OpenSearch Dashboards

El servidor Dashboards ja el vam posar en marxa dins el mateix "pod" on estava funcionant el servidor OpenSearch que vam estar estudiant a l'anterior PDF, així que en principi, no caldria fer gaire cosa al respecte: ja podem accedir als panells web oferits per aquest servidor sense fer res més.

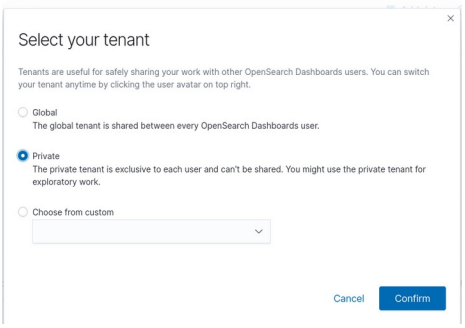
> NOTA: Igual que passava amb l'OpenSearch, el servidor Dashboards també un arxiu de configuració on podríem especificar directives personalitzades com "server.host", "server.port", "opensearch.hosts", etc (en lloc de fer servir el paràmetre *-e* de la comanda *podman*) amb l'avantatge, en aquest cas, de ser permanents. Aquest arxiu és "**/usr/share/opensearch/config/opensearch-dashboards.yml**" En aquest sentit, es podria fer el mateix procediment explicat amb el servidor OpenSearch per generar una imatge nova amb els canvis introduïts per utilitzar-la com a base pels servidors Dashboards que vulguem posar en marxa.

Per accedir al panell web ofert pel servidor Dashboards només cal que obrim un navegador (a la màquina real, per exemple) i escrivim http://ip.serv.Dashboards:5601 : hauria d'aparèixer un formulari web per autenticar-nos. Allà hi escriurem l'usuari "admin" amb contrasenya "admin" (l'usuari per defecte generat en un "pod" oficial d'OpenSearch) i, llavors sí, un cop autenticats apareixerà el panell web complet on podrem treballar.

> NOTA: Tingueu en compte que estem accedint al servidor Dashboards mitjançant HTTP i no pas via HTTPS. Per poder establir una comunicació xifrada entre el nostre navegador i el servidor Dashboards, hauríem de definir la configuració adient (concretament, a les directives "server.ssl.enabled", "server.ssl.certificate", "server.ssl.key" i "opensearch_security.cookie.secure" de l'arxiu "opensearch-dashboards.yml", tal com s'explica a https://opensearch.org/docs/latest/dashboards/install/tls). Ho deixarem com exercici

EXERCICIS:

1.-a) En la mateixa màquina virtual on has fet els exercicis dels PDFs anteriors, arrenca si no ho està el "pod" OpenSearch/Dashboards Tot seguit, accedeix, a través del navegador de la teva màquina real, a http://ip.serv.Dashboards:5601. Un cop loguejat amb l'usuari "admin" i contrasenya "admin", veuràs la següent pantalla...:



...on pots triar l'opció que vulguis, però ens quedarem amb la que ve sel·leccionada per defecte ("Private"). Si vols saber què és un "tenant", llegeix la nota següent.

> NOTA: Els "tenants" són espais per desar les visualitzacions, taulers, "index patterns" i altres objectes gestionats per Dashboards. De manera predeterminada, tots els usuaris d'OpenSearch tindran ja creats per defecte dos "tenants", anomenats "Global" i "Private". El primer és compartit entre tota la resta d'usuaris d'OpenSearch i el segon és exclusiu per cada usuari i no es pot compartir. El "tenant" global (i altres que s'hi puguin crear a posteriori) són útils per compartir el treball d'un usuari d'OpenSearch amb altres usuaris, i fer-ho de manera segura (configuran-t'hi els rols que poden tenir accés a un "tenant" de tipus global, amb quins permisos, etc segons s'escaigui).

b) Crea una plantilla. Recorda que la utilitat de les plantilles radica en assegurar-se que els valors de certs camps dels documents emmagatzemats en un índex (o en un conjunt determinat d'ells) siguin reconeguts com d'un tipus diferent al de cadena (que és el tipus per defecte); així doncs, preparar una plantilla serà imprescindible si volem tractar certes dades com si fossin per exemple nombres sencers, o decimals, o valors booleans, o de tipus IP, o de tipus data, etc (i fer-ne, doncs, les operacions adients amb ells, com sumes, restes, etc). En el nostre cas, la farem servir per fer que el camp "log" que rebrem del Fluent-Bit (veure més

endavant) sigui reconegut com a nombre sencer (per així poder després operar amb ell de la forma desitjada, com veurem també). Per crear una plantilla des del Dashboards, vés al menú "**OpenSearch plugins**" -> "**Index management**"->"**Templates**" (visible al lateral esquerra de la pàgina) i a la pàgina que apareix pulsa el botó de "Create template" per crear una plantilla anomenada com es vulgui però que hauria d'estar associada obligatòriamen a un "index pattern" anomenat "pepa*" (el qual crearem aviat) i estableix (a l'apartat "Index mapping" del final de la pàgina) que el camp anomenat "log" siguin de tipus "integer"

NOTA: També es pot, alternativament, crear la plantilla manualment sense haver de fer servir Dashboards sinó contactant directament amb el servidor OpenSearch (de fet, aquesta manera ja la vam estudiar al PDF anterior). Recordem que aquest procediment consisteix en crear un arxiu (pot ser a la màquina real, allà on vulguis) anomenat per exemple "abcd.json" amb el següent contingut...

```
{
        "index_patterns": ["pepa*"],
        "mappings": {
                "properties" : {
                        "log" : { "type": "integer" } ,
                        "timestamp" : { "type": "date", "format": "yyyy-MM-dd HH:mm:ss" }
                }
        }
}
```

... i tot seguit executar la següent comanda (també a la màquina real):

```
curl -X PUT -k  -u "admin:Un4C0ntraSs3ny4C0mplicad4_" https://ip.serv.OpenSearch:9200/_template/plantilla1
                                                        -H "Content-Type:application/json" -d @abcd.json
```

c) Edita l'arxiu de configuració "/usr/local/etc/fluent-bit/fluent-bit.conf" (que és l'utilitzat per defecte pel servei "fluent-bit.service") per a què:

* Tingui comentades tant la secció [INPUT] com la secció [OUTPUT] allà presents per defecte
* Tingui afegides (al final del fitxer) les següents línies:

```
[INPUT]
  Name tail
  Path /var/log/pepa.log

[OUTPUT]
  Name opensearch
  Match *
  Host 127.0.0.1
  Port 9200
  Index pepa
  HTTP_User admin
  HTTP_Passwd Un4C0ntraSs3ny4C0mplicad4_
  Tls on
  Tls.verify off
  Suppress_Type_Name On
```

NOTA: Has de fer les indentacions al mateix nivell que les línies preexistents o si no FluentBit donarà un error en arrencar
NOTA: Assegura't (amb *systemctl cat fluent-bit*) que el fitxer de configuració llegit pel binari "fluent-bit" sigui efectivament "/usr/local/etc/fluent-bit/fluent-bit.conf" (si no ho fos, edita la línia *ExecStart=* del fitxer *.service adientment per a què ho sigui).

