In [26]:

```
# 連接 Elasticsearch
```

In [27]:

```
from datetime import datetime
from elasticsearch import Elasticsearch
import matplotlib.pyplot as plt
import pandas as pd
import requests
import time
```

In [28]:

```
es_ip = "http://127.0.0.1:9200"
```

In [29]:

```
es = Elasticsearch(es_ip)
```

In [30]:

```
# 查詢資料(讀取單一筆資料)
```

In [31]:

```
res = es.get(index="winlogbeat", id="IM3k130BMs_nTerjgcWJ")
print(res['_source'])
```

```
{'@timestamp': '2021-12-20T12:50:14.534Z', 'log': {'level': 'information'},
'host': {'name': 'DESKTOP-T3V8EOP', 'ip': ['fe80::1911:e65c:d649:9768', '19
2.168.56.1', 'fe80::24c3:baf3:3d58:f2af', '169.254.242.175', 'fe80::a832:f3
5:3de:862c', '169.254.134.44', 'fe80::d4a8:14f8:2744:a74a', '192.168.0.83',
'fe80::4d6b:1d3e:cee1:343d', '169.254.52.61'], 'mac': ['0a:00:27:00:00:10',
'24:ee:9a:ff:17:da', '26:ee:9a:ff:17:d9', '24:ee:9a:ff:17:d9', '24:ee:9a:ff:
17:dd'], 'hostname': 'DESKTOP-T3V8EOP', 'architecture': 'x86_64', 'os': {'ve
rsion': '10.0', 'family': 'windows', 'name': 'Windows 10 Pro', 'kernel': '1
0.0.22000.318 (WinBuild.160101.0800)', 'build': '22000.318', 'type': 'window
s', 'platform': 'windows'}, 'id': '1f725ed7-b14c-494d-9fc1-4bc3eeb0b29b'},
'winlog': {'record_id': 492, 'api': 'wineventlog', 'provider_guid': '{577038
5f-c22a-43e0-bf4c-06f5698ffbd9}', 'process': {'pid': 53848, 'thread': {'id':
26096}}, 'version': 5, 'channel': 'Microsoft-Windows-Sysmon/Operational', 'e
vent_id': '1', 'provider_name': 'Microsoft-Windows-Sysmon', 'computer_name':
'DESKTOP-T3V8EOP', 'user': {'identifier': 'S-1-5-18', 'domain': 'NT AUTHORIT
Y', 'name': 'SYSTEM', 'type': 'User'}, 'event_data': {'ParentProcessId': '53
12', 'OriginalFileName': 'RAPS.exe', 'Image': 'C:\\Program Files\\Rivet Netw
orks\\SmartByte\\RAPS.exe', 'Company': 'Rivet Networks LLC', 'LogonId': '0x6
ba12a0f', 'Product': 'RivetAPS', 'IntegrityLevel': 'Medium', 'UtcTime': '202
1-12-20 12:50:14.532', 'LogonGuid': '{1f725ed7-4242-61bc-0f2a-a16b0000000
0}', 'ProcessId': '31156', 'RuleName': '-', 'CommandLine': 'RAPS.exe -u', 'U
ser': 'DESKTOP-T3V8EOP\\a3789', 'FileVersion': '3.1.995.0', 'Hashes': 'MD5=F
70A23758DA94B90A01CC791ACC7F385,SHA256=EEBCC0C6FD9A7BF70BA3028DAEA19C450FCC6
98169C2E5B03F6BEF9D4BBA1A6F,IMPHASH=935B686812E8D4246E2278AF50AA30FB', 'Pare
ntImage': 'C:\\Program Files\\Rivet Networks\\SmartByte\\RAPS.exe', 'ParentC
ommandLine': '"RAPS.exe"', 'ProcessGuid': '{1f725ed7-7c06-61c0-3c1b-90810000
0000}', 'CurrentDirectory': 'C:\\Program Files\\Rivet Networks\\SmartByte
\\', 'Description': 'RivetAPS', 'ParentProcessGuid': '{1f725ed7-296e-61ab-8f
00-000000000d00}', 'TerminalSessionId': '2'}}, 'event': {'kind': 'event', 'p
rovider': 'Microsoft-Windows-Sysmon', 'created': '2021-12-20T12:50:15.928Z',
'code': '1', 'timezone': '+08:00'}, 'fields': {'endpoint_project': 'df909038
f4bcafd88f8d49c7f6ad5ccd', 'endpoint_email': 'a3789468739@gmail.com', 'endpo
int_org3': 'T7-1639616151642'}, 'ecs': {'version': '1.9.0'}, 'agent': {'vers
ion': '7.13.2', 'hostname': 'DESKTOP-T3V8EOP', 'ephemeral_id': '41f4d791-f3b
8-47ed-b193-c7151f023406', 'id': '621af60c-6ab1-4b77-803e-d523c7d8ec04', 'na
me': 'DESKTOP-T3V8EOP', 'type': 'winlogbeat'}}
```

