A report on :

“ ELastic stack integration with OsTicket System “

By:

“ Hamza Jameel “

(dev.hamzaj@gmail.com)

Table of contents :

Introduction:

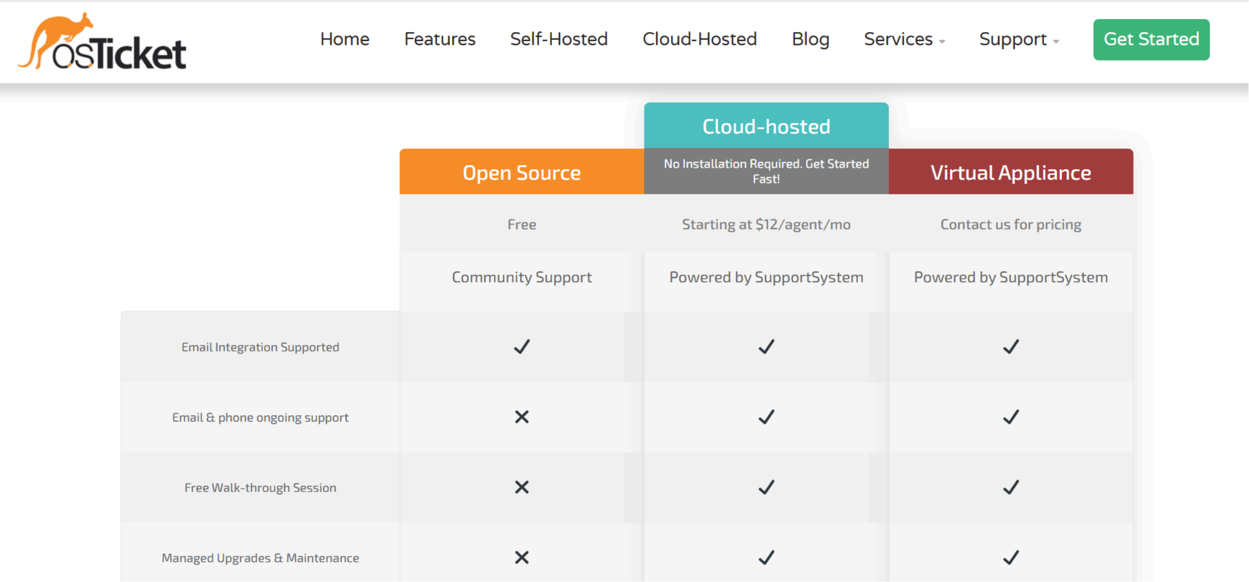
In this project, I successfully implemented a monitoring and detection setup using the Elastic Stack (ELK). This solution revolves around detecting OS ticket queries, incident tracking and management through features like managed workflows, automated ticket routing, and real-time notifications. By integrating osTicket with Elastic SIEM, the security of organizations can elevate , enabling seamless incident detection, tracking, and resolution. This integration allows security alerts generated by Elastic SIEM to be automatically converted into actionable tickets in osTicket, ensuring prompt response and effective collaboration.

Installations and Configurations :

This setup requires two different installations of different stacks . In this lab, the installation of ELK was performed on the Ubuntu base system. And osticket on windows server 2019.

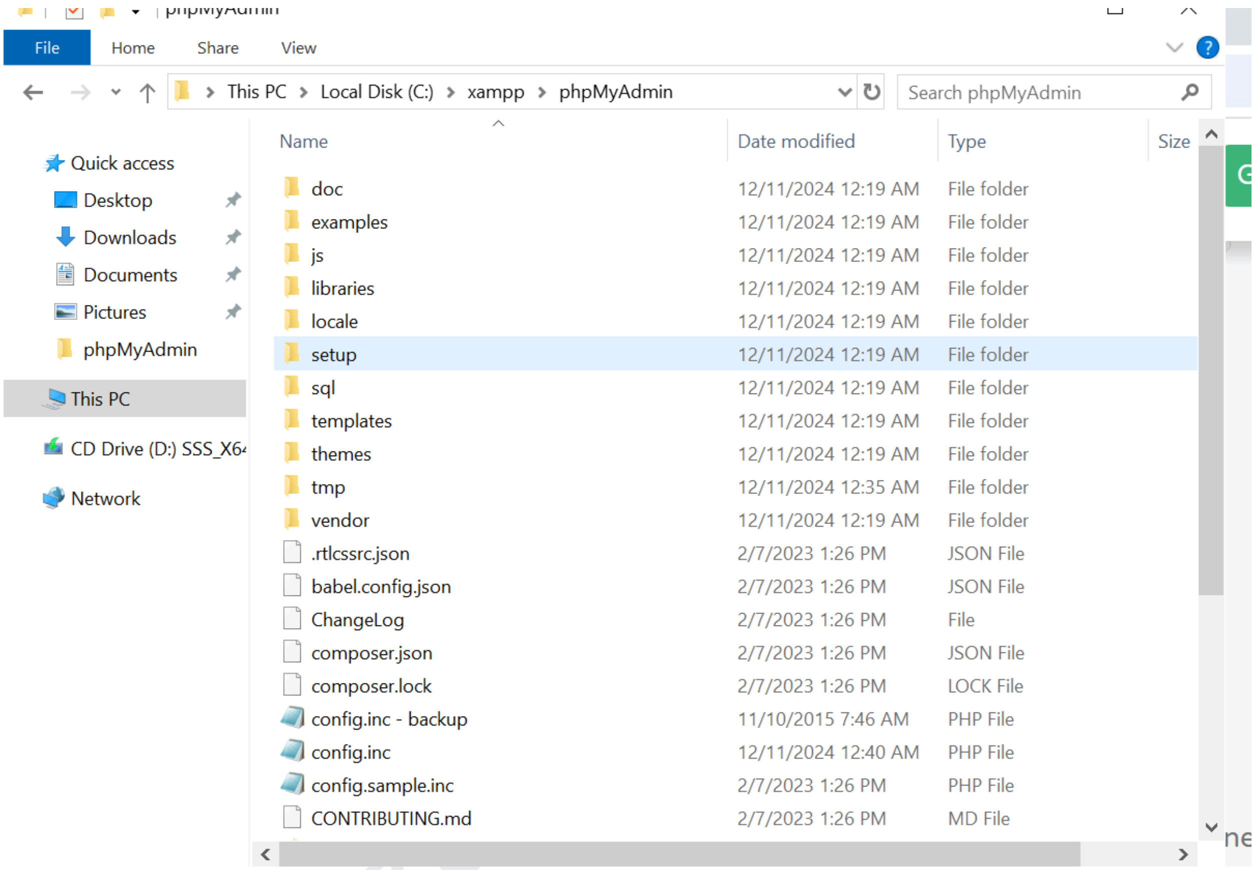
1. OS-Ticketing System:

An **OS ticketing system** (Open Source ticketing system) in information security refers to a software platform used to manage and track issues, incidents, or requests related to security operations. It acts as a centralized tool where users, teams, or organizations can report, prioritize, and resolve information security issues efficiently. For installation , follow these steps:
First navigate to os ticket official website and download the community version:



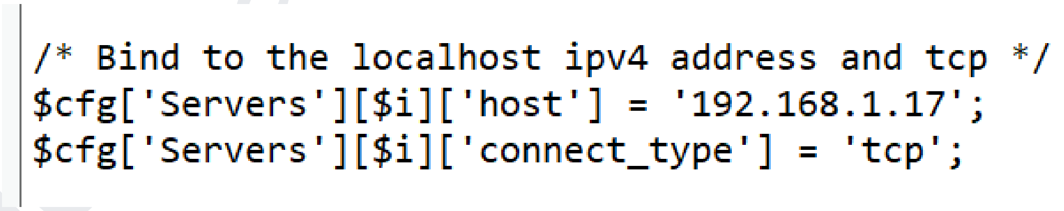
	Open Source	Cloud-hosted No Installation Required. Get Started Fast!	Virtual Appliance
	Free	Starting at $12/agent/mo	Contact us for pricing
	Community Support	Powered by SupportSystem	Powered by SupportSystem
Email Integration Supported	✓	✓	✓
Email & phone ongoing support	✕	✓	✓
Free Walk-through Session	✕	✓	✓
Managed Upgrades & Maintenance	✕	✓	✓

After downloading this , download a xampp server on windows , navigate to xampp folder in c drive and open phpmyadmin folder.



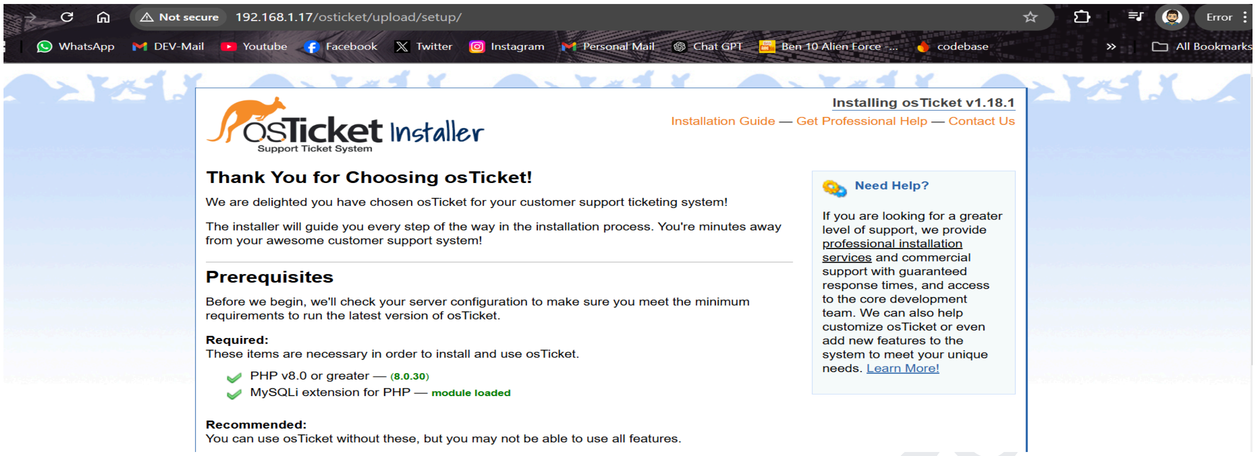
Name	Date modified	Type	Size
doc	12/11/2024 12:19 AM	File folder	
examples	12/11/2024 12:19 AM	File folder	
js	12/11/2024 12:19 AM	File folder	
libraries	12/11/2024 12:19 AM	File folder	
locale	12/11/2024 12:19 AM	File folder	
setup	12/11/2024 12:19 AM	File folder	
sql	12/11/2024 12:19 AM	File folder	
templates	12/11/2024 12:19 AM	File folder	
themes	12/11/2024 12:19 AM	File folder	
tmp	12/11/2024 12:35 AM	File folder	
vendor	12/11/2024 12:19 AM	File folder	
.rtlcssrc.json	2/7/2023 1:26 PM	JSON File	
babel.config.json	2/7/2023 1:26 PM	JSON File	
ChangeLog	2/7/2023 1:26 PM	File	
composer.json	2/7/2023 1:26 PM	JSON File	
composer.lock	2/7/2023 1:26 PM	LOCK File	
config.inc - backup	11/10/2015 7:46 AM	PHP File	
config.inc	12/11/2024 12:40 AM	PHP File	
config.sample.inc	2/7/2023 1:26 PM	PHP File	
CONTRIBUTING.md	2/7/2023 1:26 PM	MD File	

After that edit the config.inc file and make the following changes :



```
/* Bind to the localhost ipv4 address and tcp */
$cfg['Servers'][$i]['host'] = '192.168.1.17';
$cfg['Servers'][$i]['connect_type'] = 'tcp';
```

Give your IP address here and and turn on the server from the web gui. Extract the osticket folder that we have just downloaded and place it into xampp folder's htdocs. Now try to access this on your browser by typing.



Thank You for Choosing osTicket!

We are delighted you have chosen osTicket for your customer support ticketing system!

The installer will guide you every step of the way in the installation process. You're minutes away from your awesome customer support system!

Prerequisites

Before we begin, we'll check your server configuration to make sure you meet the minimum requirements to run the latest version of osTicket.

Required:
These items are necessary in order to install and use osTicket.

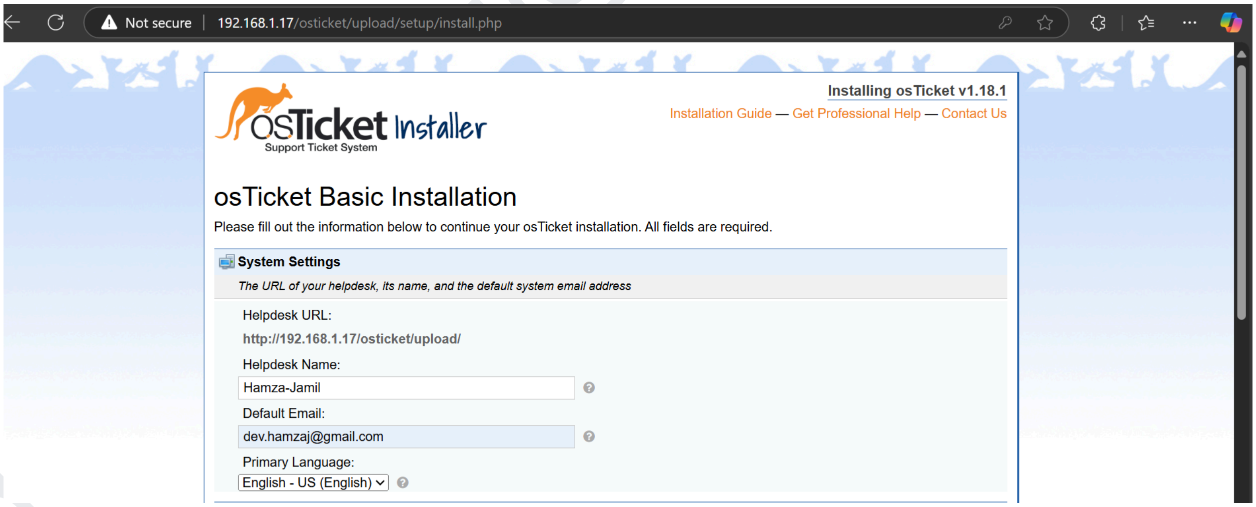
- ✓ PHP v8.0 or greater — (8.0.30)
- ✓ MySQLi extension for PHP — module loaded

Recommended:
You can use osTicket without these, but you may not be able to use all features.

Need Help?

If you are looking for a greater level of support, we provide professional installation services and commercial support with guaranteed response times, and access to the core development team. We can also help customize osTicket or even add new features to the system to meet your unique needs. Learn More!

Navigate down the page and click on the continue button. On the next page you will be prompted with an error showing that the configuration file is missing. In order to solve this error , navigate to xampp server folder on windows and click on htdocs , after that click on osticket , upload , include and search for a file called ost-sample-config . Rename this file to ost-config and ost-config and the error will be resolved . Now , move further and fill the following form.


Not secure
192.168.1.17/osticket/upload/setup/install.php
osTicket Installer
Support Ticket System
Installing osTicket v1.18.1
Installation Guide — Get Professional Help — Contact Us

osTicket Basic Installation

Please fill out the information below to continue your osTicket installation. All fields are required.

System Settings

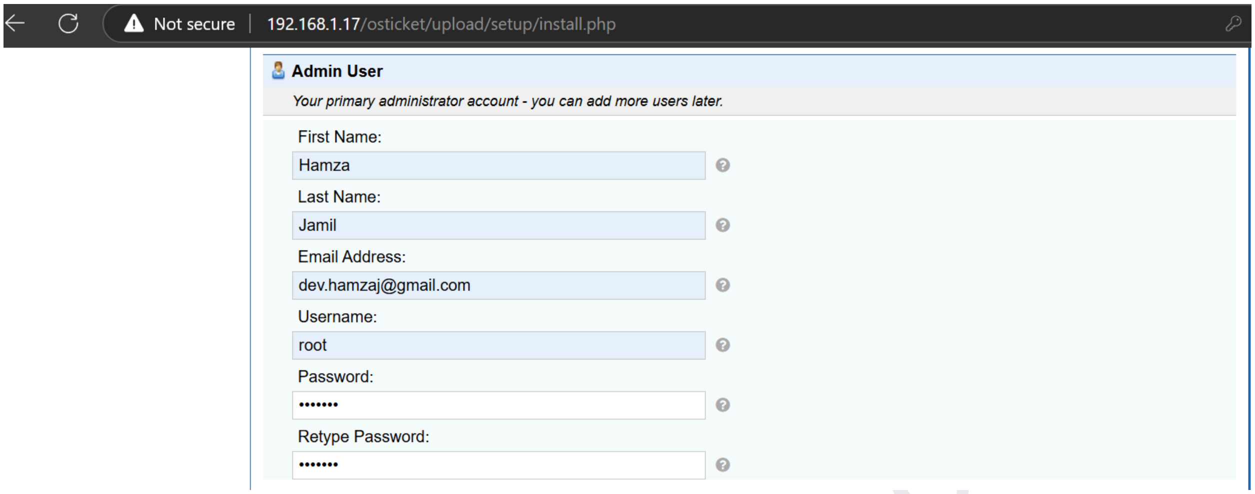
The URL of your helpdesk, its name, and the default system email address

Helpdesk URL:
http://192.168.1.17/osticket/upload/

Helpdesk Name:
Hamza-Jamil

Default Email:
dev.hamzaj@gmail.com

Primary Language:
English - US (English)



Not secure | 192.168.1.17/osticket/upload/setup/install.php

Admin User

Your primary administrator account - you can add more users later.