¿Què farà, tal i com està establerta la seva configuració? Un cop gravada, inicia el servei Fluent-Bit (*sudo systemctl start fluent-bit)*

d) Obre un terminal de la màquina virtual i executa-hi varis cops la comanda *echo $RANDOM | sudo tee -a /var/log/pepa.log*

NOTA: Cal executar la comanda *tee* com a "root" per a què pugui escriure sota la carpeta "/var/log"

e) Entra de nou al panel web de Dashboards i vés ara al link "**Management**" -> "**Stack Management**" que apareix al final del menú principal (sempre es pot arribar a ell clicant al botó de la cantonada superior esquerra amb la icona de les tres línies horitzontals) i, en el nou menú lateral que hi apareix llavors, vés al link "Index patterns" i llavors pulsa sobre el botó "Create index pattern" que apareixerà al centre de la pantalla. Hauries de veure llavors una llista dels índexs actuals disponibles a OpenSearch, els quals, com a mínim, haurien de ser, entre altres dels exercicis anteriors, "pepa". Escriu al quadre de text allà mostrat el valor "pepa*" com a valor de l'"index pattern" a crear (això és per a què Dashboards sàpiga que ha de mostrar les dades de només els índexs emmagatzemats a OpenSearch el nom dels quals quadri amb aquest patró). A la pantalla següent, defineix el camp "@timestamp" com a camp temporal de referència (pels gràfics on hi aparegui algun eix temporal).

f) Vés ara al link "**OpenSearch Dashboards**" -> "**Discover**" del menú principal ¿Què mostra la taula de files visible a la part central de la finestra? ¿Què mostra la gràfica de barres que apareix sobre aquesta taula?

> NOTA: Si Dashboards t'avisa de què no tens dades en el rang de temps actual, hauràs de modificar-lo al desplegable que apareix a la cantonada de dalt a la dreta, al costat del botó "Refresh".

fII) Clica sobre el botonet petitó "+" que apareix al costat dels noms dels camps que es veuen a la barra vertical a l'esquerra de la taula de files central per tal de personalitzar aquesta taula per a què mostri només dues columnes: les corresponents a les dades dels camps "timestamp" (encara que per defecte aquesta columna sempre es mostra amb el títol de "Time") i "log".

> NOTA: Si has afegit varis "Index patterns" a la configuració de Dashboards, pots anar alternant les visualitzacions d'un o altre si cliques sobre el desplegable mostrat sobre la barra vertical que mostra els noms dels camps

fIII) ¿Què es veu quan es clica sobre la icona del ">" mostrada a l'esquerra de cada registre de la taula central?

Es pot fer servir el quadre de recerca que apareix a dalt de la pàgina "Discover" per escriure el mateix que si fos el paràmetre *q* d'una consulta GET a OpenSearch (és a dir, una recerca Lucene, amb la sintaxi *nomCamp:valorABuscar*). Igual que llavors:

*Les recerques dels noms de camps i els seus valors són case-insensitive
*Es poden escriure cometes al valor per indicar una recerca exacta
*Es poden fer servir els comodins * i ? en els valors
*Es poden indicar rangs de valors per un camp amb la sintaxi *nomCamp:[x TO y]* o *nomCamp:{x TO y}* (si s'escriu entre [] éls extrems del rang s'inclouen i si s'escriu entre {} els extrems no s'inclouen)
*Es poden indicar operadors booleans com AND, OR o NOT
*Es pot emprar el "Dashboards Query Language" (per defecte és així, tal com es pot veure al botó "DQL" (https://opensearch.org/docs/latest/dashboards/dql), el qual representa una ampliació del llenguatge de consultes Lucene que aporta més flexibilitat i facilitat (per exemple, amb DQL es poden utilitzar els símbols < o > per indicar una recerca matemàtica, entre altres ampliacions que anirem veient)

> NOTA:Alternativament, per tal d'escriure filtres de forma més fàcil, es pot utilitzar botó/assistent "Add a filter" que apareix a la banda esquerra dalt de tot, sobre la llista de camps. D'altra banda, també es pot clicar sobre la icona que apareix al costat de cada nom de camp amb el dibuix d'un lupa amb el símbol "+" al seu interior per tal de filtrar pels documents que tinguin exactament el mateix valor en el camp seleccionat. Finalment, també es pot utilitzar el botó "Filter by type" (que apareix sobre la llista de camps), per si ens fos necessari fer aquest tipus de filtratge

fIV) ¿Què es veu si escrius el filtre *log > 20000* al quadre de recerca de la pàgina "Discover"?

2.-a) Vés al link "OpenSearch plugins" -> "Index management" -> "Templates". ¿Què veus? Selecciona la (única) plantilla existent: ¿quines opcions se't mostren llavors al desplegable "Actions"? ¿Quina informació obtens quan cliques sobre el nom de la plantilla existent?

b) Vés al link "OpenSearch plugins" -> "Index management" -> "Indices". ¿Quina informació veus? ¿A quina comanda *curl* seria equivalent aquesta pàgina? Selecciona un index qualsevol dels existents: ¿quines opcions se't mostren llavors al desplegable "Actions" (per tenir una idea de la seva utilitat llegeix https://opensearch.org/docs/latest/dashboards/admin-ui-index/index-management)?¿Quina informació obtens quan cliques sobre el nom d'un índex qualsevol (i en especial,a la pestanya "Mappings" que hi surt a la nova pàgina mostrada)?

Les visualitzacions de Dashboards es basen en "agregacions" de dades (és a dir, mitjanes, sumes, mínims, màxims, recomptes,...tot de càlculs concrets realitzats sobre un conjunt de dades determinat) realitzades realment per OpenSearch. Dashboards simplement subministra la UI per definir-les, enviar-ne la petició corresponent a OpenSearch i visualitzar-ne el resultat. Per mostrar una visualització, sigui del tipus que sigui (gràfic de barres, de pastís, de línies, etc) el procediment més comú és el següent:

1) Definir un "Bucket": És a dir, definir el criteri que vulguem per tal d'agrupar els documents seguint determinada lògica. Hi ha diferents tipus de "bucket" (és a dir, criteris per agrupar dades):

*"**Date Histogram**" : Agrupa documents per data (per tant, normalment es basarà en el camp "timestamp"). En general s'utilitza per mostrar la variació de valors numèrics al llarg del temps. La mida del grup (és a dir, l'interval de temps que defineix els límits en cada agrupació: grups de 5 segons, de 10 minuts, etc) és únic però personalitzable

*"**Histogram**": Agrupa documents segons el valor d'un determinat camp numèric sencer: tots els documents que tinguin el mateix valor per aquest camp de referència pertanyeran al mateix "bucket". En general s'utilitza per mostrar la variació dels valors d'un altre camp respecte aquest camp de referència.

***Terms**": Agrupa documents segons el valor d'un determinat camp de cadena: tots els documents que tinguin el mateix valor per aquest camp de referència pertanyeran al mateix "bucket". En general s'utilitza per mostrar la quantitat de documents que existeixen amb cada valor diferent d'aquest camp de referència.

*"**Range**": Permet especificar un rang de valors per un camp numèric. Un cas especial és el "bucket" "**IPv4 Range**", el qual permet especificar un rang d'adreces IPs

*"**Filters**": Permet especificar un filtre DQL per definir les dades que pertanyen al "bucket"

NOTA: Per més informació sobre casos d'ús concrets d'aquests (i altres) tipus de "buckets" es pot consultar https://qbox.io/blog/comprehensive-guide-to-buckets-aggregations-in-elasticsearch

2) Definir una "Metric": És a dir, definir el càlcul a realitzar sobre els documents agrupats en cada "bucket" per tal d'obtenir un determinat valor únic (mitjana, recompte, suma, min, max, etc.), diferent per cada "bucket".

