

Day 4 – Kibana Setup

Kibana setup

Come primo passo, individuiamo il link per il download direttamente dal sito ufficiale di **Elasticsearch**.

```
root@ELK:~# https://artifacts.elastic.co/downloads/kibana/kibana-8.15.1-amd64.deb
-bash: https://artifacts.elastic.co/downloads/kibana/kibana-8.15.1-amd64.deb: No such file or directory
root@ELK:~# wget https://artifacts.elastic.co/downloads/kibana/kibana-8.15.1-amd64.deb
--2024-09-15 12:58:32-- https://artifacts.elastic.co/downloads/kibana/kibana-8.15.1-amd64.deb
Resolving artifacts.elastic.co (artifacts.elastic.co)... 34.120.127.130, 2600:1901:0:1d7::
Connecting to artifacts.elastic.co (artifacts.elastic.co)|34.120.127.130|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 340199408 (324M) [application/vnd.debian.binary-package]
Saving to: 'kibana-8.15.1-amd64.deb'

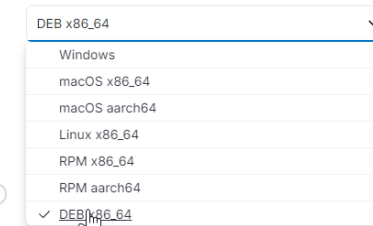
kibana-8.15.1-amd64.deb      7%[==>                ] 24.00M  32.3MB/s
```

```
root@ELK: ~
root@ELK:~# ls
elasticsearch-8.15.1-amd64.deb  kibana-8.15.1-amd64.deb  snap
root@ELK:~# dpkg -i kibana-8.15.1-amd64.deb
Selecting previously unselected package kibana.
(Reading database ... 122374 files and directories currently installed.)
Preparing to unpack kibana-8.15.1-amd64.deb ...
Unpacking kibana (8.15.1) ...
Setting up kibana (8.15.1) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.15/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
root@ELK:~#
```

Download Kibana

1 Download and unzip Kibana

Choose platform:



Kibana setup

Passiamo ora alla configurazione, specificando l'indirizzo IP e la porta del server **Kibana**.

```
root@ELK: ~  
GNU nano 6.2 /etc/kibana/kibana.yml *  
# For more configuration options see the configuration guide for Kibana in  
# https://www.elastic.co/guide/index.html  
  
# ===== System: Kibana Server =====  
# Kibana is served by a back end server. This setting specifies the port to use.  
server.port: 5601  
  
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.  
# The default is 'localhost', which usually means remote machines will not be able to connect.  
# To allow connections from remote users, set this parameter to a non-loopback address.  
server.host: 155. [REDACTED]
```

Kibana setup

Utilizziamo i seguenti comandi:

1. **Daemon-reload:** Applica le modifiche ai file di configurazione ricaricando le configurazioni.
2. **Enable:** Configura il servizio per avviarsi automaticamente al prossimo riavvio del sistema.
3. **Start:** Avvia immediatamente il servizio.
4. **Status:** per verificare che il servizio sia attivo e funzioni correttamente.

```
root@ELK:~# systemctl status Kibana.service
● kibana.service - Kibana
   Loaded: loaded (/lib/systemd/system/kibana.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2024-09-15 15:10:37 UTC; 7s ago
     Docs: https://www.elastic.co
   Main PID: 30707 (node)
      Tasks: 11 (limit: 19042)
     Memory: 298.1M
        CPU: 6.696s
   CGroup: /system.slice/kibana.service
           └─30707 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

Sep 15 15:10:37 ELK kibana[30707]: Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to
Sep 15 15:10:37 ELK kibana[30707]: {"log.level":"info","@timestamp":"2024-09-15T15:10:37.703Z","log.logger":"elastic-apm-node","ecs.version":1.6.0}
Sep 15 15:10:37 ELK kibana[30707]: Native global console methods have been overridden in production environment.
Sep 15 15:10:38 ELK kibana[30707]: [2024-09-15T15:10:38.480+00:00][INFO ][root] Kibana is starting
Sep 15 15:10:38 ELK kibana[30707]: [2024-09-15T15:10:38.532+00:00][INFO ][node] Kibana process configured with roles: [background_tasks, updat
Sep 15 15:10:42 ELK kibana[30707]: [2024-09-15T15:10:42.389+00:00][INFO ][plugins-service] The following plugins are disabled: "cloudChat, updat
Sep 15 15:10:42 ELK kibana[30707]: [2024-09-15T15:10:42.433+00:00][INFO ][http.server.Preboot] http server running at http://155.138.148.6
Sep 15 15:10:42 ELK kibana[30707]: [2024-09-15T15:10:42.524+00:00][INFO ][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup
Sep 15 15:10:42 ELK kibana[30707]: [2024-09-15T15:10:42.531+00:00][INFO ][preboot] "interactiveSetup" plugin is holding setup: Validating
Sep 15 15:10:42 ELK kibana[30707]: [2024-09-15T15:10:42.552+00:00][INFO ][root] Holding setup until preboot stage is completed.
```