First Name: Hamza

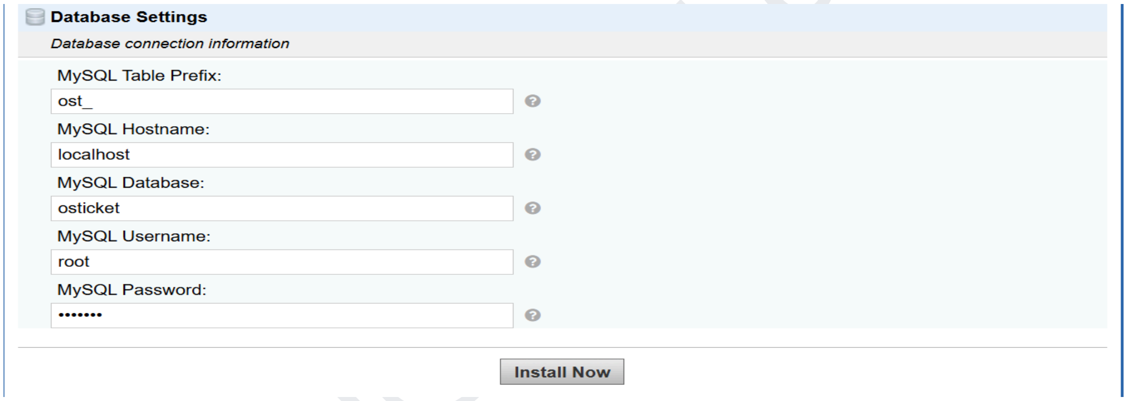
Last Name: Jamil

Email Address: dev.hamzaj@gmail.com

Username: root

Password: •••••••

Retype Password: •••••••



Database Settings

Database connection information

MySQL Table Prefix: ost_

MySQL Hostname: localhost

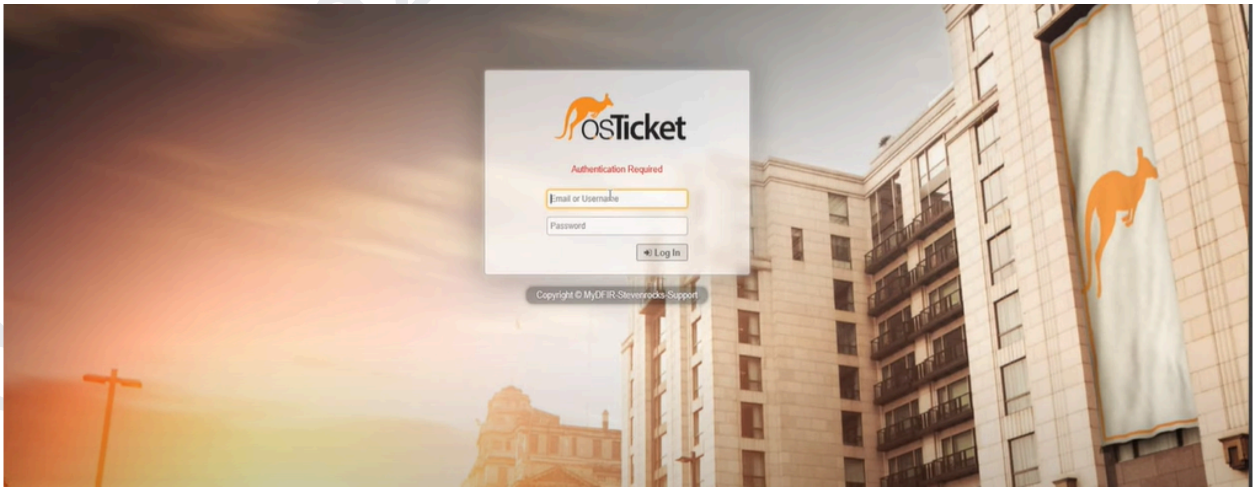
MySQL Database: osticket

MySQL Username: root

MySQL Password: •••••••

After filling the form , click on install now.

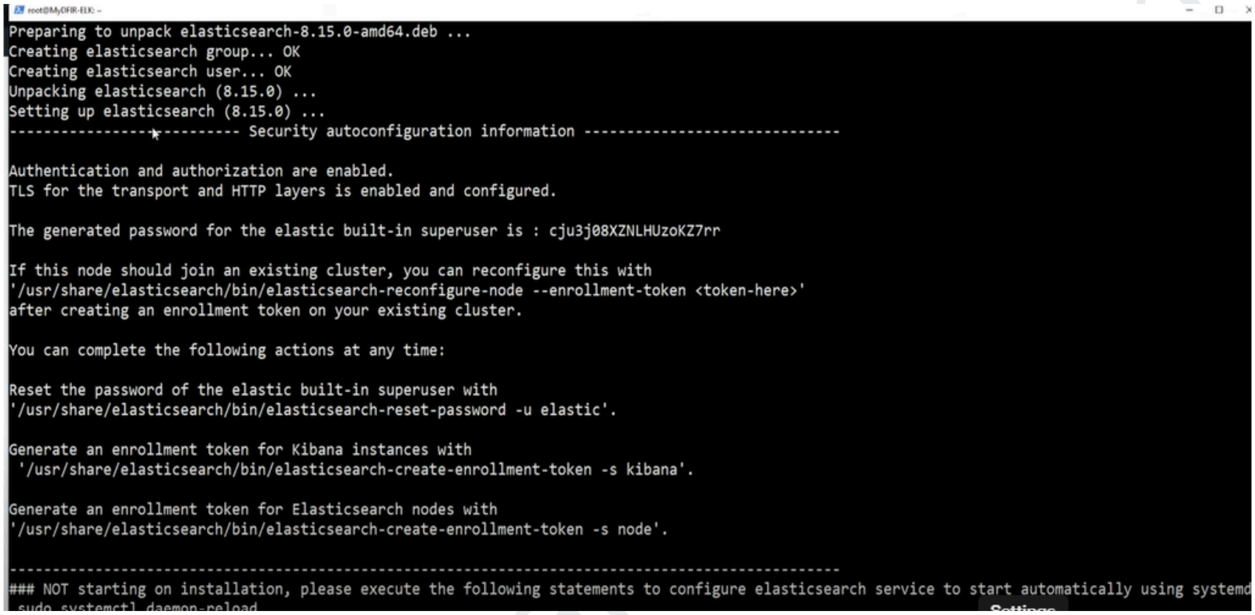
After that the osticket system will be installed and a dashboard will be visible for admin.



2. ELK Stack:

Download the elastic search latest file from the official repository or from their webpage . In my case I am using the base operating system linux ubuntu. For ELK setup , two different modules needed to be downloaded: the elastic search and kibana . Then they both will be interlinked to share and visualize the data .

Use the wget command to download the package and then use dpkg -i command to install the elastic search into the target system.

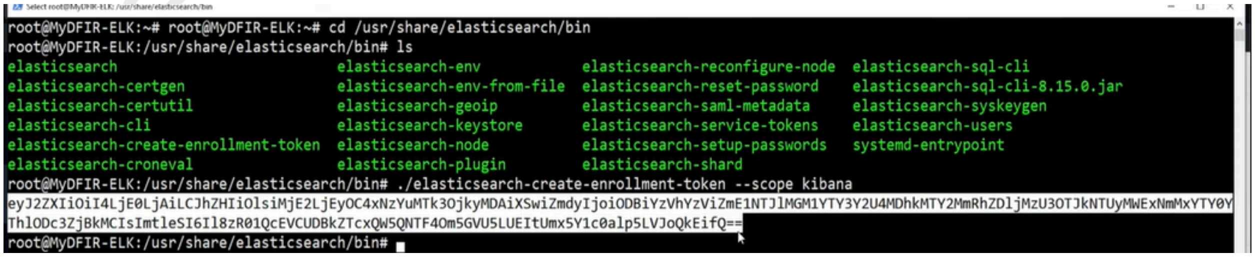


```
Preparing to unpack elasticsearch-8.15.0-amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Unpacking elasticsearch (8.15.0) ...
Setting up elasticsearch (8.15.0) ...
-------------------------- Security autoconfiguration information ------------------------------

Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : cju3j08XZNLHUzoKZ7rr

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:

Reset the password of the elastic built-in superuser with
'/usr/share/elasticsearch/bin/elasticsearch-reset-password -u elastic'.

Generate an enrollment token for Kibana instances with
 '/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s kibana'.

Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

-------------------------------------------------------------------------------------------------
### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
 sudo systemctl daemon-reload
```

After successful installation it will show some useful credentials that we will need to set up our kibana instance. Note these credentials and save them in a notepad file. After successful setup of our elastic instance we will setup kibana instance.

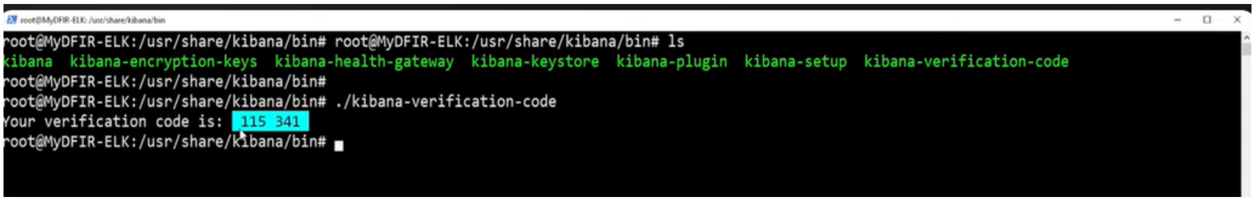
Download the kibana debian file from the official webpage and use the command dpkg -i to unpack it.

After that , move towards the elastic search directory and create an enrollment token for kibana as shown:

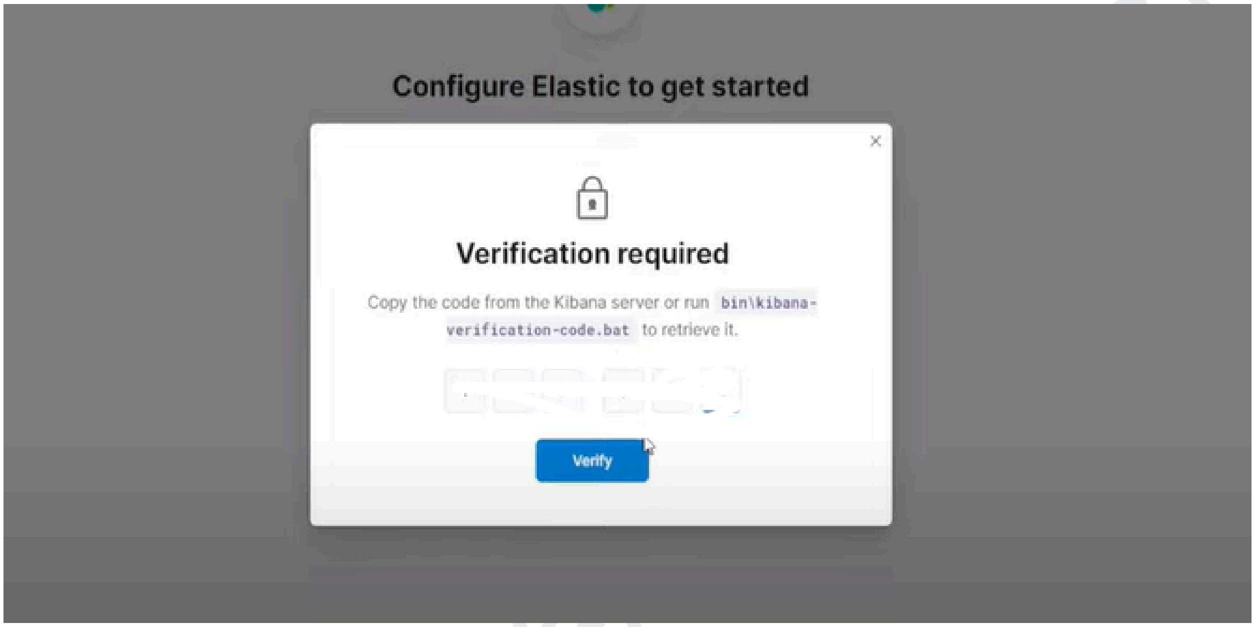


```
root@MyDFIR-ELK:~# root@MyDFIR-ELK:~# cd /usr/share/elasticsearch/bin
root@MyDFIR-ELK:/usr/share/elasticsearch/bin# ls
elasticsearch                           elasticsearch-env            elasticsearch-reconfigure-node  elasticsearch-sql-cli
elasticsearch-certgen                   elasticsearch-env-from-file  elasticsearch-reset-password    elasticsearch-sql-cli-8.15.0.jar
elasticsearch-certutil                  elasticsearch-geoip          elasticsearch-saml-metadata     elasticsearch-syskeygen
elasticsearch-cli                       elasticsearch-keystore       elasticsearch-service-tokens    elasticsearch-users
elasticsearch-create-enrollment-token   elasticsearch-node           elasticsearch-setup-passwords   systemd-entrypoint
elasticsearch-croneval                  elasticsearch-plugin         elasticsearch-shard
root@MyDFIR-ELK:/usr/share/elasticsearch/bin# ./elasticsearch-create-enrollment-token --scope kibana
eyJ2ZXIiOiI4LjE0LjAiLCJhZHIiOlsiMjE2LjEyOC4xNzYuMTk3OjkyMDAiXSwiZmdyIjoiODBiYzVhYzViZmE1NTJlMGM1YTY3Y2U4MDhkMTY2MmRhZDljMzU3OTJkNTUyMWExNmMxYTY0Y
Thl0Dc3ZjBkMCIsImtleSI6Il8zR01QcEVCUDBkZTcxQW5QNTF4Om5GVU5LUEItUmx5Y1c0alp5LVJoQkEifQ==
root@MyDFIR-ELK:/usr/share/elasticsearch/bin#
```