NOTA: Per més informació sobre casos d'ús concrets de les mètriques més comunes es pot consultar https://qbox.io/blog/comprehensive-guide-to-elasticsearch-metrics-aggregations-part-i i https://qbox.io/blog/comprehensive-guide-to-elasticsearch-metrics-aggregations-part-ii

3.-a) Vés al link "**OpenSearch Dashboards" -> "Visualize**" del menú principal per crear una gràfica de punts (per això s'ha d'escollir la visualització "Line") que, després d'haver triat l'"índex pattern" "pepa*", mostri en l'eix de les X un "bucket" de tipus "Date Histogram" amb el camp "timestamp" com a referència amb un interval de 10 segons (això vol dir que les agrupacions dels eventuals valors tindran cadascuna "'una mida" de 10 segons) i en l'eix de les Y mostri la mitjana de tots els valors del camp "log" (que és de tipus sencer gràcies al "mapping" que vam definir-li en la plantilla: si no ho haguéssim fet OpenSearch l'hauria assignat un tipus cadena i llavors no podríem fer aquest apartat!) encabits en cada agrupació (és a dir, en cada interval de 10 segons). Finalment, clica sobre el botó "Update" (el qual mostra el símbol de "play") per renderitzar la gràfica. ¿Què veus?

b) Personalitza l'aparença de la gràfica anterior anant a la pestanya "Metrics & Axes" i, sota l'apartat "Average log", canviant el valor de l'opció "Chart type" per a què sigui "Area" en comptes de "Line", i canviant el valor de l'opció "Line mode" per a què sigui "Smoothed" en comptes de "Straight". Guarda aquesta visualització amb el botó "Save" que apareix al menú horitzontal de links de la zona superior dreta del panel web (amb el nom que vulguis).

bII) ¿Què passa si sel.lecciones, encara a la pestanya "Metrics & Axes", el valor "Vertical" a l'opció "Align" que apareix sota l'apartat "X-axis"? D'altra banda, ¿per a què serveix l'apartat "Legend position" que apareix a la pestanya "Panel settings"? ¿I què mostra el link "Inspect" del menú horitzontal de links?

> NOTA: Més opcions interessants mostrades en aquest panell d'edició de gràfics, i que veurem en propers exercicis, són, per exemple, la possibilitat d'actualitzar de forma automàtica els gràfics (sense haver de clicar manualment, doncs, al botó "Refresh") gràcies a la manipulació de la icona de calendari (i concretament, el seu apartat "Refresh every"), la qual es convertirà llavors en la icona d'un rellotge, així com també la possibilitat d'afegir filtres (mitjançant el desplegable "Add filter" mostrat a la part superior esquerra de la finestra) per tal de només visualitzar al gràfic les dades que concordin amb la condició indicada, que generalment serà del tipus *"nomcamp" operador "valor"*

c) Vés al link "**OpenSearch Dashboards" -> "Dashboard**" del menú principal per tal de crear un nou "dashboard" que inclogui un sol panel mostrant la visualització anterior a pantalla completa. ¿Quines opcions tens disponibles al botó de la icona de la roda dentada que apareix a la cantonada superior dreta de la visualització recentment afegida al dashboard? Guarda finalment aquest dashboard amb el botó "Save" que apareix al menú horitzontal de links de la zona superior dreta del panel web (amb el nom que vulguis).

> NOTA: Per obtenir més informació sobre com administrar "dashboards", pots consultar https://www.elastic.co/guide/en/kibana/current/dashboard-getting-started.html

d) ¿Per a què serveix el link "Share" que apareix al menú superior dret de la secció "OpenSearch Dashboards" ->"Dashboards" (tant si és de tipus "Permalink" o bé "Embed Code")? ¿I el mateix link que apareix a la secció "OpenSearch Dashboards" -> "Visualize"? ¿I el mateix link que apareix a la secció "OpenSearch Dashboards" -> "Discover"?

4.-a) Assegura't de tenir instal·lat (dels exercicis anteriors) el servidor Apache a la mateixa màquina virtual de treball on tens el Fluent-Bit i el "pod" OpenSearch/Dashboards. Seguidament, modifica la configuració del plugin d'entrada "Tail" del FluentBit per a què ara obtingui les dades d'entrada del contingut que vagi apareixent dins del fitxer "/var/log/apache2/access.log" (a Ubuntu) o "/var/log/httpd/access_log" (a Fedora)

> NOTA: En el cas de voler posar varis fitxers a monitoritzar en una sola directiva *Path* de l'"input" Tail de FluentBit (que no és el cas d'ara però podria ser útil en alguna altra situació), recorda que es poden indicar comodins (*,?,[]) o també una llista de fitxers concrets separats per comes. En tot cas, però, si es volen gestionar documents provinents de diferents fitxers "log" de forma diferenciada, el més recomanable és indicar sengles "inputs" Tail per cada fitxer respectivament. Fent-ho així, a més, es podrien etiquetar els documents entrants de forma diferent i fer servir aquesta etiqueta per operar amb aquestes entrades de forma diferent mitjançant filtres (o sortides) diferenciades

aII) Modifica també la configuració del Fluentbit per a què ara tingui un filtre nou com aquest (¿què fa?)...

```
[FILTER]
  Name parser
  Match *
```

Parser apache2
Key_name log

...i canvia també el nom de l'índex a emmagatzemar a l'OpenSearch de "pepa" a "apache"

> NOTA IMPORTANT: Estem suposant que a l'arxiu de configuració del FluentBit, concretament sota la secció *[SERVICE]*, existeix la línia *Parsers_File /usr/local/etc/fluent-bit/parsers.conf* Si no aparegués, FluentBit no sabria on trobar la definició dels "parsers" predefinits, com ara justament l'anomenat "apache2" o un altre també molt important, l'anomenat "json", estudiat anteriorment al PDF monogràfic del FluentBit

Reinicia finalment el servei (*sudo systemctl restart fluent-bit*) per aplicar els canvis.

> NOTA: És important tenir en compte la definició del parser "apache2" dins del fitxer "/usr/local/etc/fluent-bit/parsers.conf" per tal de conèixer el nom dels futurs camps que aquest parser generarà pels documents a enviar a OpenSearch

b) Obre un navegador a la màquina real i vés a la pàgina "index.html" oferida pel servidor Apache. Tot seguit vés a pàgines inventades uns quants cops (de l'estil http://ip.Serv.Apache/asdfa o http://ip.Serv.Apache/erty) i també visualitza la pàgina existent "index.html"

c) Vés ara al link "OpenSearch Plugins" ->"Index management" -> "Indices" del panell web de Dashboards i observa si apareix un nou índex anomenat "apache" . Quan aparegui, vés al link "Management" -> "Stack management" ->"Index patterns" del mateix apartat i crea un "índex pattern" anomenat "apache*" (fent servir un altre cop el camp "timestamp" com a camp temporal de referència).

d) Vés a l'apartat "OpenSearch Dashboards" -> Discover" del menú principal un altre cop. A la caixa de text on es poden escriure els filtres de consulta (l'anomenarem "capsa DQL"), escriu el filtre *path:*asdf** i digues quins documents veus i per què, i quants es mostren en relació als que es mostren sense cap filtre (aquest número es pot saber observant la quantitat de "hits" mostrada a la part central, sota el diagrama de barres).

e) Escriu ara a la capsa DQL el filtre *code:404* . ¿Què veus ara? ¿I si escrius el filtre *code:404 or code:200*?

f) En comptes d'indicar al filtre un determinat camp on realitzar la recerca, es poden escriure filtres de "text lliure" que buscaran els valors concordants en tots els camps dels documents (incloent el camp "_source"). Prova-ho escrivint els següents filtres a la capsa DQL i observa quins documents es mostren en cada cas i en quin camp s'ha trobat cada valor trobat:

> *GET*
> *Get*
> *get*
> *g**
> *g?t*
> *"get"*

> NOTA: Com s'haurà comprovat en aquest apartat, les recerques "globals" són case-insensitive, admeten els comodins "*" i "?" i permeten utilitzar cometes per especificar concordància exacta. En canvi, les capacitats de les recerques sobre un determinat camp (com les que hem fet a l'apartat anterior) depenen del tipus de camp en qüestió: no tots els camps són analitzats per defecte, i això vol dir que les recerques sobre ells podrien ser case-sensitive i no admetre comodins. Per més informació sobre diferents possibilitats a l'hora d'escriure filtres, podeu consultar https://logz.io/blog/kibana-tutorial/ En tot cas, el nom dels camps, si s'indiquen en el filtre, sempre son case-sensitive

g) Segueix els següents passos per realitzar una visualització de tipus "Pie" a partir de l'index pattern "apache*" amb les següents característiques i clica llavors al botó "Play": ¿què obtens?:

> -"Bucket" de tipus "Split slices" amb una agregació de tipus "Terms" i sel.leccionant el camp "code.keyword" com a referència. Això generarà grups de documents que a aquest camp tinguin com a valor la mateixa cadena
>
> -Com a mètrica "Slice size" deixar el valor "Count". Això farà que es compti el número de documents agrupats a cada "bucket" (que serà la quantitat a visualitzar a la gràfica de porcions)

h) Canvia ara el camp de referència de "code.keyword" a "path.keyword" i torna a donar-li al "play". ¿Quina gràfica veus ara? ¿I si canvies el camp a "method.keyword"? ¿I si canvies el camp a "host.keyword"? ¿I si canvies el camp a "agent.keyword"?

