomalies, troubleshoot, and prevent security-related issues.

### Business Intelligence (BI)

Business intelligence refers to the process of leveraging technologies, software, applications, tools, and best practices to turn raw data into actionable insights that help make better data-driven business decisions and improve performance and collaboration.

The ELK stack is great for processing big data. The ELK stack collects raw data from multiple sources such as supply chain, manufacturing data, databases, personnel records, sales, and marketing campaigns, and many others. Understanding your customers and their online behavior better and how they are accessing your website are just of few of the benefits of using Elastic logging for this purpose.

### SEO

By using the ELK stack, you can leverage web server access logs to increase the relevancy and visibility of your site. They allow you to see who’s visiting your website, both people and the bots used by search engines to crawl the site. Keeping an eye for bots belonging to Google, Yahoo, Baidu, Yandex, and any other such platform helps SEO specialists to detect when bots crawled the site, optimize the crawl budget, monitor website errors, and faulty redirects, and many more.

### Generic Search

Even though ELK is mostly used for log aggregation and log analysis, one of the use cases, for the stack can also be generic search – searching through a website for example – by leveraging reverse indexing.

Github, Wikipedia, and Stack Overflow are just a few of the companies that use ELK for their searching and filtering features.

### Using Sematext as a Hosted ELK Solution

We offer ELK as a service to make it easier for you to focus on productive work instead of managing the stack. Just ship your logs to Sematext Logs and it will make them accessible for you in real-time via a simple and intuitive user interface.

You can see logs and errors as they stream in from however many data sources you may have. Sematext Logs handles massive amounts of data without blinking an eye. It further allows you to set up alerts on both logs and metrics. On top of that, there’s anomaly detection, which also works across both logs and metrics.

Sematext Logs adds a security blanket around your logs with TLS/SSL encryption and multi-user RBAC (Role-Based Access Control) which allows you to give access to an unlimited number of users, as well as revoke their privileges when you need to.

Sematext Logs features sophisticated searching and filtering capabilities along with syslog support to make it easier for you to identify and troubleshoot issues before they affect your users, and spot opportunities to drive business growth.

### What Do You Choose: Open Source ELK Stack or Commercial Tools?

As your company grows, so is the volume of data. If you’re looking for a good, scalable, and affordable log management and analysis solution to help make sense of your logs, the ELK stack is the one for you. It has impressive features that can very well compete with those of commercial tools. Not to mention, you may not even need them.

Commercial tools, like Sematext Cloud, give you a fast start. You don’t have to learn or worry about Elasticsearch or any of the features on top, such as access control. This way, you have more time to grow your business.

On the other hand, if ELK is closer to the core of your business it might be worth growing your ELK and scale it, along with the operations team. To help you on this route, Sematext offers ELK trainings, consulting, and production support.

Nevertheless, remember that your organization requirements and your use case dictate the kind of tool you need and, if you choose ELK, the architecture setup as well.

**Chapter 4:**

Ubuntu Server

# Install Ubuntu Server

Installing Ubuntu Server provides a stable, secure, and flexible operating system for running web servers, databases, applications, and other services. It's lightweight, open-source, and widely used for hosting servers in both production and development environments.

## Install & Configure Elastic Stack v8

Installing and configuring Elastic Stack v8 provides you with a powerful system for collecting and analyzing logs, monitoring cybersecurity, and creating dashboards — all from one central platform.

### Download & Install Elastic Stack :

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

sudo apt-get install apt-transport-https

echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

sudo apt-get update && sudo apt-get install elasticsearch

### Check Elastic service & Reset Elastic password:

systemctl start elasticsearch

systemctl status elasticsearch

cd /usr/share/elasticsearch/bin

./elasticsearch-reset-password -i -u elastic

### Configure Elastic Configuration File:

sudo nano /etc/elasticsearch/elasticsearch.yml

cluster.name: my\_network (Optional)

network.host: elkserver (Real Host Name)

http.port: 9200 (Do Not Change)

### Connect To Elastic Search Port:

ss -ntpl

https://192.168.1.243:9200

### Enabled elasticsearch Start on Boot

sudo systemctl enable elasticsearch

sudo systemctl start elasticsearch

sudo systemctl status elasticsearch

### Enable SSL

Enabling SSL provides a fundamental layer of security for any environment using Elastic Stack, ensuring that communication between all components is secure and encrypted.