After creating the token from elastic enter it into the kibana dashboard and then create a verification code from kibana’s backend. Enter it into the kibana front page as shown:



```
root@MyDFIR-ELK:/usr/share/kibana/bin# root@MyDFIR-ELK:/usr/share/kibana/bin# ls
kibana  kibana-encryption-keys  kibana-health-gateway  kibana-keystore  kibana-plugin  kibana-setup  kibana-verification-code
root@MyDFIR-ELK:/usr/share/kibana/bin#
root@MyDFIR-ELK:/usr/share/kibana/bin# ./kibana-verification-code
Your verification code is:  115 341
root@MyDFIR-ELK:/usr/share/kibana/bin#
```



Configure Elastic to get started

Verification required

Copy the code from the Kibana server or run `bin\kibana-verification-code.bat` to retrieve it.

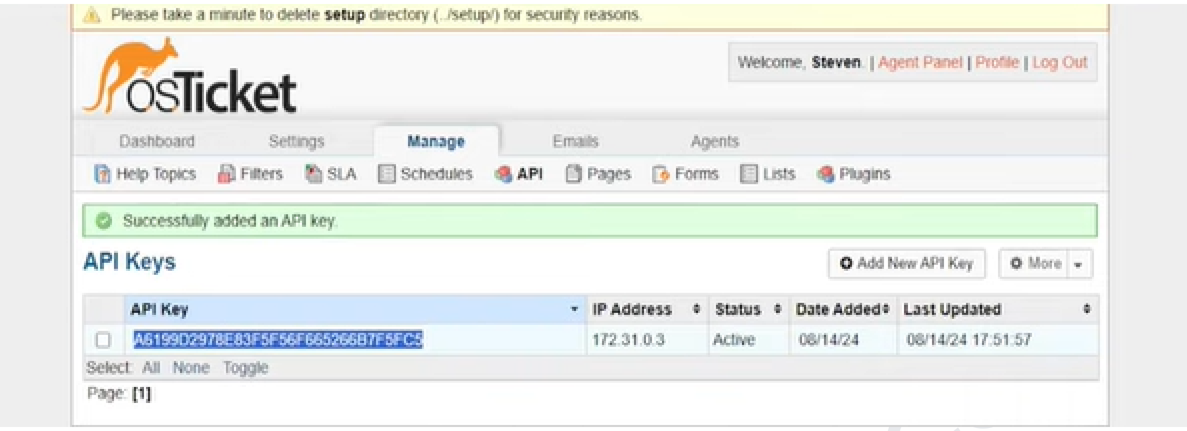
Now after these steps all the verifications are done and the instances are created and configured and ready to use now .

OS ticket Integration with ElasticSearch:

To parse the data generated by mythic server into elastic stack you need the following things :

Generating API key :

Navigate to osticket dashboard enter the credentials and generate an API key as shown in the picture pasted below :



Please take a minute to delete **setup** directory (../setup/) for security reasons.

Successfully added an API key.

	API Key	IP Address	Status	Date Added	Last Updated
□	A6199D2978E83F5F56F665266B7F5FC5	172.31.0.3	Active	08/14/24	08/14/24 17:51:57

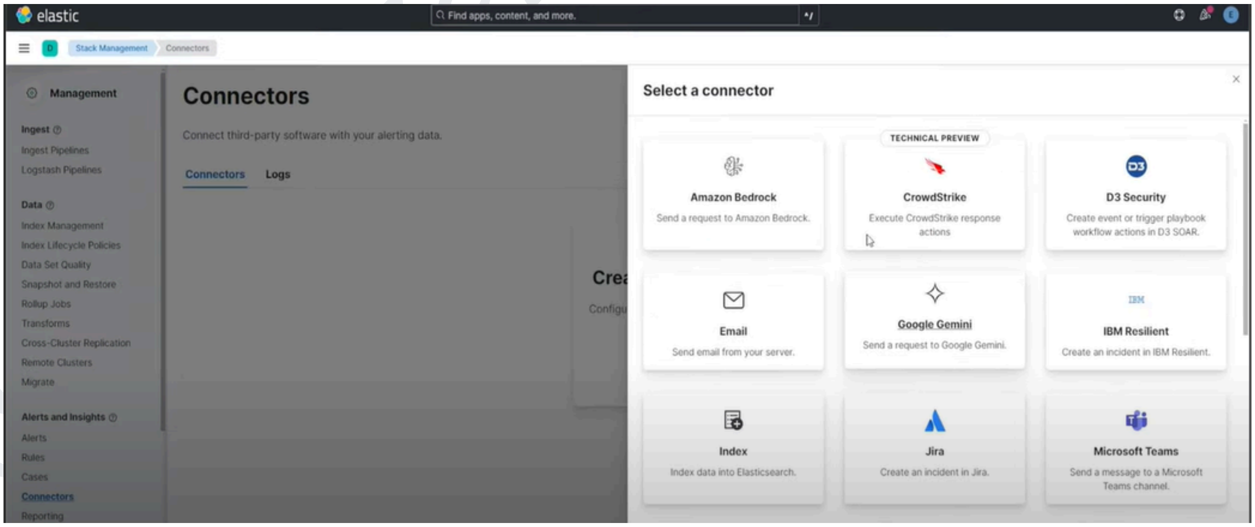
Select: All None Toggle

Page: [1]

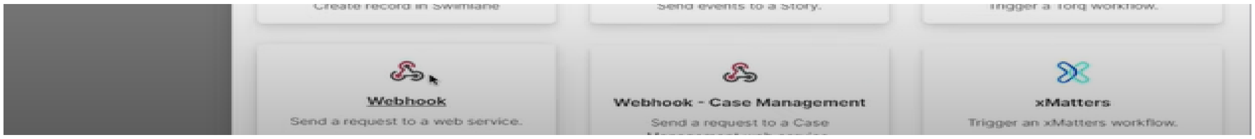
Now , after successfully generating the API key from the osticket , this needed to be pasted in kiabana's console.

Creating web-hook in kibana :

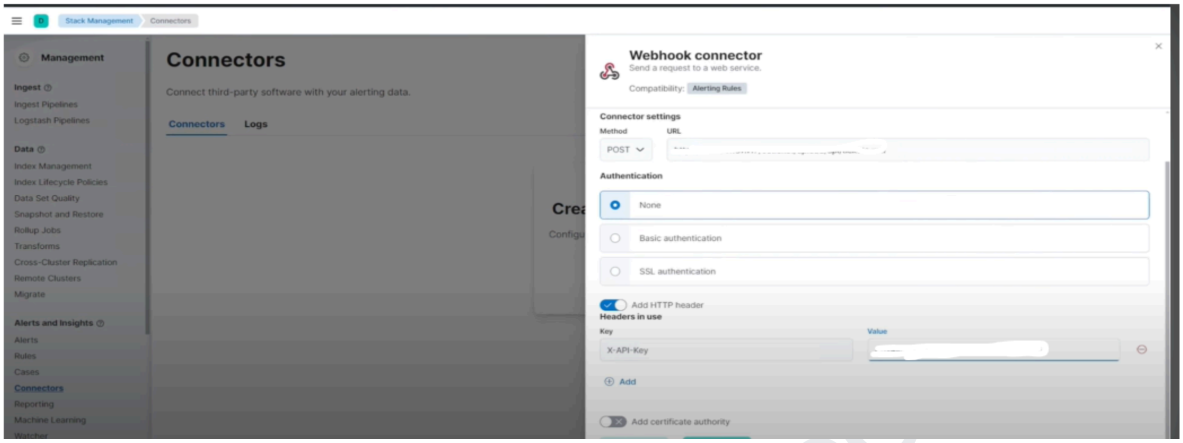
In order to fetch the data from osticket we need to paste the api key into the web hook section of elasticsearch and kibana so that our logs from osticket will be generated in osticket end and can easily be fetched from the source and visualize in destination. Note the webhook section of kibana is paid and only subscribed users can used this , navigate to stack management then connectors and select web-hook api connector and test the connection:



elastic
Find apps, content, and more.
Stack Management
Connectors
Management
Ingest
Ingest Pipelines
Logstash Pipelines
Data
Index Management
Index Lifecycle Policies
Data Set Quality
Snapshot and Restore
Rollup Jobs
Transforms
Cross-Cluster Replication
Remote Clusters
Migrate
Alerts and Insights
Alerts
Rules
Cases
Connectors
Reporting
Connectors
Connect third-party software with your alerting data.
Connectors
Logs
Crea
Configu
Select a connector
TECHNICAL PREVIEW
Amazon Bedrock
Send a request to Amazon Bedrock.
CrowdStrike
Execute CrowdStrike response actions
D3 Security
Create event or trigger playbook workflow actions in D3 SOAR.
Email
Send email from your server.
Google Gemini
Send a request to Google Gemini.
IBM
IBM Resilient
Create an incident in IBM Resilient.
Index
Index data into Elasticsearch.
Jira
Create an incident in Jira.
Microsoft Teams
Send a message to a Microsoft Teams channel.



Create record in Swimlane
Send events to a Story.
Trigger a Torq workflow.
Webhook
Send a request to a web service.
Webhook - Case Management
Send a request to a Case
xMatters
Trigger an xMatters workflow.



Webhook connector
Send a request to a web service.
Compatibility: Alerting Rules

Connector settings
Method: POST
URL: [redacted]