> NOTA : Una agregació diferent de "Terms" és "Significant terms" però no la farem servir. El seu significat es pot consultar a https://www.elastic.co/guide/en/elasticsearch/reference/current/search-aggregations-bucket-significantterms-aggregation.html, on també es mencionen diferents possibilitats d'ús amb exemples reals. Un altre tutorial força aclaridor sobre les agregacions de tipus "Significant terms" és https://qbox.io/blog/a-deep-dive-into-significant-terms-and-significant-text-bucket-aggregations-in-elasticsearch

5.-a) Vés al link "Management" -> "Stack management" -> "Saved objects". ¿Què hi veus? ¿Què et permeten fer les icones que apareixen sota la columna "Actions"?

aII) ¿Per a què creus que pot servir el botó "Export" que hi apareix (juntament amb el botó "Import" present a la barra superior)? ¿En quin format s'implementen els objectes exportats?

b) Vés al link "Management" -> "Stack management" -> "Advanced settings". ¿Per a què serveix l'opció "Date format" indicada dins de la secció "General"? ¿I l'opció "Timezone for date formatting"? ¿I l'opció "Number format"? ¿I l'opció "Dark mode"? ¿I l'opció "Time filter quick ranges"? ¿I l'opció "Default sort direction" (dins de la secció "Discover")?

c) Vés al link "Management" -> "Dev Tools" del menú principal i, un cop allà, escriu a la primera línia del panell gris esquerra la comanda *GET nomindexqualsevol/_search* i tot seguit pulsa el botó "Play" que apareix a la cantonada superior dreta d'aquest mateix panell. ¿Què veus al panell dret?

cII) Ara escriu a la primera línia del panell gris esquerra la comanda *DELETE nomindexqualsevol* i pulsa de nou el botó "Play". ¿Què passa ara? ¿I si executes la comanda *DELETE _template/nomplantillaqualsevol?* ¿A quina comanda de terminal, doncs podria substituir aquesta finestra?

6.-a) Vés al link "OpenSearch Plugins" -> "Security" i a partir d'aquí:

> * Clica en el botó "Review authentication i authorization". Després de llegir les explicacions que allà s'hi mostren (i també la "nota" d'aquest apartat, a sota), digues què significa que l'únic "domain name" activat a secció "Authorization sequences" sigui l'anomenat "basic_auth_internal_domain" i que no n'hi hagi cap activat a la secció "Authorization".
>
> * Clica en el botó "Explore existing roles". Després de llegir les explicacions que allà s'hi mostren, digues què és un "rol". En concret, ¿per a què serveix el rol "readall" (pots clicar-hi a sobre del seu nom per obtenir els detalls)? Tot seguit, crea un rol nou anomenat "pepes" que només tingui el permís de crear índexs i prou (això a la pràctica consisteix en assignar un "Index permissions" -els "Cluster permissions" tenen a veure més amb la gestió del clúster internament- que afecti a tots els índexs -cal indicar "*" al nom- i que sigui del grup predefinit "create_index" -apareixerà la llista de grups a triar en un desplegable-; per conèixer la llista de permisos concrets que formen part d'aquests grups es pot anar a "OpenSearch Plugins" -> "Security" -> "Permissions").
>
> * Clica en el botó "Create internal user" i crea allà un nou usuari intern anomenat "pepe" que pertanyi al rol "pepes"
>
> > NOTA: Tot el que hem fet a l'apartat anterior s'ha basat en fer servir un "backend" (és a dir, una base de dades) intern propi d'OpenSearch on s'emmagatzemen els usuaris reconeguts i rols/permisos associats. En implementacions grans, però, és preferible utilitzar altres "backends" més especialitzats (com per exemple un servidor LDAP). Això, no obstant, implica una edició manual de diversos fitxers de configuració que se surt de l'àmbit d'aquest document. Per més informació sobre aquest tema, consulta https://opensearch.org/docs/latest/security-plugin/configuration/configuration/ (i també https://opensearch.org/docs/latest/security-plugin/configuration/yaml/)

aII) Tanca la sessió en Dashboards de l'usuari "admin" i entra-hi de nou però amb l'usuari "pepe". ¿Pots fer alguna cosa? Vés en canvi a "Management" -> "Dev tools" i executa la comanda *PUT lalala*. ¿Què fa?

> NOTA: El "plugin" "Security" d'OpenSearch proporciona una API per tal de realitzar totes les tasques anteriors (creació de rols, d'usuaris, mapeig entre ells, etc) directament des de peticions HTTP (de fet, el propi Dashboards és el que fa). Si es vol conèixer com realitzar aquestes tasques fent servir per exemple la comanda *curl* al terminal, es pot consultar la següent documentació: https://opensearch.org/docs/latest/security-plugin/access-control/users-roles/ , https://opensearch.org/docs/latest/security-plugin/access-control/permissions/ , https://opensearch.org/docs/latest/security-plugin/access-control/default-action-groups/ , https://opensearch.org/docs/latest/security-plugin/access-control/document-level-security/ i https://opensearch.org/docs/latest/security-plugin/access-control/api/
> NOTA: Pots anar a https://opensearch.org/docs/latest/security-plugin/index/ per saber més sobre aquest "plugin" en general

b) Vés al link "OpenSearch Plugins" -> "Reporting" i allà defineix un informe a partir d'alguna visualització (o dashboard complet, com vulguis) que tinguis guardada, en format PDF i amb capçaleres de cap i de peu. Fes que aquest informe mostri les dades de la darrera mitja hora i fer precisament que es vagin generant diferents informes d'aquest tipus periòdicament cada mitja hora.

bII) No cal que t'esperis mitja hora per obtenir l'informe: si cliques sobre el seu nom a la llista de definicions d'informes aniràs a la seva pàgina de detalls i allà, clicant sobre l'enllaç "PDF" obtindràs l'informe generat en aquell instant. Fes-ho i observa què obtens.

> NOTA: Consulta https://opensearch.org/docs/latest/dashboards/reporting/ per saber més sobre aquest "plugin". També és interessant l'article https://opensearch.org/blog/feature/2021/06/feature-highlight-reporting/

c) Vés al link "OpenSearch Plugins" -> "Query Workbench" ¿Què mostra la consulta *SHOW tables LIKE %;* ? ¿I la consulta *SELECT * FROM apache*;* ? ¿Per a què serveix el botó "Download" que apareix sobre els resultats?

cII) Llegeix https://opensearch.org/docs/latest/search-plugins/sql/ppl/index per saber què és "PPL" i quina relació té amb el "Query Workbench"

> NOTA: Consulta https://opensearch.org/docs/latest/search-plugins/sql/index/ per saber més sobre aquest "plugin"

d) Llegeix https://opensearch.org/docs/latest/observing-your-data/alerting/index i explica per a què serveix el plugin "Alerting" (en combinació amb el plugin "Notifications") del Dashboards

> NOTA: És molt interessant aquest aspecte de les alertes però necessitaríem un altre document monogràfic per tractar-les

e) ¿Què s'explica a https://opensearch.org/docs/latest/install-and-configure/install-opensearch/plugins/ ?

