X-PACK
SECURITY

SECURITY

Plugin que provee de seguridad al clúster y a los datos que en él se encuentran.

En este módulo se crearán usuarios, securizarán comunicaciones y roles con distintos permisos.

1.

PRIMERAS MEDIDAS

PRIMERAS MEDIDAS

- Necesario X-Pack en cada nodo.

- Autenticación básica activada por defecto.
  Usuario: elastic | Pass: changeme

  *$ curl -XPUT -u elastic 'localhost:9200/_xpack/security/user/elastic/_password' -H "Content-Type: application/json" -d ‘{ "password" : “**openweb**” }'*

PRIMERAS MEDIDAS

Autenticación de mensajes

- Verifica que los mensajes intercambiados entre los nodos ES no están corruptos ni se han alterado.
- Clave simétrica (misma en todos los nodos)

$ bin/x-pack/syskeygen

Clave generada en: *CONFIG_DIR/x-pack/system_key*

PRIMERAS MEDIDAS

Auditoría de acciones

- Se registra toda interacción con el clúster.
- **Qué usuario** ha realizado **el qué** y **cuándo**.

- Necesario añadir al archivo *elasticsearch.yml*

```
$ xpack.security.audit.enabled: true
$ xpack.security.audit.outputs: [ index, logfile ]
```

2.

SECURIZACIÓN DE COMUNICACIONES

CIFRADO DE COMUNICACIONES

Posibilidad: **Información almacenada = Confidencial!**

Pueden producirse ataques como:

- *Sniffing* de comunicaciones.
- Manipulación de datos.
- Ganar acceso al servidor.
- Intercambio “*usuario*:*clave*” en texto plano.
- …

CIFRADO DE COMUNICACIONES

Configuración SSL/TLS en el clúster

Para habilitar este cifrado habrá que seguir estos pasos:

1. Generar una clave privada y certificado X.509
2. Configurar los nodos para que se identifiquen con el certificado firmado y habiliten SSL en la capa de transporte y HTTP.
3. Reiniciar Elasticsearch.

CIFRADO DE COMUNICACIONES

Certificados de nodos

- Certificados firmados por una CA confiable.
- Recomendable que contengan SAN (*Subject Alternative Names*) como IP o DNS.

- Herramienta ***certgen*** incluida en X-Pack. Genera una CA y firma los certificados con la misma.
  Funcionamiento *interactivo* o por *fichero* (silent).

CIFRADO DE COMUNICACIONES

Habilitar SSL en la configuración de los nodos

Necesario modificar el fichero *elasticsearch.yml:*

xpack.ssl.key: etc/elasticsearch/x-pack/elastic1/elastic1.key
xpack.ssl.certificate: /etc/elasticsearch/x-pack/elastic1/elastic1.crt
xpack.ssl.certificate_authorities: ["/etc/elasticsearch/x-pack/ca/ca.crt"]
xpack.security.transport.ssl.enabled: true
xpack.security.http.ssl.enabled: true

CIFRADO DE COMUNICACIONES

HTTPS en Kibana y conexión con Elasticsearch.

Necesario modificar el fichero *kibana.yml:*

elasticsearch.ssl.certificate: /etc/elasticsearch/x-pack/elastic1/elastic1.crt
elasticsearch.ssl.key: /etc/elasticsearch/x-pack/elastic1/elastic1.key
elasticsearch.ssl.certificateAuthorities: ["/etc/elasticsearch/x-pack/ca/ca.crt"]
server.ssl.certificate: /etc/elasticsearch/x-pack/elastic1/elastic1.crt
server.ssl.key: /etc/elasticsearch/x-pack/elastic1/elastic1.key

3.

AUTENTICACIÓN DE USUARIOS

AUTENTICACIÓN DE USUARIOS

Distintos *realms* soportados para la autenticación:

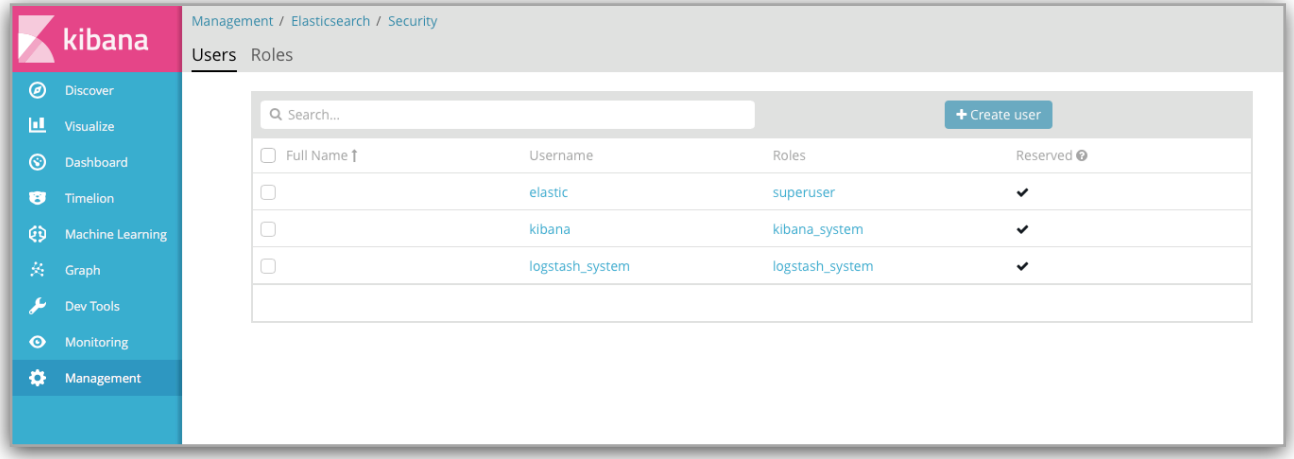
- *Nativo*
- *LDAP*
- *Directorio activo*
- *PKI*
- *File*

Posibilidad de integrarlo con otros sistemas de autenticación construyendo plugins personalizados.

