



EPICODE

Esercizio W24D4

Progetto

Importate su Splunk i dati di esempio "tutorialdata.zip":

- Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.
- Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente "djohnson" e mostrare il timestamp e l'ID utente.
- Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60". La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.
- Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.
- Crea una query Splunk per trovare tutti gli Internal Server Error.

Trarre delle conclusioni sui log analizzati utilizzando AI.

- Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.

Svolgimento punto 1

The screenshot shows the Splunk web interface with the following details:

- Search Bar:** The query entered is: `source="tutorialdata.zip:*" host="DESKTOP-8CAJRT0" Failed password| sort - Timestamp| rex field=_raw "reason: (<failure_reason>.)"`
- Results Summary:** 10.000 eventi (prima di 02/01/25 18:16:13,000) Nessun campionamento degli eventi.
- Event List:** The results list shows multiple entries of failed password attempts from the host `DESKTOP-8CAJRT0`. Each entry includes the timestamp (e.g., `Thu Dec 15 2024 12:42:06`), the source (e.g., `mailsv1 sshd[5276]`), and the reason (e.g., `Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2`). The list is sorted by timestamp.
- Left Sidebar:** Shows selected fields like `host`, `source`, and `sourcetype`, and a list of interesting fields including `# date_hour`, `# date_minute`, `# date_month`, `# date_second`, `# date_wday`, `# date_year`, `# date_zone`, `# index`, `# linecount`, `# punct`, `# splunk_server`, `# timeendpos`, and `# timestamppos`.
- Bottom Status:** Shows system status including CPU usage, memory, and disk usage.

Per il primo punto abbiamo semplicemente usato la query "Failed Password", che ci mostra tutti i tentativi di accesso di password errate.

Il **Timestamp** lo possiamo aggiungere con:

`sort - Timestamp` che farà vedere l'ora e il giorno dell'errore commesso, possiamo comunque modificarlo a piacimento cliccando accanto alla lente d'ingrandimento a destra dello schermo dove è scritto "Sempre".

L'**indirizzo IP di origine** è sempre scritto dopo la voce "from".

Il **nome utente** può essere inserito con la query "user" per specificare l'utente che si vuole cercare, in questo caso è sempre presente.

Il **motivo del Fallimento** invece può essere scritto (se presente) con `rex field=_raw "reason: (<failure_reason>.)"`

- Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente "djohnson" e mostrare il timestamp e l'ID utente.

Svolgimento Punto 2

The screenshot shows the Splunk interface with a search results page. The search bar contains the following query:

```
source=tutorialdata.zip host=DESKTOP-8CAJRT0 Accepted password djohnson | rex field=_raw user (?<user_id>\$+) | table _time user_id | rename _time as "Timestamp", user_id as "User ID" | sort -Timestamp user=djohnson
```

The results table displays 2,865 events, all from the same timestamp (Thu Dec 15 2024 12:42:06) and user (djohnson). The columns are labeled "Ora" (Time), "Evento" (Event), and "User ID". The event details show multiple successful password attempts from port 5143, 3914, and 2652 on the host DESKTOP-8CAJRT0.

Per il secondo punto dobbiamo trovare tutte le sessioni aperte con successo, filtrando per l'utente "djohnson" mostrando il timestamp e ID

Nella query mettiamo "Accepted Password" per indicare le sessioni aperte

L **utente** possiamo definirlo con user="djohnson" e mostrerà solo i suoi tentativi

Per il **Timestamp** abbiamo sempre usato sort - Timestamp

Possiamo comunque anche usare: **rex field=_raw "user (?<user_id>\\$+)"** che estrae l'ID utente (user_id) dalla stringa dei log

- Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP "86.212.199.60". La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.

Svolgimento Punto 3

The screenshot shows the Splunk interface with the following details:

- Search Bar:** The search bar contains the query: `source="tutorialdata.zip:*" host="DESKTOP-8CAJRT0" "Failed password" "86.212.199.60" | rex field=_raw "Failed password for (?<username>\S+) from 86\.212\.199\.60 port (?<port>\d+)" | table _time username port | sort -Timestamp`
- Results Summary:** 474 eventi (prima di 02/01/25 20:14:18,000) Nessun campionamento degli eventi.
- Event View:** The main pane displays a table of events. The columns are **Ora** (Time), **Evento** (Event). The table lists multiple entries for failed logins on port 22 from the IP 86.212.199.60, occurring on Thu Dec 15 2024 at 12:42:06. The events are as follows:

Ora	Evento
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5728]: Failed password for invalid user agushto from 86.212.199.60 port 3692 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[4843]: Failed password for invalid user tomcat from 86.212.199.60 port 1464 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5718]: Failed password for invalid user desktop from 86.212.199.60 port 3518 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[1008]: Failed password for invalid user yp from 86.212.199.60 port 2856 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2
15/12/24 12:42:06	host = DESKTOP-8CAJRT0 source = tutorialdata.zip:\mailsv\secure.log sourcetype = wwwl\secure
15/12/24 12:42:06	Thu Dec 15 2024 12:42:06 mailsvl sshd[5878]: Failed password for mail from 86.212.199.60 port 1054 ssh2

In questa Query dobbiamo trovare i tentativi di accesso falliti provenienti da un indirizzo IP specifico, mostrando sempre i timestamp, nome e in questo caso anche numero di porta

Per i **tentativi di accesso falliti** inseriamo nuovamente "Failed Password"

Per mostrare uno **specifico IP**, lo inseriamo tra le virgolette subito dopo il "Failed Password" quindi "86.212.199.60"

la voce **rex** estrae il nome utente e il numero di porta aggiungendo:
(?<username>\S+): cattura l'username

86.212.199.60: Cerca l IP specifico

port (?<port>\d+): cattura il numero di porta
e sempre per il **Timestamp** usiamo il classico **sort - Timestamp**

- Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.

Svolgimento Punto 4

Splunk Server [in esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Auto

Ricerca | Splunk 9.4.0

127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D*tutorialdata.zip%3A*%20host%3D"DESKTOP-8CAJRT0"%20"Failed%20password"%20%7C%20rex%20field%3D_raw%20"Failed%20password%20for%20.*from%20(%3F<ip_address>%5Cd%2B%5C.%5Cd%2B%5C.%5Cd%2B%5C.%5Cd%2B)"%7C%20stats%20count%20...

splunk>enterprise App ▾

Administrator ▾ 2 Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova

Ricerca Analytics Set di dati Report Allarmi Dashboard

Search & Reporting

Nuova ricerca

source="tutorialdata.zip;*" host="DESKTOP-8CAJRT0" "Failed password" | rex field=_raw "Failed password for .* from (?<ip_address>\d+\.\d+\.\d+\.\d+)"| stats count as Attempt_Count by ip_address| where Attempt_Count > 5| sort - Attempt_Count| rename ip_address as "IP Address", Attempt_Count as "Number of Attempts"

99.759 eventi (prima di 02/01/25 20:26:44,000) Nessun campionamento degli eventi ▾ Processo ▾ Modalità dettagliata ▾

Eventi (99.759) Pattern Statistiche (182) Visualizzazione

✓ Formato timeline ▾ — Zoom indietro + Zoom area selezionata X Deseleziona 1 giorno per colonna

15.102 events 11 dic 2024

✓ Formato ▾ Mostra: 20 per pagina ▾ Visualizza: Elenco ▾

< Nascondi campi ▾ Tutti i campi ▾ Ora Evento

CAMPARI SELEZIONATI a host 1 a source 4 a sourcetype 1

CAMPARI INTERESSANTI # date_hour 1 # date_mday 8 # date_minute 1 # date_month 1 # date_second 4 # date_wday 7 # date_year 1 # date_zone 1 a index 1 a ip_address 100+ # linecount 1 a punct 3 a splunk_server 1 # timeendpos 1 # timestamppos 1

+ Estrai nuovi campi

i	Ora	Evento
>	15/12/24 12:42:06,000	The Dec 15 2024 12:42:06 mailsvl sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24 12:42:06,000	Thu Dec 15 2024 12:42:06 mailsvl sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure
>	15/12/24	Thu Dec 15 2024 12:42:06 mailsvl sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = DESKTOP-8CAJRT0 source = tutorialdata.zip.:mailsvl/secure.log sourcetype = wwwvl/secure

Cerca

2027 02/01/2025

11°C Nuvoloso 2027 02/01/2025

In questo Punto dobbiamo trovare gli indirizzi IP che hanno tentato di accedere per piu di 5 volte,dovremmo quindi scrivere la query mostrando indirizzo IP e numero di tentativi

Failed password sempre per specificare i log

rex estrarre gli indirizzi ip,aggiungendoci:
(?<ip_address>\d+\.\d+\.\d+\.\d+):cattura in indirizzo IP in formato IPv4
stats count as Attempt_Count by ip_address:Raggruppa i risultati per ip_address e conta il numero di eventi per ciascun indirizzo IP.

where Attempt_Count > 5: filtra per mostrare solo gli indirizzi IP che hanno effettuato più di 5 tentativi di accesso falliti.

(OPZIONALE) sort -

Attempt_Count: Ordina i risultati in ordine decrescente di numero di tentativi.

(OPZIONALE) **rename**: che rinomina i campi per una migliore rileggibilità

- Crea una query Splunk per trovare tutti gli Internal Server Error.

Svolgimento Punto 5

Nella ricerca troviamo i seguenti risultati:

```
source="tutorialdata.zip:" host="DESKTOP-8CAJRT0" | stats count by status_code host source| rename status_code as "Status Code", count as "Occurrences", host as "Host", source as "Source" | sort - Occurrences status_code="5*"
```

Ora	Evento
15/12/24 18:24:02,000	[15/Dec/2024:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:24:02,000	[15/Dec/2024:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:24:02,000	[15/Dec/2024:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:46,000	[15/Dec/2024:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:46,000	[15/Dec/2024:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:46,000	[15/Dec/2024:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:46,000	[15/Dec/2024:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:31,000	[15/Dec/2024:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:31,000	[15/Dec/2024:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:31,000	[15/Dec/2024:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:23:31,000	[15/Dec/2024:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:22:59,000	[15/Dec/2024:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:22:59,000	[15/Dec/2024:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:22:59,000	[15/Dec/2024:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:22:59,000	[15/Dec/2024:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:22:48,000	[15/Dec/2024:18:22:48] VendorID=1239 Code=K AcctID=5822351159954748 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales
15/12/24 18:22:48,000	[15/Dec/2024:18:22:48] VendorID=1239 Code=K AcctID=5822351159954748 host = DESKTOP-8CAJRT0 source = tutorialdata.zip:vendor_sales/vendor_sales.log sourcetype = vendor_sales/vendor_sales

Nel punto 5 dobbiamo filtrare per qualunque Internal Server Error, e facciamo:

status_code="5*":

- Cerca tutti i codici di stato HTTP che iniziano con "5", inclusi:
 - **500: Internal Server Error**
 - **502: Bad Gateway**
 - **503: Service Unavailable**
 - **504: Gateway Timeout**

stats count by status_code host

source: Raggruppa i risultati per codice di stato, host, e sorgente, e conta quante volte ogni codice di errore appare.

(OPZIONALE) **rename:** rinomina i campi per leggibilità migliore

(OPZIONALE) **sort - Occurrences:** che ordina i risultati in ordine decrescente per il numero di occorrenze