In [32]:

```
# 查詢資料(取得前150筆資料)
```

In [33]:

```
query_str = '{"query":{"range":{"@timestamp":{"gte":"2021-12-20", "lte":"2021-12-20"}}}}'
res = es.search(index="winlogbeat", body=query_str, from_=0, size=150)
```

```
C:\Users\enya\AppData\Local\Temp/ipykernel_16072/3274430468.py:2: Deprecatio
nWarning: The 'body' parameter is deprecated for the 'search' API and will b
e removed in a future version. Instead use API parameters directly. See http
s://github.com/elastic/elasticsearch-py/issues/1698 (https://github.com/elas
tic/elasticsearch-py/issues/1698) for more information
  res = es.search(index="winlogbeat", body=query_str, from_=0, size=150)
```

In [34]:

```
# 取得筆數
```

In [35]:

```
total_hits = res["hits"]["total"]
print("total : " + str(total_hits))
```

```
total : 8028
```

In [36]:

```
# 顯示 150 筆資料
```

In [37]:

```
print(res["hits"]["hits"])
```

```
[{'_index': 'winlogbeat', '_type': 'doc', '_id': 'IM3k130BMs_nTerjgcWJ',
'_score': 1.0, '_source': {'@timestamp': '2021-12-20T12:50:14.534Z', 'lo
g': {'level': 'information'}, 'host': {'name': 'DESKTOP-T3V8EOP', 'ip':
['fe80::1911:e65c:d649:9768', '192.168.56.1', 'fe80::24c3:baf3:3d58:f2af',
'169.254.242.175', 'fe80::a832:f35:3de:862c', '169.254.134.44', 'fe80::d4a
8:14f8:2744:a74a', '192.168.0.83', 'fe80::4d6b:1d3e:cee1:343d', '169.254.5
2.61'], 'mac': ['0a:00:27:00:00:10', '24:ee:9a:ff:17:da', '26:ee:9a:ff:17:
d9', '24:ee:9a:ff:17:d9', '24:ee:9a:ff:17:dd'], 'hostname': 'DESKTOP-T3V8E
OP', 'architecture': 'x86_64', 'os': {'version': '10.0', 'family': 'window
s', 'name': 'Windows 10 Pro', 'kernel': '10.0.22000.318 (WinBuild.160101.0
800)', 'build': '22000.318', 'type': 'windows', 'platform': 'windows'}, 'i
d': '1f725ed7-b14c-494d-9fc1-4bc3eeb0b29b'}, 'winlog': {'record_id': 492,
'api': 'wineventlog', 'provider_guid': '{5770385f-c22a-43e0-bf4c-06f5698ff
bd9}', 'process': {'pid': 53848, 'thread': {'id': 26096}}, 'version': 5,
'channel': 'Microsoft-Windows-Sysmon/Operational', 'event_id': '1', 'provi
der_name': 'Microsoft-Windows-Sysmon', 'computer_name': 'DESKTOP-T3V8EOP',
'user': {'identifier': 'S-1-5-18', 'domain': 'NT AUTHORITY', 'name': 'SYST
EM', 'type': 'User'}, 'event_data': {'ParentProcessId': '5312', 'OriginalF
ileName': 'RAPS.exe', 'Image': 'C:\\Program Files\\Rivet Networks\\SmartBy
```

In [38]:

```
# Show Event Count by Datetime
```

In [39]:

```
query_str = {"size": 0,"aggs": {"result": {"date_histogram": {"field": "@timestamp","interv
res = es.search(index="winlogbeat", body=query_str)
result = res["aggregations"]["result"]["buckets"]
#print(result)
```