100

Generiamo il **token di enrollment** per **Kibana** in **Elasticsearch**, che è una chiave temporanea generata da Elasticsearch per consentire l'installazione e la registrazione sicura di Kibana al cluster di Elasticsearch.

[illegible]

Prima di accedere alla nostra istanza **Kibana** è opportuno mettere in sicurezza l'accesso configurando il firewall.

Kibana setup

Imposteremo una doppia protezione con i firewall, offrendo due livelli di sicurezza:

1.Cloud provider: qui limitiamo il traffico in ingresso sull'**IP pubblico**, filtrando chi può accedere alla VPS **prima che il traffico raggiunga la macchina**.

2.Sistema operativo: configuriamo il firewall della VPS per gestire il traffico sulle **porte specifiche** del sistema, come ad esempio la **porta 5601** per il servizio **Kibana**.

Questo crea una doppia barriera: il firewall del cloud filtra gli **IP**, mentre il firewall della VPS protegge i **servizi specifici** (come Kibana), bloccando traffico non autorizzato anche in caso di errori nel primo livello.

```
root@ELK:/usr/share/elasticsearch/bin# ufw allow 5601
Rule added
Rule added (v6)
root@ELK:/usr/share/elasticsearch/bin#
```

Inbound IPv4 Rules

ⓘ Please note: rule updates may take up to 120 seconds to propagate to all servers

Action	Protocol	Port (or range) ?	Source	Notes	Action
accept	SSH	22	Anywhere	0.0.0.0/0	Add note +
accept	TCP	1 - 65535	151. [redacted]		

Kibana setup

Dopo aver creato il **token di enrollment**, mi collego all'indirizzo IP del server con la porta di Kibana per accedere alla **Web UI di Kibana** e visualizzarne l'interfaccia. Ci verrà chiesto un codice di verifica che possiamo ottenere grazie al file indicato nella schermata.

The image shows a composite of three screenshots from the Kibana setup process. The top screenshot is a terminal window showing the command `./kibana-verification-code` being executed, which outputs a verification code. The bottom-left screenshot shows the Kibana Web UI with the 'Enrollment token' field filled with a redacted token and the 'Connect to' field showing `https://155.155.155.155:5601`. The bottom-right screenshot shows the 'Verification required' screen with a red arrow pointing to the 'bin\kibana-verification-code.bat' command. A progress bar on the right indicates the setup steps: 'Saving settings' (completed), 'Starting Elastic' (completed), and 'Completing setup' (in progress).

```
root@ELK:/usr/share/elasticsearch/bin# cd /usr/share/kibana/bin
root@ELK:/usr/share/kibana/bin# ls
kibana  kibana-encryption-keys  kibana-health-gateway  kibana-keystore  kibana-plugin  kibana-setup  kibana-verification-code
root@ELK:/usr/share/kibana/bin# ./kibana-verification-code
-bash: ./: Is a directory
root@ELK:/usr/share/kibana/bin# ./kibana-verification-code
Your verification code is: [REDACTED]
root@ELK:/usr/share/kibana/bin#
```

