

Day 25 -osTicket + ELK Integration

INTEGRAZIONE DI OSTICKET CON ELK ED INVIO DI UN ALERT DI TEST SU OSTICKET

osTicket + ELK Integration

Andiamo sull'Admin Panel sul portale di **osTicket**, poi su Manage->API->Add API Key , a questo punto inserirò il private IP del server **ELK** dato che sono nella stessa VPC, la chiave ottenuta la useremo su Elasticsearch per connettere i due componenti:

✓ Successfully added an API key.

API Keys

[Add New API Key](#) [More](#)

	API Key	IP Address	Status	Date Added	Last Updated
<input type="checkbox"/>	EAF [REDACTED]	[REDACTED]	Active	10/09/24	10/09/24 14:15:39

Select: All None Toggle

Page: [1]

Add New API Key

API Key is auto-generated. Delete and re-add to change the key.

Status: ☒ Active ☐ Disabled *

IP Address: [REDACTED] *

Services: Check applicable API services enabled for the key.

☒ Can Create Tickets (XML/JSON/EMAIL)

☐ Can Execute Cron


Internal Notes: Be liberal, they're internal

elastic connector

Andiamo sulla web UI di Elasticsearch , sezione Management->Stack Management->Alert and Insights->Connectors e da qui clicchiamo su 'Create Connector', quindi da qui decidiamo una volta ricevuto l'alert come comunicarlo e dove. In questo caso scegliamo '**Webhook**'.


osTicket + ELK Integration

Lo configuriamo nel seguente modo cliccando poi su 'Save and Test'.

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

Connector name

Connector settings

Method	URL
POST 	http://[redacted]osticket/upload/api/tickets.xml

Authentication


☒ None

☐ Basic authentication

☐ SSL authentication

☒ Add HTTP header

Headers in use

Key	Value
X-API-Key	EAS [redacted] 

osTicket + ELK Integration

Per il body da inserire lo prendiamo da GitHub.

Prima di continuare mi accerto che sull'osTicket server il private ip assegnato alla scheda di rete sia quello previsto dal cloud provider.

```
Ethernet adapter Ethernet Instance 0 2:  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::5801:5ff:fe20:534%4  
IPv4 Address. . . . . : 172.31.0.5  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . :
```

Edit connector

Configuration Rules **Test**

1 Create an action

Body

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

2 Run the test

▶ Run

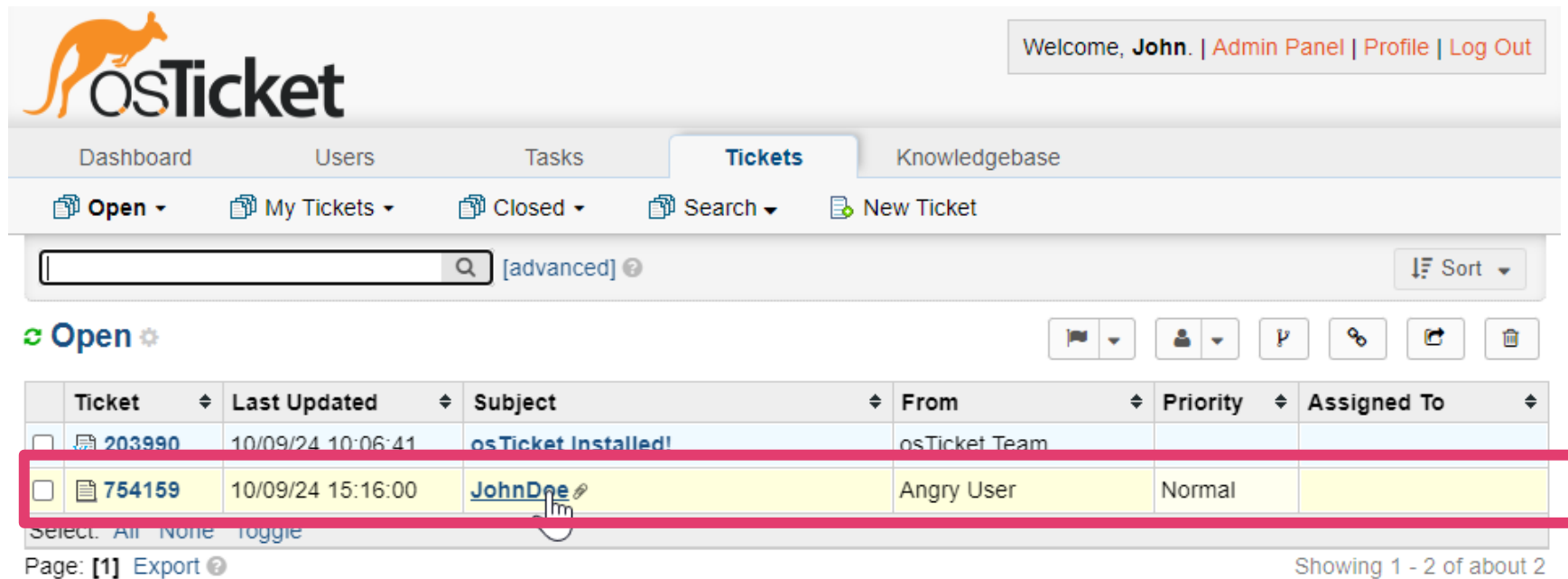
3 Results

✓ Test was successful

Ensure the results are what you expect.

osTicket + ELK Integration

Andiamo sull'Agent Panel e se tutto è stato configurato correttamente troveremo il ticket appena generato anche qui:



The screenshot shows the osTicket Agent Panel interface. At the top, there's a header with the osTicket logo and a welcome message for John. Below the header, there's a navigation bar with tabs for Dashboard, Users, Tasks, Tickets (selected), and Knowledgebase. Under the Tickets tab, there are buttons for Open, My Tickets, Closed, Search, and New Ticket. A search bar is present with a search icon and a link to advanced search. A sort dropdown is also visible. Below the search bar, there's a section for 'Open' tickets. A table lists the tickets with columns: Ticket, Last Updated, Subject, From, Priority, and Assigned To. The second row of the table is highlighted with a red box, showing a ticket with ID 754159, last updated on 10/09/24 at 15:16:00, with the subject 'JohnDoe', from 'Angry User', with a priority of 'Normal', and assigned to 'JohnDoe'. Below the table, there's a 'Select' dropdown set to 'All', a 'None' button, and a 'Toggle' button. At the bottom, it says 'Page: [1] Export' and 'Showing 1 - 2 of about 2'.

Ticket	Last Updated	Subject	From	Priority	Assigned To
203990	10/09/24 10:06:41	osTicket Installed!	osTicket Team		
754159	10/09/24 15:16:00	JohnDoe	Angry User	Normal	JohnDoe