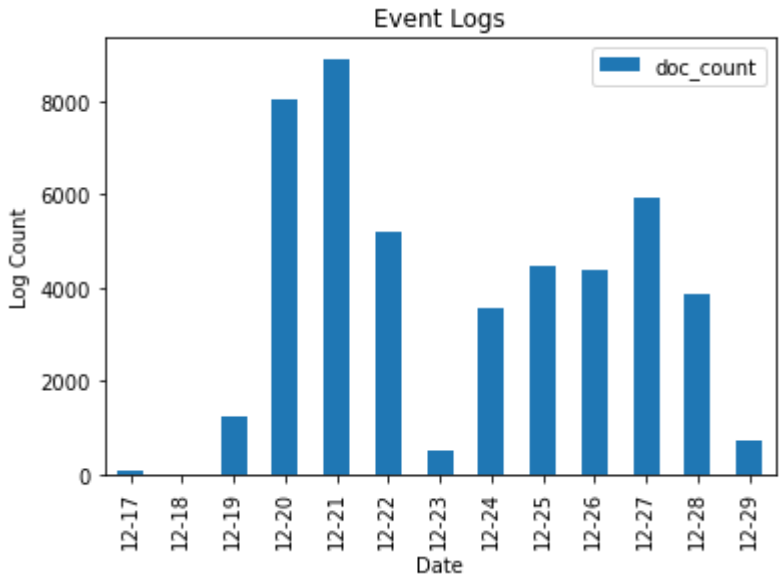
```
C:\Users\enya\AppData\Local\Temp/ipykernel_16072/3439329284.py:2: Deprecatio
nWarning: The 'body' parameter is deprecated for the 'search' API and will b
e removed in a future version. Instead use API parameters directly. See http
s://github.com/elastic/elasticsearch-py/issues/1698 (https://github.com/elas
tic/elasticsearch-py/issues/1698) for more information
  res = es.search(index="winlogbeat", body=query_str)
```

In [40]:

```
event_pd = pd.DataFrame(result, columns=["key_as_string", "doc_count"])
#print(event_pd)
event_pd.plot(x="key_as_string", y="doc_count", kind="bar");
plt.xlabel('Date')
plt.ylabel('Log Count')
plt.title('Event Logs')
```

Out[40]:

```
Text(0.5, 1.0, 'Event Logs')
```



In [41]:

```
# Show Event Count by EventID
```

In [42]:

```
query_str = {"size": 0,"aggregations": {"result": {"terms": {"field": "winlog.event_id.keyw
res = es.search(index="winlogbeat", body=query_str)
result = res["aggregations"]["result"]["buckets"]
#print(result)
```

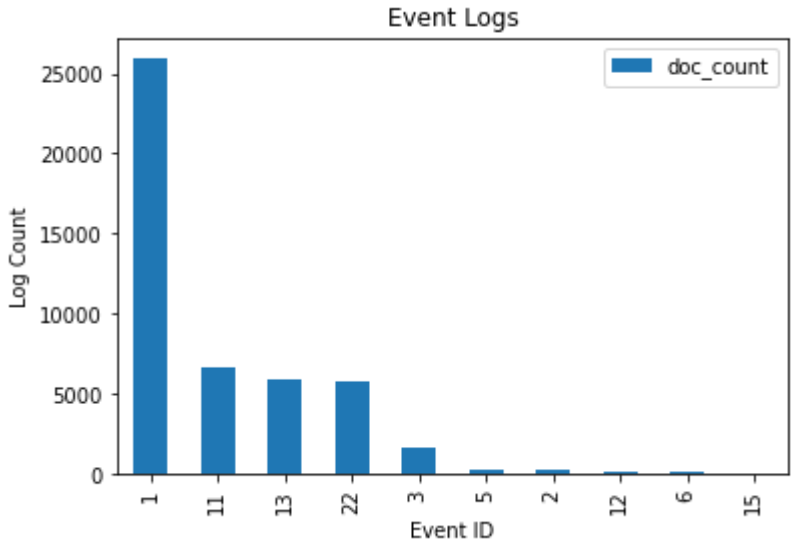
```
C:\Users\enya\AppData\Local\Temp/ipykernel_16072/2552605711.py:2: Deprecatio
nWarning: The 'body' parameter is deprecated for the 'search' API and will b
e removed in a future version. Instead use API parameters directly. See http
s://github.com/elastic/elasticsearch-py/issues/1698 (https://github.com/elas
tic/elasticsearch-py/issues/1698) for more information
  res = es.search(index="winlogbeat", body=query_str)
```