Configure Elastic to get started

Enrollment token

Connect to `https://155.155.155.155:5601`

Configure manually **Configure Elastic**

Configure Elastic to get started

Verification required

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

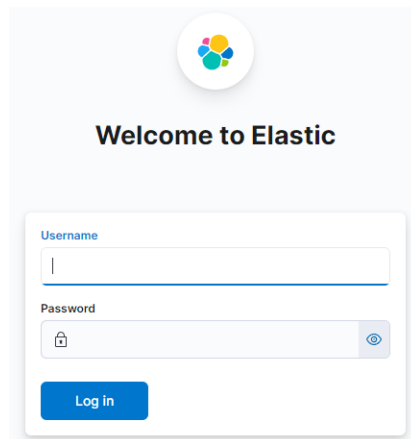
Verify

Configure Elastic to get started

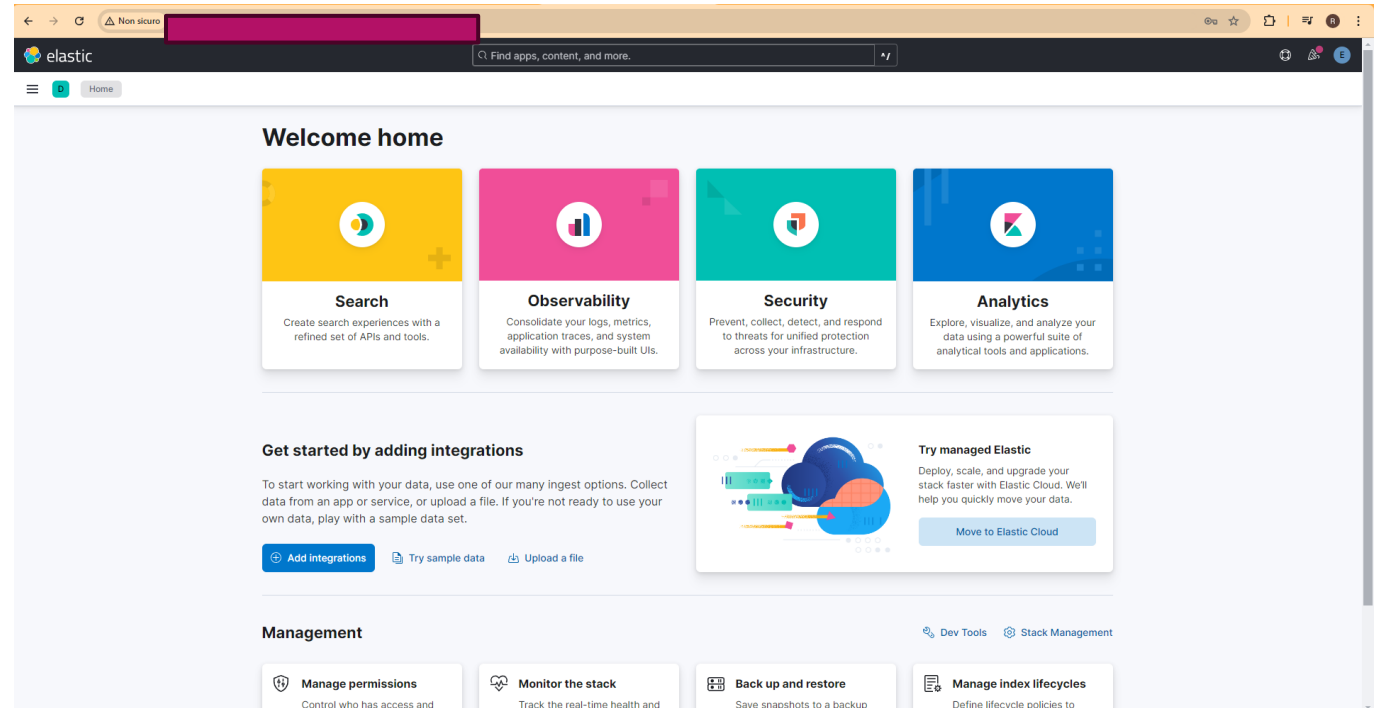
- ✓ Saving settings
- ✓ Starting Elastic
- Completing setup

Kibana setup

Una volta effettuato l'accesso questa è la schermata che si presenterà. Utilizzerò le credenziali generate nel Day 3 in fase di setup di Elasticsearch.



The login page features the Elastic logo at the top, followed by the heading "Welcome to Elastic". Below this is a login form with two input fields: "Username" and "Password". The "Password" field includes a toggle for visibility. A "Log in" button is positioned at the bottom of the form.



The dashboard is titled "Welcome home" and features four main functional areas: Search, Observability, Security, and Analytics, each with a brief description. Below these is a section for "Get started by adding integrations" with links to add integrations, try sample data, or upload a file. To the right is a "Try managed Elastic" section with a "Move to Elastic Cloud" button. The bottom section, "Management", includes links for managing permissions, monitoring the stack, backing up and restoring, and managing index lifecycles. The interface is clean with a light blue and white color scheme and a sidebar on the left.