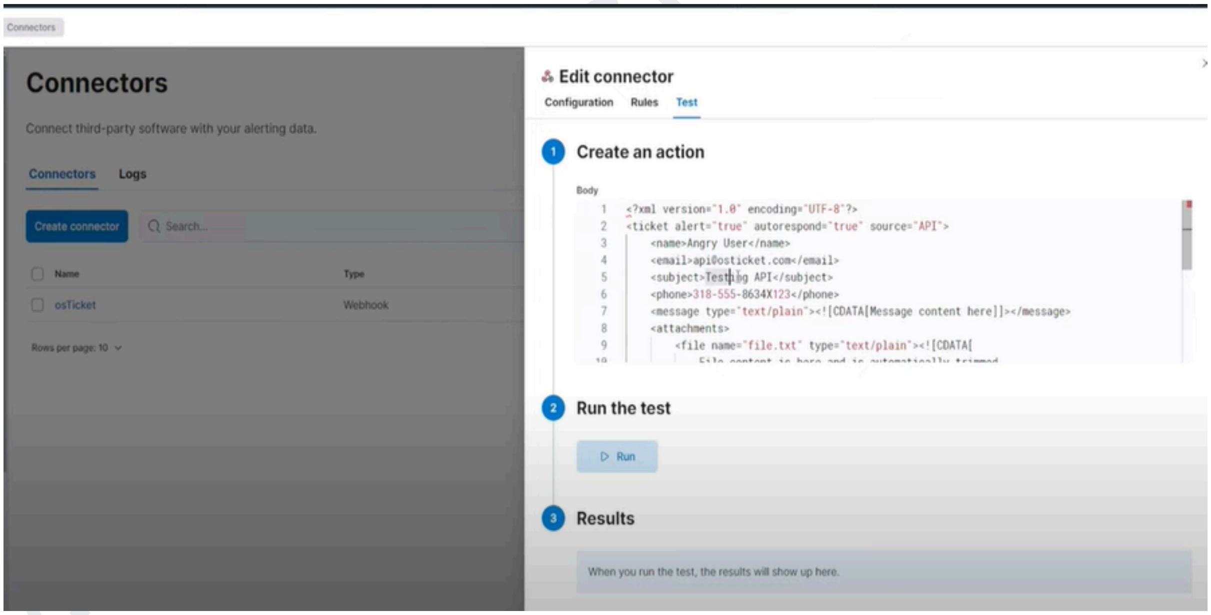
Authentication
● None
○ Basic authentication
○ SSL authentication

Add HTTP header (on)
Headers in use
Key: X-API-Key
Value: [redacted]

⊕ Add

Add certificate authority (off)

Fill the above mentioned fields with your data e:g api key generated from the osticket server , http request method and the server url and click ok.
At this point , the elastic will ask to input some payload , enter the xml payload example from the official github repo of osticket given and paste the code here :



Edit connector
Configuration | Rules | Test

1 Create an action

Body

```
<?xml version="1.0" encoding="UTF-8"?>
<ticket alert="true" autorespond="true" source="API">
    <name>Angry User</name>
    <email>api@osticket.com</email>
    <subject>Testing API</subject>
    <phone>318-555-8634X123</phone>
    <message type="text/plain"><![CDATA[Message content here]]></message>
    <attachments>
        <file name="file.txt" type="text/plain"><![CDATA[
            File content is here and is automatically trimmed
```

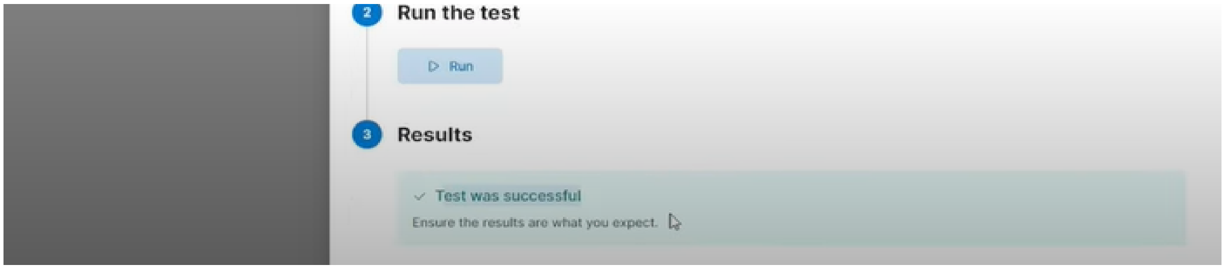
2 Run the test

▷ Run

3 Results

When you run the test, the results will show up here.

If everything goes well , the message will be displayed :



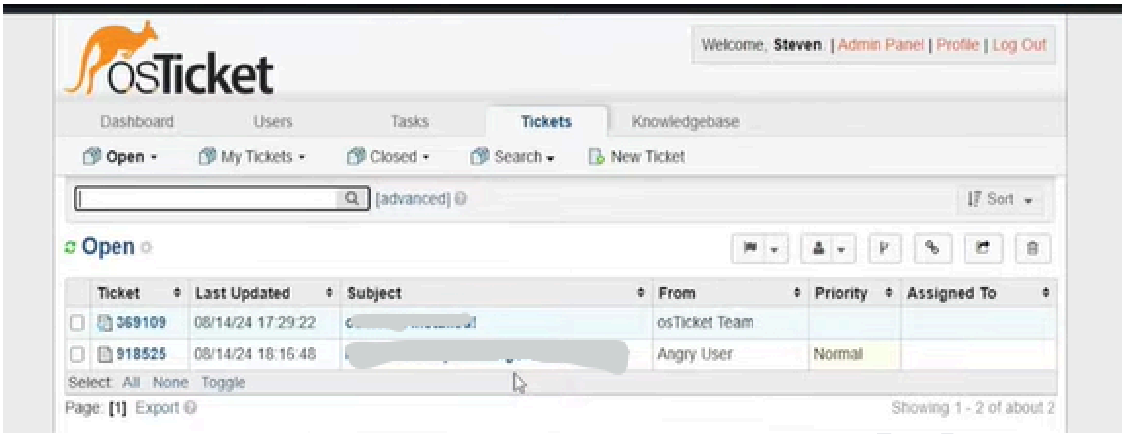
2 Run the test

▷ Run

3 Results

✓ Test was successful
Ensure the results are what you expect.

You can cross check the connection by going to osticket panel :



	Ticket	Last Updated	Subject	From	Priority	Assigned To
□	369109	08/14/24 17:29:22	[redacted]	osTicket Team		
□	918525	08/14/24 18:16:48	[redacted]	Angry User	Normal	

Select: All None Toggle

Page: [1] Export

Showing 1 - 2 of about 2

Now anytime our alert is generated from elastic itself , we can then start automatically creating a ticket in OSTICKET to start tracking our alerts. And by having our open source ticketing system , we are now fulfilling the AAA’s which are accounting and auditing .

Summary:

The project involved setting up an OSTICKET server on windows by using apache and sql and deployment of ELK stack for centralized management. Using ELK's detection rules and alerting mechanisms, I identified os ticket alerts, highlighted malicious patterns, and configured alerts to notify of threats in real time. Finally, I designed an intuitive ELK dashboard, providing actionable insights and visualizations for enhanced situational awareness and threat mitigation