In [43]:

```
event_pd = pd.DataFrame(result, columns=["key", "doc_count"])
#print(event_pd)
event_pd.plot(x="key", y="doc_count", kind="bar");
plt.xlabel('Event ID')
plt.ylabel('Log Count')
plt.title('Event Logs')
```

Out[43]:

```
Text(0.5, 1.0, 'Event Logs')
```



In [44]:

```
# Show Event Count by DestinationIp
```

In [45]:

```
query_str = {"size": 0,"aggregations": {"result": { "terms": {"field": "winlog.event_data.D
res = es.search(index="winlogbeat", body=query_str)
result = res["aggregations"]["result"]["buckets"]
#print(result)
```

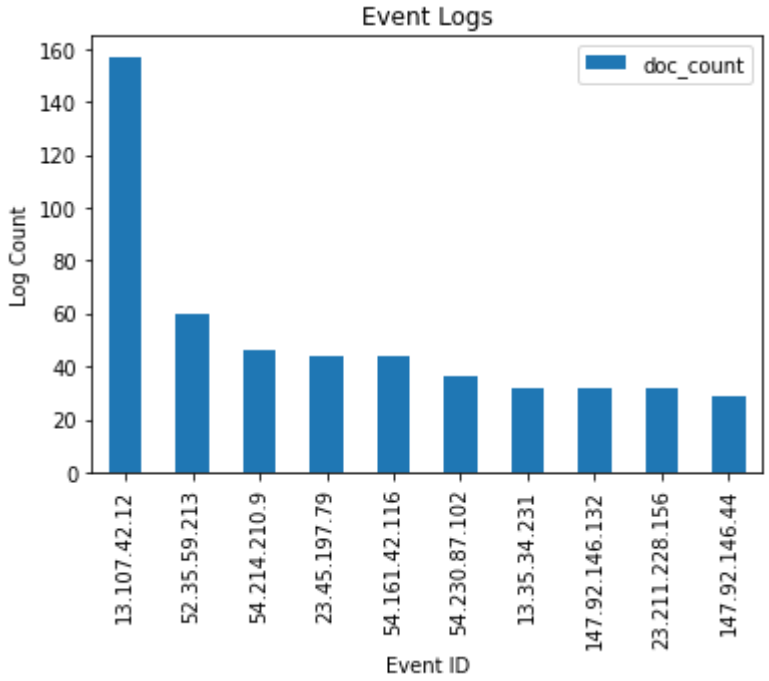
```
C:\Users\enya\AppData\Local\Temp/ipykernel_16072/3936957868.py:2: Deprecatio
nWarning: The 'body' parameter is deprecated for the 'search' API and will b
e removed in a future version. Instead use API parameters directly. See http
s://github.com/elastic/elasticsearch-py/issues/1698 (https://github.com/elas
tic/elasticsearch-py/issues/1698) for more information
  res = es.search(index="winlogbeat", body=query_str)
```

In [46]:

```
event_pd = pd.DataFrame(result, columns=["key", "doc_count"])
#print(event_pd)
event_pd.plot(x="key", y="doc_count", kind="bar");
plt.xlabel('Event ID')
plt.ylabel('Log Count')
plt.title('Event Logs')
```