Kibana setup

Effettuato l'accesso si presenta questo messaggio, che indica che è necessario un **"API integration key"** per garantire la **persistenza** dei dati criptati tra i riavvii di Kibana. Questo avviene perché Kibana utilizza una chiave di crittografia per proteggere gli oggetti salvati (come dashboard, visualizzazioni, ecc.).

The screenshot shows the Kibana Security Alerts page. A red warning banner at the top states: "API integration key required. A new encryption key is generated for saved objects each time you start Kibana. Without a persistent key, you cannot delete or modify rules after Kibana restarts. To set a persistent key, add the xpack.encryptedSavedObjects.encryptedKey setting with any text value of 32 or more characters to the kibana.yml file." Below the banner is a "Dismiss" button. On the left, the "Alerts" section is selected in the sidebar, and a table shows one alert with the status "open". A red arrow points from the "Alerts" table header to the warning banner. The top navigation bar includes the Elastic logo, a search bar, and links for "ML job settings", "Add integrations", "Data view", "Alerts", and "AI Assistant".

⚠ API integration key required

A new encryption key is generated for saved objects each time you start Kibana. Without a persistent key, you cannot delete or modify rules after Kibana restarts. To set a persistent key, add the `xpack.encryptedSavedObjects.encryptedKey` setting with any text value of 32 or more characters to the `kibana.yml` file.

Dismiss

Kibana setup

Utilizziamo il file che ci serve per generare tali chiavi:

```
root@ELK:/usr/share/kibana/bin# ./kibana-encryption-keys generate
## Kibana Encryption Key Generation Utility

The 'generate' command guides you through the process of setting encryption keys for:

xpack.encryptedSavedObjects.encryptionKey
  Used to encrypt stored objects such as dashboards and visualizations
  https://www.elastic.co/guide/en/kibana/current/xpack-security-secure-saved-objects.html#xpack-security-secure-saved-objects

xpack.reporting.encryptionKey
  Used to encrypt saved reports
  https://www.elastic.co/guide/en/kibana/current/reporting-settings-kb.html#general-reporting-settings

xpack.security.encryptionKey
  Used to encrypt session information
  https://www.elastic.co/guide/en/kibana/current/security-settings-kb.html#security-session-and-cookie-settings

Already defined settings are ignored and can be regenerated using the --force flag. Check the documentation links for instructions on how
to rotate encryption keys.
Definitions should be set in the kibana.yml used configure Kibana.

Settings:
xpack.encryptedSavedObjects.encryptionKey: [REDACTED]
xpack.reporting.encryptionKey: [REDACTED]
xpack.security.encryptionKey: [REDACTED]
```

Kibana setup

Questo comando aggiunge le chiavi generate al **keystore** di **Kibana**. Un keystore è un file sicuro che memorizza dati sensibili, come chiavi di crittografia e credenziali. Con «kibana-keystore add», salviamo la chiave di crittografia nel keystore di Kibana, ciò per far sì che le chiavi siano utilizzate nella configurazione di Kibana.

```
root@ELK: /usr/share/kibana/bin
root@ELK:/usr/share/kibana/bin# ls
kibana kibana-encryption-keys kibana-health-gateway kibana-keystore kibana-plugin kibana-setup kibana-verification-code
root@ELK:/usr/share/kibana/bin# ./kibana-keystore add
error: missing required argument 'key'
root@ELK:/usr/share/kibana/bin# ./kibana-keystore add xpack.encryptedSavedObjects.encryptionKey
Enter value for xpack.encryptedSavedObjects.encryptionKey: *****
root@ELK:/usr/share/kibana/bin# ./kibana-keystore add xpack.reporting.encryptionKey
Enter value for xpack.reporting.encryptionKey: *****
root@ELK:/usr/share/kibana/bin# ./kibana-keystore add xpack.security.encryptionKey
Enter value for xpack.security.encryptionKey: *****
root@ELK:/usr/share/kibana/bin# systemctl restart kibana.service
root@ELK:/usr/share/kibana/bin#
```

Kibana setup

Aggiornando la configurazione e aggiungendo la chiave al keystore, abbiamo risolto il problema di persistenza della chiave di crittografia. Ora, Kibana può utilizzare questa chiave persistente per criptare e decriptare i dati salvati anche dopo un riavvio. Questo significa che possiamo ora modificare o eliminare gli oggetti salvati senza problemi, poiché la chiave di crittografia è mantenuta costante.