Un **HIDS** ("Host Intrusion Detection System") és un software que monitoritza un sistema per tal de detectar activitat maliciosa o infraccions de política. La seva tasca és examinar els esdeveniments dins d'un ordinador, no el trànsit de xarxa que pugui rebre/enviar.. Un agent HIDS utilitza diversos mètodes de detecció (com ara la supervisió de registres, la detecció de "rootkits" -mitjançant mètodes de verificació de checksums-, la supervisió de la integritat de fitxers, etc.), i permet alertar sobre esdeveniments específics i canvis de configuració. Si hi hagués més d'un amfitrió HIDS a la vostra xarxa, no hauria de caldre iniciar sessió en cadascun d'ells per obtenir "feedback": és per això que un sistema HIDS distribuït hauria d'incloure un mòdul de control centralitzat (anomenat SIEM) i, a més, tenir xifrades les comunicacions entre aquest i els agents amfitrions.

Un **NIDS** ("Network Intrusion Detection System") és un software que monitoritza el trànsit de la xarxa per detectar activitats malicioses o infraccions de política. Com a tal, un NIDS típic ha d'incloure un "sniffer" de paquets per poder analitzar el trànsit de xarxa i utilitza un conjunt predeterminat de regles de "mal comportament" per fer-les coincidir amb el paquets recollits i així identificar trànsit sospitós. Tota infracció detectada normalment genera una alerta o es recull de forma centralitzada mitjançant un sistema SIEM.

Un **SIEM** ("Security Information Event Management") és un sistema que proporciona anàlisis en temps real de les alertes de seguretat generades per diversos orígens de la xarxa (software o hardware), gràcies a realitzar correlació d'esdeveniments i, a partir d'aquí, proporcionar intel·ligència sobre les amenaces. Un SIEM configurat correctament pot ajudar a detectar atacs i disminuir la quantitat de temps que un adversari maliciós pot estar a la xarxa.

A partir de l'ús de Falco i la suite FOsD es pot implementar un HIDS amb SIEM integrat. Això és el que farem a continuació: primer instal.larem el Falco, el qual serà el generador de les alertes i, per tant, d'orígen dels missatges a enviar a un servidor central OpenSearch/Dashboards, el qual ens permetrà monitoritzar i visibilitzar totes aquestes dades, a més de tractar-les estadísticament de forma centralitzada.

7.-a) A la màquina on ja tens instal.lat dels exercicis anteriors FluentBit, OpenSearch i Dashboards, ara instal.la-hi Falco (llegeix el PDF corresponent si no recordes com s'havia de fer):

b) Comprova que Falco ja estigui en marxa (*systemctl status falco-modern-bpf*) i que les seves regles per defecte ja funcionin. Això últim ho pots comprovar executant algun event sospitós (com ara *sudo touch /bin/virus* o bé *sudo touch /etc/fstab*) i observant seguidament la sortida de la comanda *journalctl -u falco -p err*

> NOTA: Estem suposant que la configuració de Falco és la per defecte, on gràcies a tenir activada la línia *syslog_output* de l'arxiu de configuració "falco.yaml" totes les incidències de seguretat són enviades al registre-journal del sistema. Si no fos el cas, caldria editar aquesta línia convenientment. D'altra banda, recorda que el format concret del missatge enviat al Journal per cada event detectat es podria modificar a la línia "output" de la regla corresponent, definida a l'arxiu "falco_rules.yaml"

La idea seria ara que, en gravar Falco un eventual missatge d'alerta al Journald, hi hagi un dimoni FluentBit "subscrit" que detecti l'aparició d'aquest nou missatge i el reenvïi a un servidor OpenSearch. Així doncs, a continuació muntarem tota aquesta infraestructura

c) Escriu una configuració dins del fitxer "/usr/local/etc/fluent-bit/fluent-bit.conf" que...:

* Tingui comentades les eventuals seccions *[INPUT]* i *[OUTPUT]* que allà hi puguin haver presents
* Tingui afegides (al final del fitxer) les següents línies:

```
[INPUT]
  Name systemd
  Systemd_filter_type and
  Systemd_filter _COMM=falco
  Systemd_filter PRIORITY=3

[FILTER]
   Name modify
   Match *
   Rename _COMM COMM

[OUTPUT]
   Name opensearch
   Match *
   Host 127.0.0.1
   Port 9200
   Index falco
   HTTP_User admin
   HTTP_Passwd Un4C0ntraSs3ny4C0mplicad4_
   Tls on
   Tls.verify off
   Suppress_Type_Name On
```

... i tot seguit inicia el servei Fluent-bit (*sudo systemctl start fluent-bit*)

NOTA: El valor numèric del camp PRIORITY indica la "gravetat" del missatge: un nº 3 equival a "error". Nombres menors equivalen a fallades més greus i nombres majors a avisos i noticies no tan "perillosos"

NOTA: El filtre "modify" és necessari perquè OpenSearch és incapaç de fer agregacions on intervenen camps el nom dels quals comença per "_". És per això que canviem el nom del/s camp/s que sabem que properament voldrem processar en algun dashboard. En les versions més modernes de Fluent-Bit hi ha una directiva del "plugin" d'entrada Systemd que ja ho fa això automàticament (*Strip_Underscores On)*, però s'ha volgut deixar la implementació del filtre "modify" per curiosa.

d) Obre el navegador de la teva màquina real per accedir al servidor Dashboards. Crea una plantilla, tal com ja has fet anteriorment, que en aquest cas assigni el tipus "integer" al camp anomenat "PRIORITY", pertanyent a un eventual "index pattern" anomenat "falco*"

NOTA: Una altra forma d'haver fet el mateix és havent anat al link "Management" -> "Dev Tools" i, un cop allà, escrivint a la primera línia del panell gris esquerra la comanda següent (i tot seguit pulsant el botó "Play" que apareix a la cantonada superior dreta d'aquest mateix panell per executar-la).

```
PUT _template/plantillafalco
{
        "index_patterns": [ "falco*" ],
        "mappings": {
                "properties" : {
                        "PRIORITY": { "type": "integer" },
                        "timestamp": { "type": "date", "format": "yyyy-MM-dd HH:mm:ss" }
                }
        }
}
```

e) Provoca algun event sospitós a la màquina virtual (com ara *sudo touch /bin/virus* o *sudo touch /etc/fstab* o *sudo rm /bin/virus* , etc) i seguidament comprova que els missatges d'avís corresponents generats per Falco s'hagin guardat dins un índex OpenSearch anomenat "falco" (això ho pots fer, recorda, anant a l'apartat "OpenSearch Plugins->"Index management"->"Indices" del Dashboards, o bé, alternativament, executant *curl -k -u "admin:Un4C0ntraSs3ny4C0mplicad4_" https://ip.serv.OpenSearch:9200/_cat/indices* i veient com aquest índex apareix; en tot cas, si vas provocant varis events sospitosos la quantitat de documents existents dins d'aquest índex hauràs de veure que anirà variant).

f) Afegeix, des de l'apartat pertinent del Dashboards, un nou "index pattern" anomenat "falco*" i tot seguit sel·lecciona aquest nou "index pattern" dels disponibles a la pàgina "Discover": hauràs d'observar llavors els missatges d'error rebuts. Fes, finalment, que en aquest panell "Discover" només es vegin tres columnes: "timestamp", "MESSAGE" i "PRIORITY".

g) ¿Què passa quan al quadre de recerca de la zona superior del panel "Discover" de Dashboards escrius l'expressió "PRIORITY *>= 3 and PRIORITY <= 5*" (amb la sintaxis DQL activada) o bé *"PRIORITY:[1 TO 3]"* (amb la sintaxis Lucene)?