AUTENTICACIÓN DE USUARIOS

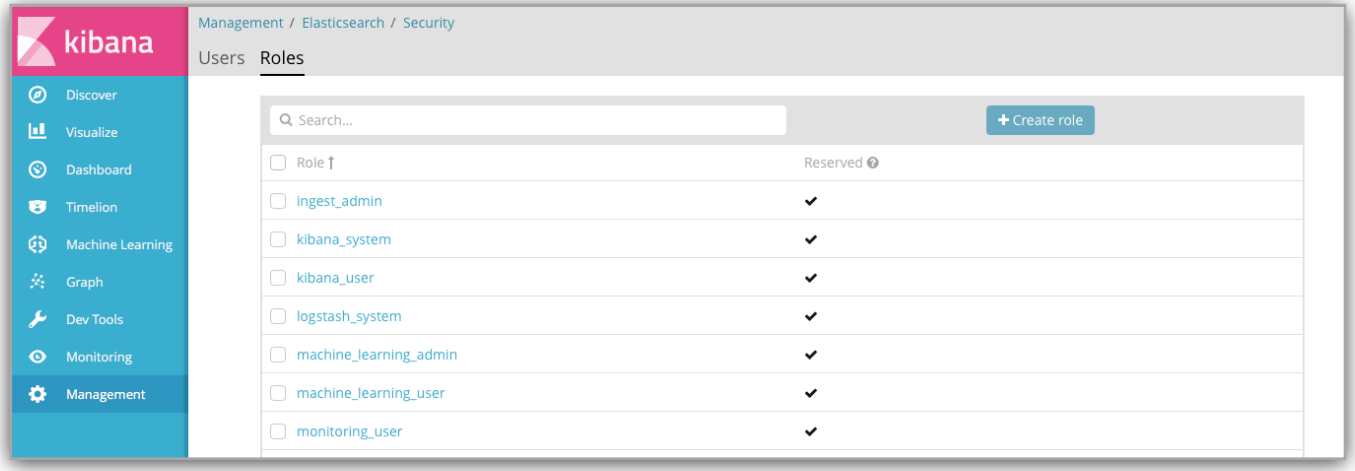
Creación de usuarios a través de la interfaz.

Aunque se puede usar la API



AUTENTICACIÓN DE USUARIOS

Creación de roles a través de la interfaz.



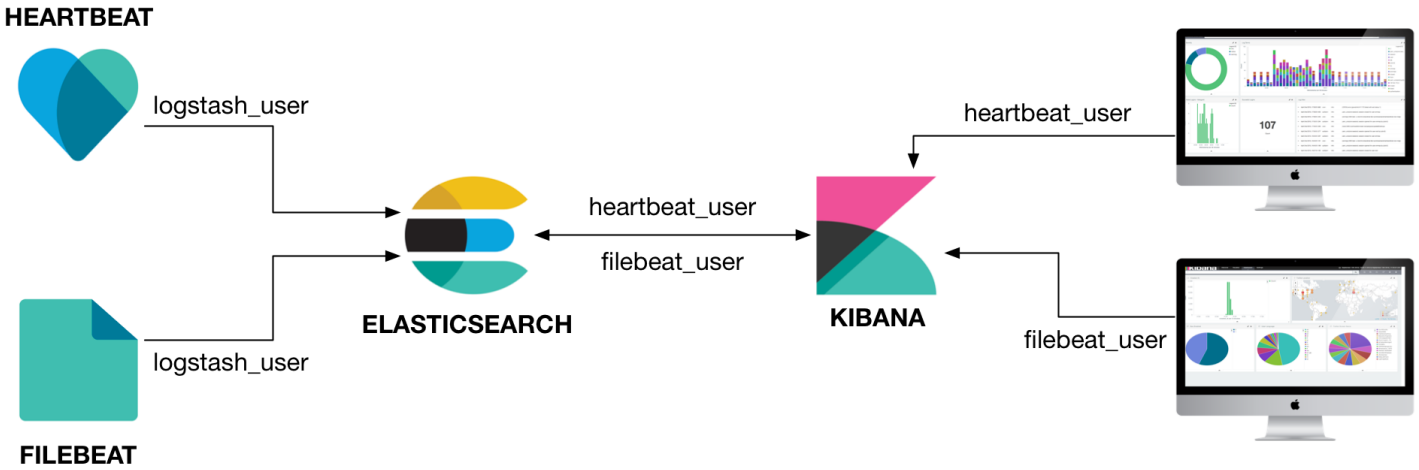
AUTENTICACIÓN DE USUARIOS

Creación de usuario logstash para indexar información.

Rol: *logstash_writer*
Cluster: *manage_index_templates*, *monitor*
Privilegios: *write*, *delete*, *create_index*

Estos permisos son necesarios para que o logstash o los beats puedan indexar datos en el clúster.

AUTENTICACIÓN DE USUARIOS



AUTENTICACIÓN DE USUARIOS

Creación de usuario para cada índice

*heartbeat_user = heartbeat-**
*filebeat_user = filebeat-**