#### Create CA File :

cd /usr/share/elasticsearch/bin

sudo ./elasticsearch-certutil ca --pem --out /etc/elasticsearch/certs/ca.zip

cd /etc/elasticsearch/certs

apt install unzip

sudo unzip ca.zip

## Create Certificate For Elastic :

cd /usr/share/elasticsearch/bin

sudo ./elasticsearch-certutil cert --out /etc/elasticsearch/certs/elastic.zip --name elastic --ca-cert /etc/elasticsearch/certs/ca/ca.crt --ca-key /etc/elasticsearch/certs/ca/ca.key --dns elastic --pem

cd /etc/elasticsearch/certs

sudo unzip elastic.zip

## Enable Certificate in Elastic Configuration File :

sudo nano /etc/elasticsearch/elasticsearch.yml

Comment #keystore.path: certs/http.p12

enabled: true

certificate: certs/elastic/elastic.crt

key: certs/elastic/elastic.key

certificate\_authorities: certs/ca/ca.crt

cd /etc/elasticsearch

ls -alh certs/ca

chown -R elasticsearch:elasticsearch .

ls -alh certs/ca

sudo systemctl restart elasticsearch.service

sudo systemctl status elasticsearch.service

## Install Kibana

Kibana helps you visually view and analyze data stored in Elasticsearch by creating custom dashboards, analyzing time-based data, and enabling advanced search. It also allows you to create and share reports, making it easier to understand data and make informed decisions.

## Install & Configure Kibana On Ubuntu

### Install Kibana :

apt-get install kibana -y

sudo nano /etc/kibana/kibana.yml

uncomment : server.host: "0.0.0.0"

uncomment : server.port: 5601

uncomment : server.publicBaseUrl: "https://elkserver:5601"

2. Create Certificate For Kibana:

cd /usr/share/elasticsearch/bin

sudo ./elasticsearch-certutil cert --out /etc/kibana/kibana.zip --name kibana --ca-cert /etc/elasticsearch/certs/ca/ca.crt --ca-key /etc/elasticsearch/certs/ca/ca.key --dns kibana --pem

cd /etc/kibana

sudo unzip kibana.zip

cp /etc/elasticsearch/certs/ca/ca.crt /etc/kibana/kibana

cd /etc/kibana/kibana

ls -alh

chown -R kibana:kibana ./

ls -alh

ls -alh kibana

3. Enable Certificate in Kibana Configuration File:

sudo nano /etc/kibana/kibana.yml

uncomment : server.ssl.enabled: true

server.ssl.certificateAuthorities: [ "/etc/kibana/kibana/ca.crt" ]

server.ssl.certificate: /etc/kibana/kibana/kibana.crt

server.ssl.key: /etc/kibana/kibana/kibana.key

elasticsearch.hosts: ["https://elkserver:9200"]

4. Enable Create Account Token:

cd /usr/share/elasticsearch/bin/

sudo ./elasticsearch-service-tokens create elastic/kibana kibana\_token

cd /etc/elasticsearch

chown -R elasticsearch:elasticsearch service\_tokens

ls -alh

sudo nano /etc/kibana/kibana.yml

uncomment : elasticsearch.serviceAccountToken: "AAEAAWVsYXN0aWMva2liYW5hL2tpYmFuYV90b2tlbjoxMHRuZzBJUlJZUzYwcnhaZlNPRU13"

elasticsearch.ssl.verificationMode: none

xpack.encryptedSavedObjects.encryptionKey: "put 32 char"

### Adjust Kibana Startup Time :

mkdir /etc/systemd/system/kibana.service.d

echo -e "[Service]\nTimeoutStartSec=1200" | tee /etc/systemd/system/kibana.service.d/startup-timeout.conf

6. Start Kibana Start On Boot:

sudo systemctl enable kibana

sudo systemctl start kibana

sudo systemctl status kibana

## Install Fleet Server & File Beat

Fleet Server and Filebeat help in collecting, centralizing, and managing logs and metrics from various sources. Fleet Server manages the integration of agents (like Filebeat), which ship logs and data to Elasticsearch, enabling real-time monitoring and analysis of system performance and security.

### Installing Elastic Agent :

apt install elastic-agent -y

systemctl enable elastic-agent

#### Add & Configure Fleet Server :

Open Fleet Page > Setting > Edite Elastic Host : https://<IP>:9200 > ssl.verification\_mode: "none"

Add Fleet Server > Click On Settings > https://<IP>:8220 > Advanced > Generate Fleet Server Token >

sudo elastic-agent enroll --url=https://192.168.1.243:8220 \

--fleet-server-es=https://192.168.1.243:9200 \

--fleet-server-service-token= Your\_Token\_Here \

--fleet-server-policy=fleet-server-policy \

--certificate-authorities=/etc/kibana/kibana/ca.crt \

--fleet-server-es-ca=/etc/kibana/kibana/ca.crt \

--fleet-server-cert=/etc/kibana/kibana/kibana.crt \

--fleet-server-cert-key=/etc/kibana/kibana/kibana.key \

--fleet-server-port=8220 \

--insecure

systemctl start elastic-agent

#### Filebeat Threat Intel module :

apt install filebeat -y

filebeat modules enable threatintel

sudo nano /etc/filebeat/modules.d/threatintel.yml :

MISP: false

OTX:false

uncomment the following :

var.username: guest

var.password: guest

sudo nano /etc/filebeat/filebeat.yml :

uncomment out the username and password & type password for elastic accouont

add the following line : ssl.verification\_mode: none : under elastic search output section

uncomment protocol: "https" under elastic search output section

uncomment > host: "https://192.168.1.243:5601" > under kibana section

add the following line > ssl.verification\_mode: none > under kibana section

filebeat test config

filebeat test output

sudo filebeat setup

systemctl enable filebeat

systemctl start filebeat

## Install Winlogbeat Agent On Windows

Winlogbeat on Windows collects and ships Windows Event Logs to Elasticsearch or Logstash. It helps in monitoring system security, troubleshooting, and compliance by sending logs such as application, security, and system events for analysis and alerting.

### Enable Power shell Logging :

function Enable-PSScriptBlockLogging

{

$basePath = 'HKLM:\Software\Policies\Microsoft\Windows' +

'\PowerShell\ScriptBlockLogging'

if(-not (Test-Path $basePath))

{

$null = New-Item $basePath -Force

}

Set-ItemProperty $basePath -Name EnableScriptBlockLogging -Value "1"

}

### Install Winlog Beat On Windows Client:

https://www.elastic.co/downloads/beats/winlogbeat

Extract ZIP File to program files > run cmd as admin > cd winlogbeat colder

winlogbeat.exe keystore create > winlogbeat.exe keystore add ES\_PWD

notepad.exe winlogbeat.yml :

- Kibana Section :

- Uncomment : host: "https://192.168.1.243:5601"

- Add ssl.verification\_mode: none

- Elasticsearch Output:

- hosts: ["https://192.168.1.243:9200"]

- Uncomment username: "elastic" & Uncomment password: "${ES\_PWD}"

- Add ssl.verification\_mode: none

winlogbeat.exe test config

winlogbeat.exe test output

winlogbeat.exe setup

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

Md c:\ProgramData\winlogbeat

copy "C:\Program Files\winlogbeat-{version}-windows-x86\_64\data\winlogbeat.keystore" c:\ProgramData\winlogbeat\

Run "winlogbeat" service

Netstat -n

### Install Packet Beat Agent On Windows

Packetbeat on Windows captures and analyzes network traffic in real-time. It helps monitor network performance, detect issues, and provide insights into network protocols and application communication, enabling better troubleshooting and security monitoring.

Extract ZIP File to program files > run cmd as admin > cd packetbeat colder

packetbeat.exe keystore create > packetbeat.exe keystore add ES\_PWD

packetbeat.exe devices

notepad.exe packetbeat.yml :

- interfaces.device: 0

- Kibana Section :

- Uncomment : host: "https://192.168.1.243:5601"

- Add ssl.verification\_mode: none

- Elasticsearch Output:

- hosts: ["https://192.168.1.243:9200"]

- Uncomment username: "elastic" & Uncomment password: "${ES\_PWD}"

- Add ssl.verification\_mode: none

packetbeat.exe test config

packetbeat.exe test output

packetbeat.exe setup

PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-packetbeat.ps1

Md c:\ProgramData\packetbeat

copy "C:\Program Files\packetbeat-8.12.2\data\packetbeat.keystore" c:\ProgramData\packetbeat

Run "packetbeat" service

Netstat -n

### Install Elastic Security Endpoint On Windows

**Elastic Security Endpoint** on Windows provides real-time threat detection, prevention, and response for endpoints. It helps protect against malware, ransomware, and other security threats by monitoring activities and providing insights into potential risks.

1. Make Sure Win log Beat & Packet Beat Services Are Run Automatic On Windows

2. Install sysmon Service

Microsoft Sysmon Internals

https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon Configuration File

https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml

Sysmon64.exe -i config-file.xml

Run sysmon64 service

Check windows logs are generated from sysmon

3. Add Windows Policy Fleet Server

Fleet > agent policies > create agent policy : Windows & Unchecked system metrics

Add Integration > Windows & Elastic Defend

4. Add Elastic Agent For Windows

Download Elastic Agent for windows & extract files to program files

Open powershell as admin

Go to elastic agent path

Run install commands with --insecure flag

Add ssl.verification\_mode: "none" in fleet server settings

5. Enabling Elastic Security Endpoint Rules :

Open Security > rules > Detection Rules

**Chapter 5:**

**System Work**

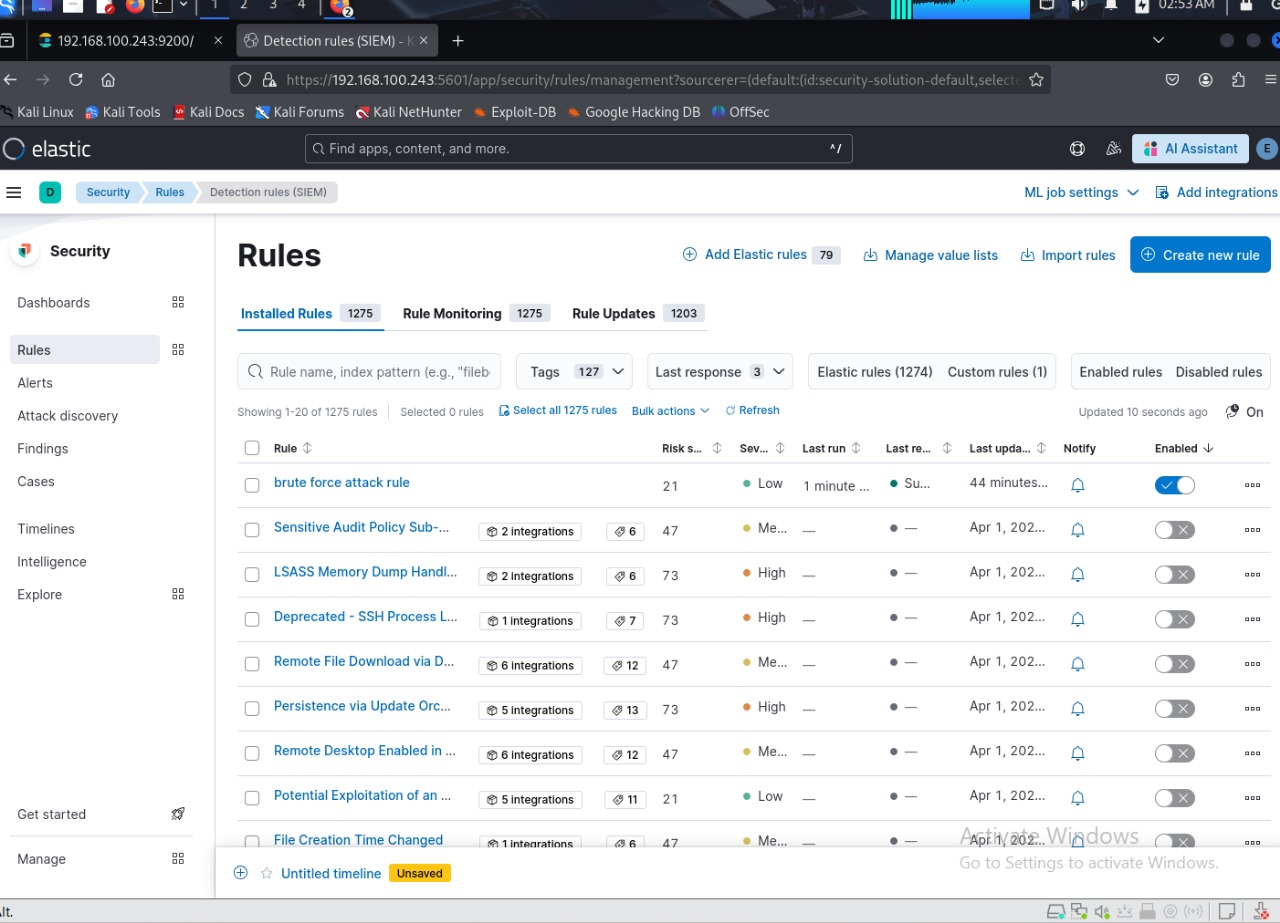
# Rules

The Rules page is a central feature in Elastic Security (SIEM) within Kibana, where you can create, manage, and monitor detection rules. These rules are used to detect suspicious or malicious behavior in your data (like login attempts, file changes, network activity, etc.).

## What does the Rules page do?

1. View Existing Rules:
   * You can see all active or inactive detection rules.
   * Filter by severity, rule type (custom, Elastic prebuilt), status, or tags.
2. Create New Rules:
   * Use KQL (Kibana Query Language) or EQL (Event Query Language) to define detection logic.
   * Choose the data source (e.g., log index or endpoint events).
   * Define conditions under which the rule triggers.
3. Manage Rules:
   * Enable or disable rules.
   * Edit or delete them.
   * Organize and tag for easier management.
4. Set Actions on Rule Trigger:
   * When a rule detects something, it can:
     + Send an email
     + Push a Slack message
     + Trigger a webhook
     + Or initiate an automated response (like a SOAR playbook)

### New Roles

* Under rules tab we clicked to create a new rule named brute force attack rule
* Configured to detect brute force attack trial

A computer screen shot of a computer

AI-generated content may be incorrect.

* Then based on rule alert created if there is such attack with high login failure attempts alert will be triggered And showing on dashboard