NOTA: Per saber més sobre les diferències sintàctiques entre els filtres Lucene i els filtres DQL podeu consultar https://www.elastic.co/guide/en/kibana/current/lucene-query.html i https://www.elastic.co/guide/en/kibana/current/kuery-query.html respectivament

h) ¿Quina és la diferència entre els valors dels camps _COMM (renombrat a "COMM"), _EXE, _CMDLINE i _SYSTEMD_UNIT d'un event qualsevol dels mostrats a la pantalla "Discover"?

i) Atura el servei Fluent-Bit i modifica la seva configuració per a què ara "xucli" els missatges provinents igualment de Falco però que ara tinguin qualsevol prioritat (és a dir, comenta la línia S*ystemd_filter PRIORITY=3*). Torna a posar en marxa Fluent-Bit i ara torna a provocar algun error (com ara *sudo touch /bin/virus* o *sudo touch /etc/fstab* o *sudo rm /bin/virus* , etc). Observa com, efectivament, a la pantalla "Discover" comencen a aparèixer missatges amb prioritats diferents de 3.

j) Realitza una visualització de tipus "Pie" on, després de sel·leccionar l'índex pattern "falco*" d'entre tots els possibles que apareixin llistats al quadre emergent, a l'apartat "Metrics" mantinguis "Count" com a valor de l'ítem "'Slice size" i on a l'apartat "Bucket" (de tipus "Split Slices") sel.leccionis una "Aggregation" de tipus "Histogram", el valor "PRIORITY" al desplegable "Field" i el valor "1" al desplegable "Minimum interval". ¿Quin és el significat del diagrama resultant?

k) Grava aquest diagrama anterior amb el nom de "aaa" i tot seguit crea un nou "dashboard" que inclogui aquest diagrama. Prova uns quants errors més i tot seguit pulsa el botó "Refresh" del dashboard: ¿què li passa al diagrama? ¿Per a què serviria, en aquest sentit, l'opció "Refresh every" disponible al desplegable mostrat en clicar sobre la icona del calendari -la qual es convertirà en la d'un rellotge si s'activa- que apareix a la cantonada superior dreta del dashboard (la qual, per cert, també apareix a la finestra "Discover"). Grava el dashboard amb el nom de "xxx".

> NOTA: Un pas extra que seria convenient de fer és "parsejar" el camp MESSAGE obtingut de Falco per obtenir i separar les dades concretes ubicades dins del missatge que ens interessin. Però aquesta pràctica la farem als propers exercicis, on treballarem amb missatges registrats provinents no de Falco sinó d'altres programes, però la idea és la mateixa

El fet d'obtenir les dades del Journal del sistema fa que qualsevol aplicació que gravi els seus logs allà sigui susceptible de ser utilitzada com orígen de dades a emmagatzemar a OpenSearch. Per tant, no només podem guardar informació valiosa provinent de Falco sinó que també podrem obtenir-ne d'altres programes que considerem interessants, com ara la comanda *sudo* (per saber, per exemple, qui, quan i quina comanda privilegiada han volgut executar al sistema -amb éxit o no-), o el servidor SSH (per saber, per exemple, qui, quan i des d'on es realitzen els inicis de sessió -vàlids o no-), etc. Veiem-ho primer amb un exercici genèric, per començar.

8.-a) Atura el servei Fluent-Bit posat en marxa a l'exercici anterior i torna a modificar ara la seva configuració per a què ara "xucli" els missatges de qualsevol prioritat provinents de qualsevol programa (és a dir, comenta la línia S*ystemd_filter _COMM=falco* present a la configuració de l'exercici anterior i deixa la resta tal com està). Torna a posar en marxa Fluent-Bit i observa com, quasi immediatament, a la pantalla "Discover" de Dashboards (havent triat per mostrar l'"index pattern" "falco*") comencen ara a aparèixer missatges provinents no només de Falco sinó de tots els programes que envien logs al Journald.

b) Realitza ara una altra visualització de tipus "Pie" on, després de sel·leccionar l'índex pattern "falco*" de nou, a l'apartat "Metrics" mantinguis "Count" com a valor de l'ítem "'Slice size" i a l'apartat "Bucket" (també de tipus "Split Slices") sel.leccionis ara una "Aggregation" de tipus "Terms", el valor "COMM.keyword" al desplegable"Field" i el valor "Metric:Count" al desplegable "Order by". ¿Quin és el significat del diagrama resultant?

c) El diagrama actual mostra el total de missatges separats per programa originador però... ¿què hauríem de fer si només volguéssim veure el total de missatges de prioritat=3 o 4 per programa originador? Hauríem de fer un filtre; això ho pots fer pulsant a l'enllaç "Add filter" mostrat a la cantonada superior esquerra del diagrama i posa com a condició "PRIORITY is between 3 and 5" (el darrer nombre del rang no és inclòs a la recerca) ¿Què veus ara al diagrama? Deshabilita el filtre.

d) Sense eliminar el Bucket "Split slices" que ja tens, afegeix-ne un altre Bucket a sota (també de tipus "Split Slices") i sel.lecciona ara una "Sub-aggregation" de tipus "Histogram", indicant el valor "PRIORITY" al desplegable"Field" i ja està ¿Quin és el significat del diagrama resultant? Torna a habilitar el filtre creat a l'apartat anterior. ¿Què veus ara?

Tal com hem dit, una font d'informació sobre seguretat molt important són els registres del programa *sudo*. En el següent exercici veurem com processar-los amb OpenSearch/Dashboards.

9.-a) Atura el servei Fluent-Bit i seguidament escriu una configuració dins del fitxer "/usr/local/etc/fluent-bit/fluent-bit.conf" que deixi la seva secció [SERVICE] sense modificar però que la resta del fitxer tingui el següent contingut (¿per a què serveixen els diversos filtres indicats?). A continuació reinicia el servei:

```
[INPUT]
  Name systemd
  Systemd_filter _COMM=sudo
```

```
[FILTER]
  Name modify
  Match *
  Rename _COMM COMM
[FILTER]
  Name grep
  Match *
  Regex MESSAGE COMMAND=
[OUTPUT]
  Name opensearch
  Match *
  Host 127.0.0.1
  Port 9200
  Index falco                    #Sí, afegirem els nous valors al mateix índex "falco*" d'exercicis anteriors
  HTTP_User admin
  HTTP_Passwd Un4C0ntraSs3ny4C0mplicad4_
  Tls on
  Tls.verify off
  Suppress_Type_Name On
```

b) Executa unes quantes comandes fent servir *sudo* (per exemple: *sudo fdisk -l*, *sudo cat /etc/shadow*, etc) i seguidament refresca la pàgina "Discover" del panell web Dashboards ¿Quins nous missatges hi apareixen? (pots triar veure només el camp "MESSAGE" per observar-ho millor). Compara aquests missatges amb els que et mostra la comanda *journalctl _COMM=sudo* i dedueix a partir d'aquí per a què serveix el filtre "grep" afegit a la configuració de FluentBit indicada a l'apartat anterior.

> NOTA: Observa com els nous events provinents de sudo s'emmagatzemen en el mateix índex on abans s'estaven emmagatzemant els events provinents del Falco (és per això que no ha calgut carregar cap plantilla nova ni fer un "index pattern" nou). Tot i que no seria el més recomanable, pots comprovar que és perfectament possible tenir en un mateix índex documents amb estructura totalment diferents.

Tot i que ja ho sabíem d'exercicis anteriors, a l'apartat anterior hauràs observat com el camp MESSAGE d'un registre generat per *sudo* en haver introduït la contrasenya correcta en algun dels tres intents té el següent aspecte: *usuari : TTY=pts/1 ; PWD=/home/usuari ; USER=root ; COMMAND=/bin/ls -l /etc* mentre que el registre dels tres intents fallits en introduir la contrasenya al *sudo* té el següent aspecte: *usuari : **3 incorrect password attempts** ; TTY=pts/1 ; PWD=/home/usuari ; USER=root ; COMMAND=/bin/ls -l /etc*

> NOTA: També hi hauria la possibilitat de què l'usuari que hagués executat *sudo* no en tingués permisos perquè no estigués a l'arxiu "/etc/sudoers". En aquest cas el registre seria el següent (tot i que no el tindrem en compte en aquest exercici)
> *usuari : **user NOT in sudoers** ; TTY=pts/1 ; PWD=/home/usuari ; USER=root ; COMMAND=/bin/cat /etc/shadow*

c) Després d'haver llegit el paràgraf blaus anterior, afegeix ara al FluentBit un filtre que permeti separar els valors que apareixen al camp "message" per tal de poder-los estudiar millor. Concretament, això ho hauràs de fer afegint les següents línies a la configuració ja existent de FluentBit (abans de la secció [OUTPUT])...

```
[FILTER]
   Name parser
   Match *
   Parser sudo
   Key_name MESSAGE
```

...i afegint al final del fitxer "/usr/local/etc/fluent-bit/parsers.conf" el següent contingut (respecteu els espais en blanc, són importants!; si tens algun problema recorda que pots utilitzar www.rubular.com) :

```
[PARSER]
  Name sudo
  Format regex
  Regex ^[ ]+ (?<usuari>[^ ]+) :(?<error> 3 incorrect password attempts ;)? TTY=(?<tty>[^ ]+) ; PWD=(?<pwd>[^ ]+) ; USER=(?<superuser>[^ ]+) ; COMMAND=(?<comanda>.*)$
```

NOTA: La clau de l'expressió regular anterior és el "?" ubicat darrera missatge d'error: aquest símbol vol dir que l'expressió marcada entre parèntesi és opcional (és a dir, pot estar o no). Això implica que aquesta expressió serà vàlida tant pels missatges apareguts quan s'entra correctament la contrasenya com pels missatges apareguts quan no: la diferència serà el valor del camp "error" (res en el primer cas o la cadena "3 incorrect password attempts ;" en el segon)

d) Veient l'expressió regular anterior, ¿quin noms i possibles valors creus que tindran els camps del document resultant després d'haver sigut processat per aquest "parser"? Reinicia el servei FluentBit

e) Executa ara unes quantes comandes fent servir *sudo* (per exemple: *sudo fdisk -l, sudo cat /etc/shadow*, etc), algunes introduint correctament la contrasenya en algun intent dels tres possibles i unes altres sense introduir la contrasenya bé en cap d'aquest tres intents. Seguidament refresca la pàgina "Discover" del panell web Dashboards. ¿Quins nous missatges hi apareixen i quins camps tenen? (pots triar veure només els camps "error" i "comanda" per observar-ho millor).

A l'apartat anterior haureu vist que els nous camps generats a partir del "parser" que hem implementat apareixen com a "Unknown field" si despleguem un document qualsevol. Això és perquè el "mapping" de l'índex "falco-*" es va establir la primera vegada que s'hi va inserir un document i en aquell moment aquests dos camps no hi eren. No obstant, afortunadament, el "mapping" de l'índex s'actualitza automàticament dins l'OpenSearch cada cop que van apareixent camps nous als documents que van entrant. Llavors, ¿on és el problema? El problema està en què Dashboards té definit un "índex pattern" que té constància d'una estructura de camps que es correspon amb el "mapping" antic (no pas amb el nou) i aquest "index pattern" sí que no s'actualitza automàticament. Això implica que Dashboard no sabrà de quin tipus són els camps nous (si cadena, si sencer, si data, etc) fins que no hagi refrescat l'"index pattern" associat a l'índex en qüestió i així adaptar-lo, mitjançant aquest "refresc", al seu nou "mapping". Fent això llavors sí que Dashboards podrà tenir constància de l'existència dels nous camps i gestionar-los convenientment.

f) Per fer el "refresc" explicat al paràgraf blau anteriorment cal ara al panel "Management" -> "Stack Management" ->"Index Patterns" de Dashboards i allà, un cop sel·leccionat l'"index pattern" adient, clicar sobre la icona d'"actualitzar" que apareix a la zona superior dreta (al costat de la icona de la paperera). D'aquesta manera es veurà com el número de camps reconeguts augmenta i, si tornem a la pantalla "Discover", podrem comprovar que, ara sí, els camps generats per part del "parser" que hem definit a l'apartat c) són reconeguts com a camps de tipus text. Fes-ho. És important confirmar que el reconeixement ha sigut correcte abans de passar al proper exercici perquè si hi ha camps de tipus "unknown" Dashboards els ignorarà completament en el moment de voler sel·leccionar-los per realitzar gràfiques.

g) Realitza una visualització de tipus "Pie" on, després de sel·leccionar l'índex pattern "falco-*", a l'apartat "Metrics" mantinguis "Count" com a valor de l'ítem "'Slice size" i a l'apartat "Bucket" (de tipus "Split Slices") sel.leccionis una "Aggregation" de tipus "Terms", el valor "comanda.keyword" al desplegable"Field" i el valor "Metric:Count" al desplegable "Order by". ¿Quin és el significat del diagrama resultant? ¿Què li passa al diagrama si modifiques el rang de temps observat (al desplegable superior dreta) per un altre rang qualsevol i per què?

h) Realitza una visualització de tipus "Data Table" mostrant el mateix contingut que l'apartat anterior (però amb una altra forma). Concretament, a l'apartat "Metrics" manté "Count" com a valor de l'ítem "'Slice size" i a l'apartat "Bucket" (de tipus "Split Rows") sel.lecciona una "Aggregation" de tipus "Terms", el valor "comanda.keyword" al desplegable"Field" i el valor "Metric:Count" al desplegable "Order by"

i) Realitza una visualització de tipus "Vertical Bar" que mostri en l'eix de les Y la mètrica "Count" i en l'eix de les X un "bucket" de tipus "Date Histogram" amb el camp "timestamp" com a referència amb un interval de 10 segons. ¿Què et mostra la gràfica resultant?

iII) Ara afegeix, a la gràfica anterior, un altre "bucket" addicional (ara de tipus "Split Series"), amb una subagregació de tipus "Filters", on hauràs d'indicar el filtre *error:** , i pulsa el botó "Update". ¿Quin canvi veus a la gràfica?

NOTA: Compte en no afegir un segon filtre extra buit (per error)...això faria que s'afegís a la gràfica un nou color comptant tots els documents en total.

j) Realitza una altra visualització de tipus "Vertical Bar" que mostri en l'eix de les Y la mètrica "Count" i en l'eix de les X un "bucket" de tipus "Date Histogram" amb el camp "timestamp" com a referència amb un interval de 10 segons i, a més a més, un altre "bucket" (de tipus "Split Series"), en aquest cas amb una subagregació de tipus "Terms", on es triarà el valor del camp "comanda.keyword" com a disgregador del color de les barres. . ¿Què veus?

jII) Ara afegeix, a la gràfica anterior, un altre "bucket" addicional (ara de tipus "Split Series"), amb una subagregació de tipus "Filters", on hauràs d'indicar el filtre *error:** , i pulsa el botó "Update". ¿Quin canvi veus a la gràfica?

En el següent exercici veurem com processar registres generats per un servidor SSH. Si observem els "logs" que genera un servidor SSH en el Journald, veurem que el registre d'un intent d'inici de sessió vàlid d'un usuari existent té el següent aspecte: ***Accepted*** *password for root from 116.31.116.24 port 29160 ssh2* En canvi, el registre d'un intent d'inici de sessió invàlid (perquè s'hagi introduït malament la contrasenya) d'un usuari existent té el següent aspecte: ***Failed*** *password for root from 116.31.116.24 port 29160 ssh2* mentre que els registres d'un intent d'inici de sessió invàlid perquè ja el propi nom d'usuari no existeixi (això és molt típic en atacs de força bruta realitzats contra servidors SSH públics a Internet), tenen el següent aspecte (són dues línies): *Failed password for* ***invalid user*** *root from 116.31.116.24 port 29160 ssh2* i tot just a sota *Invalid user root from 10.0.2.2*

10.-a) Atura el servei Fluent-Bit i seguidament escriu una configuració dins del fitxer "/usr/local/etc/fluent-bit/fluent-bit.conf" que deixi la seva secció [SERVICE] sense modificar però que la resta del fitxer tingui el següent contingut (¿per a què serveixen els diversos filtres indicats?):

```
[INPUT]
  Name systemd
  Systemd_filter _COMM=sshd
[FILTER]
   Name grep
   Match *
   Regex MESSAGE password.for
[FILTER]
    Name parser
    Match *
    Parser sshd
    Key_name MESSAGE
[OUTPUT]
   Name opensearch
   Match *
   Host 127.0.0.1
   Port 9200
   Index falco
   HTTP_User admin
   HTTP_Passwd Un4C0ntraSs3ny4C0mplicad4_
   Tls on
   Tls.verify off
   Suppress_Type_Name On
```

...i afegint al final del fitxer "/usr/local/etc/fluent-bit/parsers.conf" el següent contingut (respecteu els espais en blanc, són importants!) :

```
[PARSER]
   Name sshd
   Format regex
   Regex ^(?<result>[^ ]+) password for(?<invalid> invalid user)? (?<usuari>[^ ]+) from (?<clientip>[^ ]+)
(?:.*)$
```

NOTA: Fixa't que la cadena "invalid user" es marca com opcions per recollir tant els missatges corresponents a usuaris existents (ja siguin exitosos o no) com inexistents

b) Veient l'expressió regular anterior, ¿quin noms i possibles valors creus que tindran els camps del document resultant després d'haver sigut processat per aquest "parser"? Inicia el servei FluentBit de nou (sí, afegirem els nous valors al mateix índex "falco*" d'exercicis anteriors)

c) Esborra, per començar de nou (és a dir, per a què tots els camps siguin reconeguts des del començament, adaptant-se igualment a la template associada, que no hem esborrat), l'índex "falco" que has emprat als exercicis anteriors (recorda que això ho pots fer, o bé escrivint la consulta *DELETE falco-** a la consola disponible en l'enllaç "Management"->"Dev tools" del menú principal o, alternativament, triant l'opció "Delete" del desplegable "Actions" que apareix en sel·leccionar l'índex en qüestió mostrat al panel "OpenSearch Dashboards"->"Index management"->"Indices")

cII) Esborra també l'"índex pattern" "falco*" (recorda que això ho pots fer clicant sobre la icona de la paperera del panel "Management"->"Stack Management"->"Index Patterns")

d) Inicia, si no ho està ja, el servidor "sshd" a la mateixa màquina virtual on tens FluentBit+ OpenSearch+Dashboard funcionant. Prova tot seguit d'accedir-hi via SSH des de la màquina real vàries vegades de diferents formes: emprant un usuari no existent, emprant un usuari existent però amb contrasenya incorrecta i emprant un usuari existent i amb contrasenya correcta (per tant, entrant amb èxit). Un cop fet això varis cops, crea un nou "index pattern" al Dashboards per poder gestionar el nou índex "falco-*" que haurà aparegut i tot seguit refresca la pàgina "Discover" del panell web principal. ¿Quins nous missatges hi apareixen? (pots triar veure només els camps "result", "invalid", "usuari" i "clientip" per observar-ho millor).

Tot i que sembla que ja està tot correcte, hi ha un detall que pot ser important d'"arreglar" si volem fer segons quines gràfiques correctament. Es tracta de què, per defecte, el camp "clientip" és tractat com de tipus "string" (perquè a la plantilla utilitza no es va definir res al respecte) però seria molt interessant que fos tractat com de tipus "ip", justament per poder fer "buckets" segons rangs d'IPs, o representacions sobre mapes amb les IPs geolocalitzades, etc. Ja sabem que la manera d'aconseguir que un determinat camp sigui d'un determinat tipus és establint el "mapping" adient (ja sigui al panell web pertinent o amb la consulta PUT pertinent, tal com hem vist ja). Desgraciadament, OpenSearch no permet canviar el "mapping" d'un índex ja existent (a no ser que sigui per afegir-ne camps nous); és a dir, no es pot canviar el tipus d'un camp ja existent en l'índex. Això ens deixa amb dues opcions: o bé eliminar l'índex que tenim i crear llavors un nou índex (buit) associant-lo amb el "mapping" desitjat (és a dir, indicant que el camp "clientip" és de tipus "ip") -amb la qual cosa perdríem la informació que hi havia a l'índex antic- o bé, reindexar l'índex que tenim en un altre índex (és a dir, copiar el contingut de l'índex antic en un de nou i aprofitar llavors per definir el nou "mapping" a l'índex de destí, entre altres possibles característiques) -amb la qual cosa podríem aprofitar tota la informació de l'índex antic-. Aquesta darrera opció, l'API corresponent de la qual està documentada a https://opensearch.org/docs/latest/opensearch/reindex-data, és molt interessant i és la que provarem ara

e) Vés al link "Management" -> "Dev Tools" de Dashboards i, un cop allà, escriu a partir de la primera línia del panell gris esquerra les dues comandes següents (una sota l'altra) i tot seguit pulsa el botó "Play" primer en la primera comanda i després en la segona. ¿Què és el que has fet i què has aconseguit amb això?

NOTA: El mateix es pot aconseguir mitjançant l'opció "ReIndex" del desplegable "Actions" que apareix en sel·leccionar l'índex a reindexar mostrat al panel "OpenSearch Dashboards"->"Index management"->"Indices", la qual mostrarà una pàgina on podrem indicar el nom i plantilla del nou índex

```
PUT nouindex
{
        "mappings":{
                "properties" : {
                        "clientip": { "type": "ip" },
                        "timestamp": { "type": "date", "format": "yyyy-MM-dd HH:mm:ss" }
                }
          }
}
```

```
POST _reindex
{
        "source":{ "index":"falco*" },
        "dest":{ "index":"nouindex" }
}
```

f) Crea un nou "index pattern" associat a l'índex "nouindex" i observa que el nou camp "clientip" reconegut sigui de tipus "ip". Observa també com a la pantalla "Discover" continues veient els mateixos documents que quan vas fer l'apartat d).

g) Realitza una visualització de tipus "Vertical Bar" que mostri en l'eix de les X un "bucket" de tipus "Date Histogram" amb el camp "timestamp" com a referència amb un interval de 10 segons i, a més a més, un altre "bucket" (de tipus "Split Series"), en aquest cas amb una subagregació de tipus "Terms", on hauràs d'indicar el camp "usuari.keyword" (per tal d'usar el seu valor com a disgregador del color de les barres). En l'eix de les Y ha d'haver la mètrica "Count". ¿Què veus?

gII) Ara afegeix, a la gràfica anterior, un altre "bucket" addicional (ara de tipus "Split Series"), amb una subagregació també de tipus "Terms", on hauràs d'indicar el camp "result.keyword", i pulsa el botó "Update". ¿Quin canvi veus a la gràfica?

h) Realitza una visualització de tipus "Tag Cloud" que mostri un "bucket" (de tipus "Tags") amb una agregació de tipus "Terms" amb el camp "usuari.keyword" com a referència. En l'apartat "Metrics" ha d'haver la mètrica "Tag size count". ¿Què veus?

i) Realitza una altra visualització de tipus "Vertical Bar" que mostri en l'eix de les X un "bucket" de tipus "Date Histogram" amb el camp "timestamp" com a referència amb un interval de 10 segons i, a més a més, un altre "bucket" (de tipus "Split Series"), en aquest cas amb una subagregació de tipus "IPv4 Range", on hauràs d'indicar el camp "clientip" (per tal d'usar el seu valor com a disgregador del color de les barres) i diferents rangs d'adreces IP (afegeix un parell de rangs que siguin com tu vulguis però que incloguin les IPs dels clients SSH que han accedit a la màquina). En l'eix de les Y ha d'haver la mètrica "Count". ¿Què veus?

j) Realitza una visualització de tipus "Metric" que mostri un "bucket" (de tipus "Split group") amb l'agregació "Terms" i el camp "result.keyword" com a referència. En l'apartat "Metrics" ha d'haver la mètrica "Count". ¿Què veus?

11.-Digues què fa i per a què serveix el programa explicat a https://www.hackplayers.com/2020/10/siem-durmiendo-con-el-enemigo.html (disponible a https://github.com/ElevenPaths/siemframework)