Out[46]:

```
Text(0.5, 1.0, 'Event Logs')
```



In [47]:

```
# IP查詢
```

In [48]:

```
request_headers = {
    'user-agent':'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) ' \
    'AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.95 Safari/537.36'
}
for ip in event_pd["key"]:
    print(ip)
    req = requests.get("https://ipapi.co/"+ip+"/json", headers=request_headers)
    print(req.json())
    time.sleep(5)
```

```
13.107.42.12
{'ip': '13.107.42.12', 'version': 'IPv4', 'city': 'Toronto', 'region': 'Onta
rio', 'region_code': 'ON', 'country': 'CA', 'country_name': 'Canada', 'count
ry_code': 'CA', 'country_code_iso3': 'CAN', 'country_capital': 'Ottawa', 'co
untry_tld': '.ca', 'continent_code': 'NA', 'in_eu': False, 'postal': 'M3B',
'latitude': 43.7466, 'longitude': -79.3517, 'timezone': 'America/Toronto',
'utc_offset': '-0500', 'country_calling_code': '+1', 'currency': 'CAD', 'cur
rency_name': 'Dollar', 'languages': 'en-CA,fr-CA,iu', 'country_area': 998467
0.0, 'country_population': 37058856, 'asn': 'AS8068', 'org': 'MICROSOFT-CORP
-MSN-AS-BLOCK'}
52.35.59.213
{'ip': '52.35.59.213', 'version': 'IPv4', 'city': 'Boardman', 'region': 'Ore
gon', 'region_code': 'OR', 'country': 'US', 'country_name': 'United States',
'country_code': 'US', 'country_code_iso3': 'USA', 'country_capital': 'Washin
gton', 'country_tld': '.us', 'continent_code': 'NA', 'in_eu': False, 'posta
l': '97818', 'latitude': 45.8234, 'longitude': -119.7257, 'timezone': 'Ameri
ca/Los_Angeles', 'utc_offset': '-0800', 'country_calling_code': '+1', 'curre
ncy': 'USD', 'currency_name': 'Dollar', 'languages': 'en-US,es-US,haw,fr',
'country_area': 9629091.0, 'country_population': 327167434, 'asn': 'AS1650
9', 'org': 'AMAZON-02'}
54.214.210.9
{'ip': '54.214.210.9', 'version': 'IPv4', 'city': 'Boardman', 'region': 'Ore
gon', 'region_code': 'OR', 'country': 'US', 'country_name': 'United States',
'country_code': 'US', 'country_code_iso3': 'USA', 'country_capital': 'Washin
gton', 'country_tld': '.us', 'continent_code': 'NA', 'in_eu': False, 'posta
l': '97818', 'latitude': 45.8234, 'longitude': -119.7257, 'timezone': 'Ameri
ca/Los_Angeles', 'utc_offset': '-0800', 'country_calling_code': '+1', 'curre
ncy': 'USD', 'currency_name': 'Dollar', 'languages': 'en-US,es-US,haw,fr',
'country_area': 9629091.0, 'country_population': 327167434, 'asn': 'AS1650
9', 'org': 'AMAZON-02'}
23.45.197.79
{'ip': '23.45.197.79', 'version': 'IPv4', 'city': 'Kaohsiung City', 'regio
n': 'Kaohsiung', 'region_code': 'KHH', 'country': 'TW', 'country_name': 'Tai
wan', 'country_code': 'TW', 'country_code_iso3': 'TWN', 'country_capital':
'Taipei', 'country_tld': '.tw', 'continent_code': 'AS', 'in_eu': False, 'pos
tal': None, 'latitude': 22.6269, 'longitude': 120.3656, 'timezone': 'Asia/Ta
ipei', 'utc_offset': '+0800', 'country_calling_code': '+886', 'currency': 'T
WD', 'currency_name': 'Dollar', 'languages': 'zh-TW,zh,nan,hak', 'country_ar
ea': 35980.0, 'country_population': 22894384, 'asn': 'AS16625', 'org': 'AKAM
AI-AS'}
54.161.42.116
{'ip': '54.161.42.116', 'version': 'IPv4', 'city': 'Ashburn', 'region': 'Vir
ginia', 'region_code': 'VA', 'country': 'US', 'country_name': 'United State
s', 'country_code': 'US', 'country_code_iso3': 'USA', 'country_capital': 'Wa
shington', 'country_tld': '.us', 'continent_code': 'NA', 'in_eu': False, 'po
stal': '20147', 'latitude': 39.017388, 'longitude': -77.468037, 'timezone':
'America/New_York', 'utc_offset': '-0500', 'country_calling_code': '+1', 'cu
rrency': 'USD', 'currency_name': 'Dollar', 'languages': 'en-US,es-US,haw,f
r', 'country_area': 9629091.0, 'country_population': 327167434, 'asn': 'AS14
```

618', 'org': 'AMAZON-AES'}
54.230.87.102
{'ip': '54.230.87.102', 'version': 'IPv4', 'city': 'Hong Kong', 'region': 'C
entral and Western', 'region_code': None, 'country': 'HK', 'country_name':
'Hong Kong', 'country_code': 'HK', 'country_code_iso3': 'HKG', 'country_capi
tal': 'Hong Kong', 'country_tld': '.hk', 'continent_code': 'AS', 'in_eu': Fa
lse, 'postal': None, 'latitude': None, 'longitude': None, 'timezone': None,
'utc_offset': None, 'country_calling_code': '+852', 'currency': 'HKD', 'curr
ency_name': 'Dollar', 'languages': 'zh-HK,yue,zh,en', 'country_area': 1092.
0, 'country_population': 7451000, 'asn': 'AS16509', 'org': 'AMAZON-02'}
13.35.34.231
{'ip': '13.35.34.231', 'version': 'IPv4', 'city': 'Taipei', 'region': 'Taiwa
n', 'region_code': None, 'country': 'TW', 'country_name': 'Taiwan', 'country
_code': 'TW', 'country_code_iso3': 'TWN', 'country_capital': 'Taipei', 'coun
try_tld': '.tw', 'continent_code': 'AS', 'in_eu': False, 'postal': None, 'la
titude': None, 'longitude': None, 'timezone': None, 'utc_offset': None, 'cou
ntry_calling_code': '+886', 'currency': 'TWD', 'currency_name': 'Dollar', 'l
anguages': 'zh-TW,zh,nan,hak', 'country_area': 35980.0, 'country_populatio
n': 22894384, 'asn': 'AS16509', 'org': 'AMAZON-02'}
147.92.146.132
{'ip': '147.92.146.132', 'version': 'IPv4', 'city': 'Chiyoda', 'region': 'To
kyo', 'region_code': None, 'country': 'JP', 'country_name': 'Japan', 'countr
y_code': 'JP', 'country_code_iso3': 'JPN', 'country_capital': 'Tokyo', 'coun
try_tld': '.jp', 'continent_code': 'AS', 'in_eu': False, 'postal': None, 'la
titude': 35.694003, 'longitude': 139.753595, 'timezone': None, 'utc_offset':
None, 'country_calling_code': '+81', 'currency': 'JPY', 'currency_name': 'Ye
n', 'languages': 'ja', 'country_area': 377835.0, 'country_population': 12652
9100, 'asn': 'AS38631', 'org': 'LINE Corporation'}
23.211.228.156
{'ip': '23.211.228.156', 'version': 'IPv4', 'city': 'Kaohsiung City', 'regio
n': 'Kaohsiung', 'region_code': 'KHH', 'country': 'TW', 'country_name': 'Tai
wan', 'country_code': 'TW', 'country_code_iso3': 'TWN', 'country_capital':
'Taipei', 'country_tld': '.tw', 'continent_code': 'AS', 'in_eu': False, 'pos
tal': None, 'latitude': 22.6269, 'longitude': 120.3656, 'timezone': 'Asia/Ta
ipei', 'utc_offset': '+0800', 'country_calling_code': '+886', 'currency': 'T
WD', 'currency_name': 'Dollar', 'languages': 'zh-TW,zh,nan,hak', 'country_ar
ea': 35980.0, 'country_population': 22894384, 'asn': 'AS16625', 'org': 'AKAM
AI-AS'}
147.92.146.44
{'ip': '147.92.146.44', 'version': 'IPv4', 'city': 'Chiyoda', 'region': 'Tok
yo', 'region_code': None, 'country': 'JP', 'country_name': 'Japan', 'country
_code': 'JP', 'country_code_iso3': 'JPN', 'country_capital': 'Tokyo', 'count
ry_tld': '.jp', 'continent_code': 'AS', 'in_eu': False, 'postal': None, 'lat
itude': 35.694003, 'longitude': 139.753595, 'timezone': None, 'utc_offset':
None, 'country_calling_code': '+81', 'currency': 'JPY', 'currency_name': 'Ye
n', 'languages': 'ja', 'country_area': 377835.0, 'country_population': 12652
9100, 'asn': 'AS38631', 'org': 'LINE Corporation'}

In [ ]: