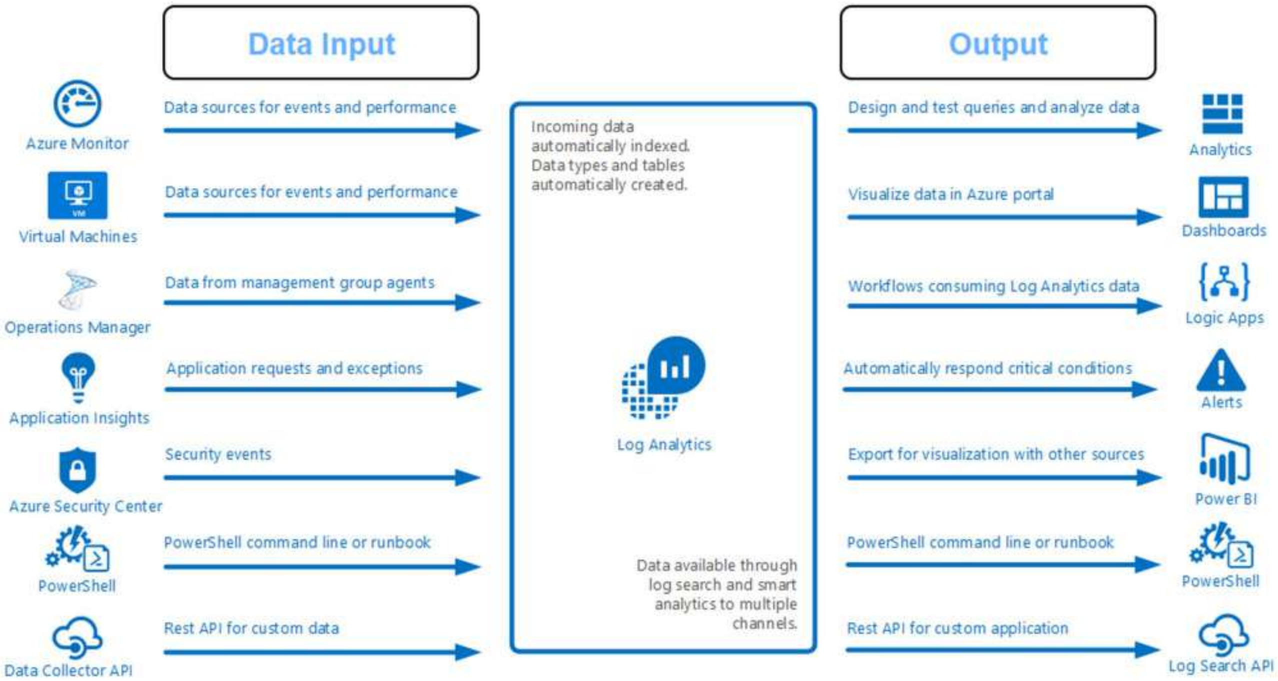
使用 Azure 監看 IT 系統狀態

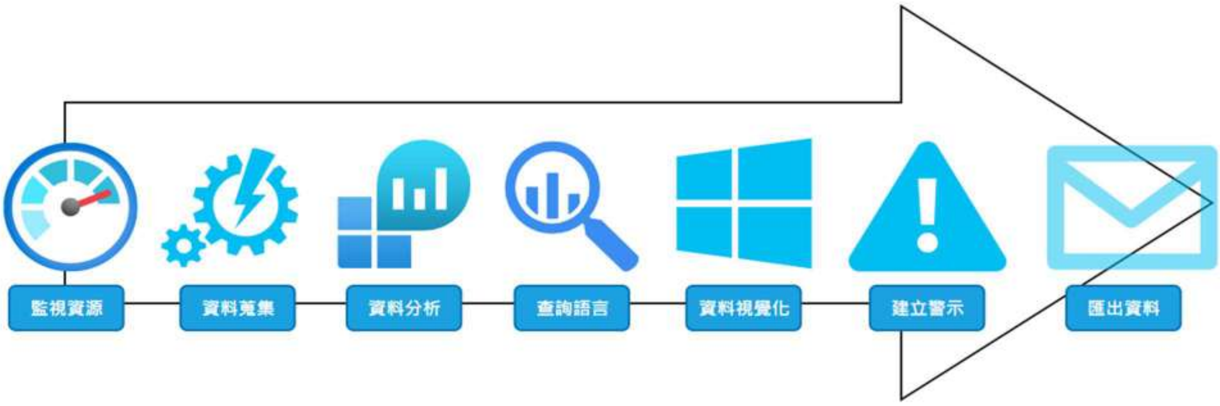
Wayne Lin

公司 IT 系統運作最害怕遇到系統停機或者出狀況，系統一旦出狀況就非常容易影響到公司正常營運，所以監控整個 IT 系統的健康狀態對公司的系統管理人員來說是非常重要的一件事情，透過 Azure Log Analytics 可以很容易地將地端及雲端所有系統的 LOG 及資源使用狀況蒐集起來，並做即時分析及告警，遇到問題的時候也可以迅速透過Ａzure 平台查找錯誤訊息。此外並可整合 Power BI 功能，產出各式系統資源及狀態之統計分析圖表。

- 以下是 Log Analytics 的方塊流程，可以看出 Azure Log Analytics 服務提供非常多樣的 Input 來源及 Output 方式


Data Input
Output
Azure Monitor
Data sources for events and performance
Virtual Machines
Data sources for events and performance
Operations Manager
Data from management group agents
Application Insights
Application requests and exceptions
Azure Security Center
Security events
PowerShell
PowerShell command line or runbook
Data Collector API
Rest API for custom data
Incoming data automatically indexed. Data types and tables automatically created.
Log Analytics
Data available through log search and smart analytics to multiple channels.
Design and test queries and analyze data
Analytics
Visualize data in Azure portal
Dashboards
Workflows consuming Log Analytics data
Logic Apps
Automatically respond critical conditions
Alerts
Export for visualization with other sources
Power BI
PowerShell command line or runbook
PowerShell
Rest API for custom application
Log Search API

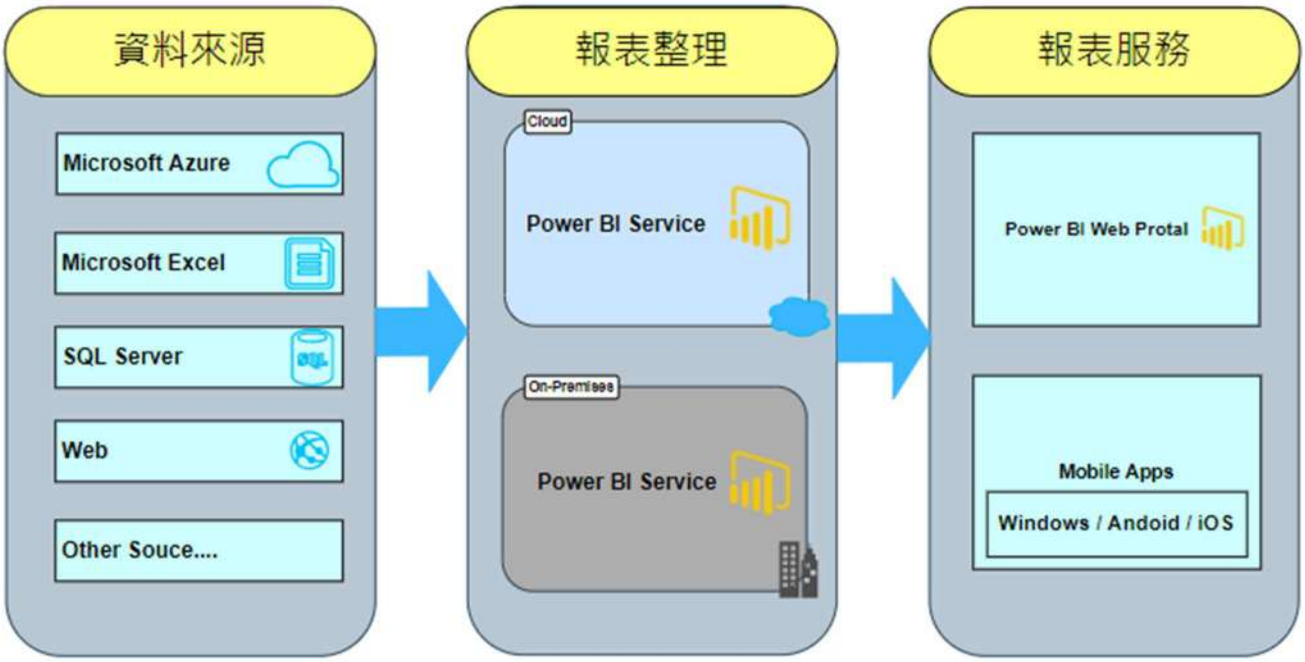
- Log 分析完整工作流程



- Log Analytics 支援主機平台

- Log Analytics 警示通報方式

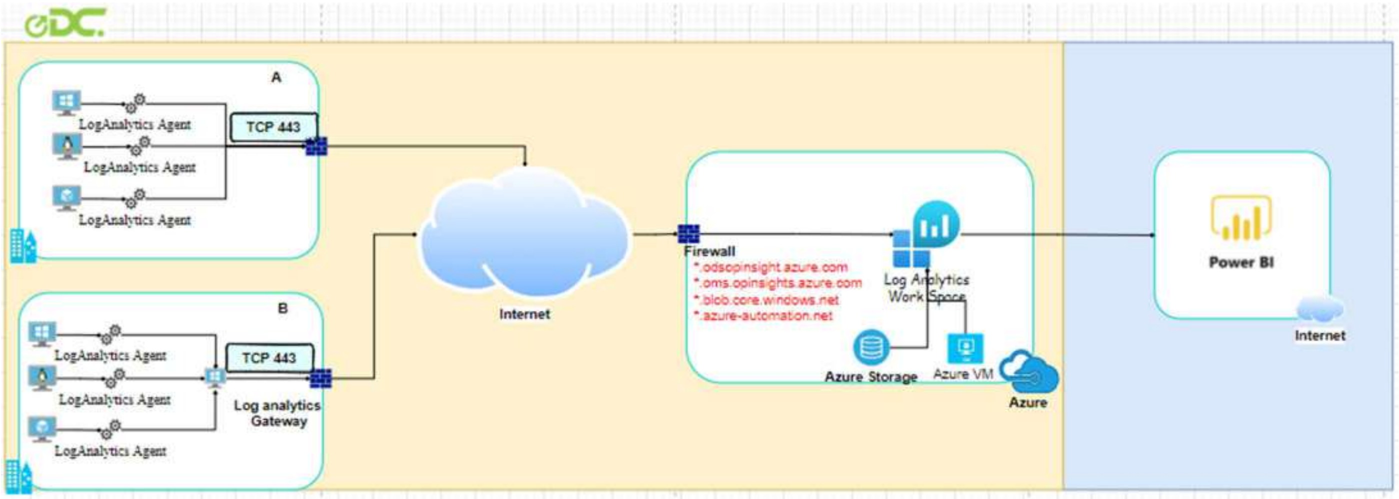
- Power BI 功能概觀



如上圖所示，Power BI 可以從多個資料來源取得資料，再將取得的資料加以整理，透過視覺化圖像的方式呈現，最後可以透過 Web、Mobile App 做查看。

實戰規劃架構說明

下圖為規劃的架構圖示，提供兩種 Log 資料收集方式，分為方法 A 及方法 B。



方法 A

- 所有虛擬機安裝 Agent， 並透過 Internet 將資訊上傳至 Log Analytics 。

方法 B

- 所有虛擬機安裝 Agent 並且將資訊傳到已安裝 Gateway 的系統，透過已安裝 Gateway 的系統連線至 Internet 將資訊上傳至 Log Analytics。

方法 A 與 B 兩者的差別為

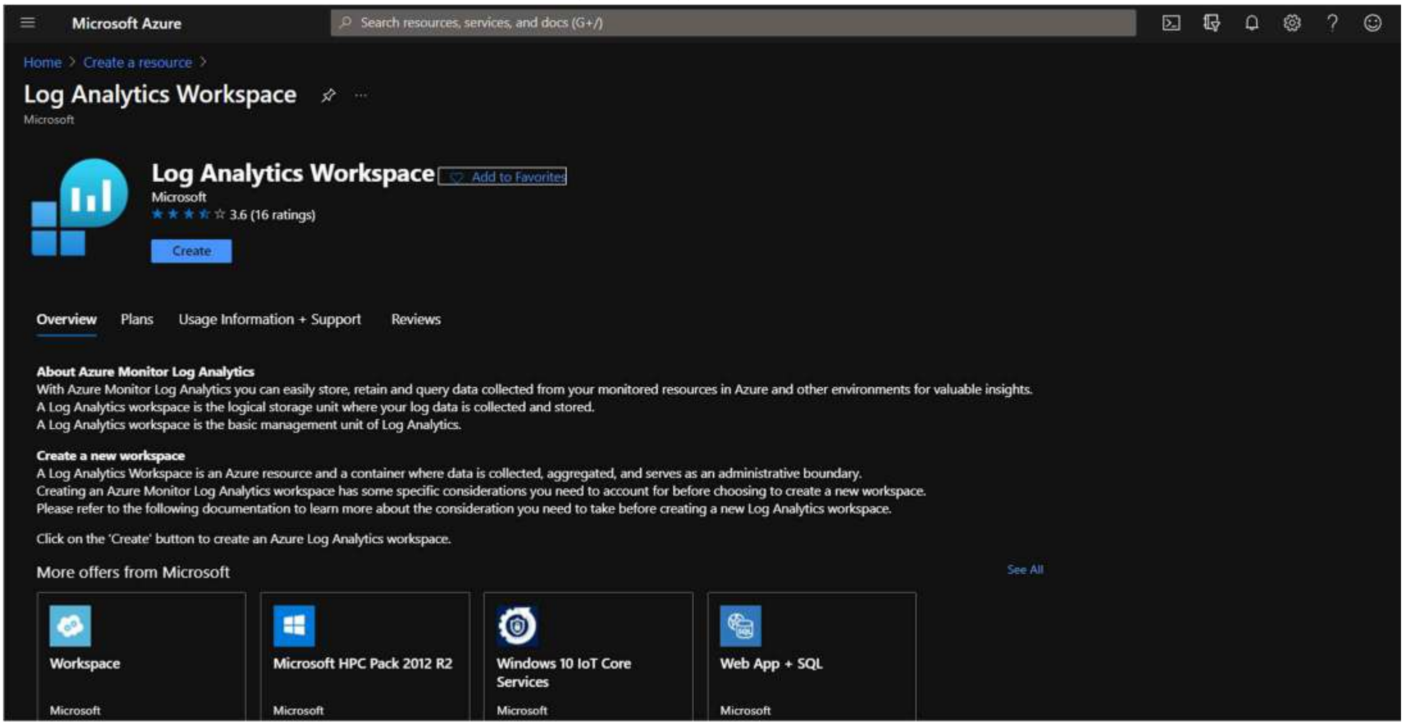
- A 需開放全部的機器對 Azure 服務連線。
- B 則只需開放安裝 Gateway 的系統對 Azure 服務連線就可以。

接下來就依據規劃的架構，一步一步來進行實戰建置說明。

Log Analytics 的建置過程

1. 建立 Log Analytics 資源

登入 Azure Portal 並且 Create Log Analytics 資源。



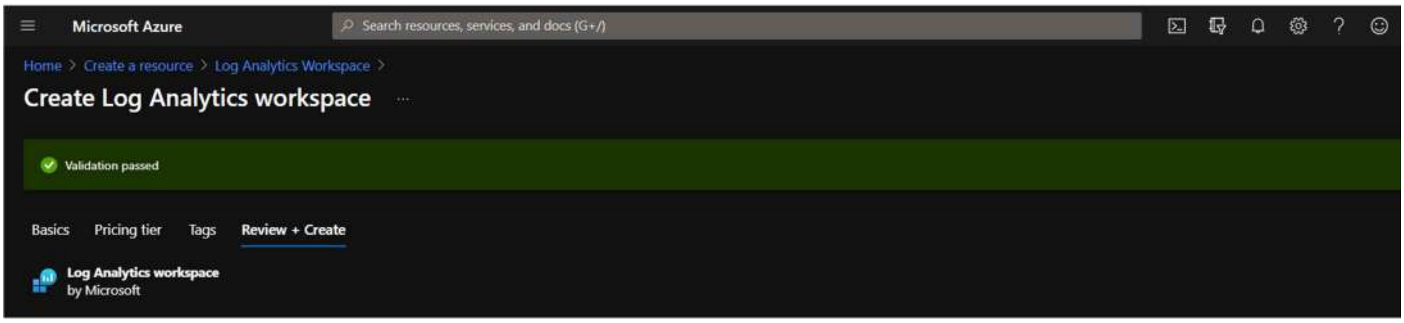
About Azure Monitor Log Analytics
With Azure Monitor Log Analytics you can easily store, retain and query data collected from your monitored resources in Azure and other environments for valuable insights.
A Log Analytics workspace is the logical storage unit where your log data is collected and stored.
A Log Analytics workspace is the basic management unit of Log Analytics.

Create a new workspace
A Log Analytics Workspace is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary.
Creating an Azure Monitor Log Analytics workspace has some specific considerations you need to account for before choosing to create a new workspace.
Please refer to the following documentation to learn more about the consideration you need to take before creating a new workspace.

Click on the 'Create' button to create an Azure Log Analytics workspace.

More offers from Microsoft
See All
Workspace
Microsoft
Microsoft HPC Pack 2012 R2
Microsoft
Windows 10 IoT Core Services
Microsoft
Web App + SQL
Microsoft

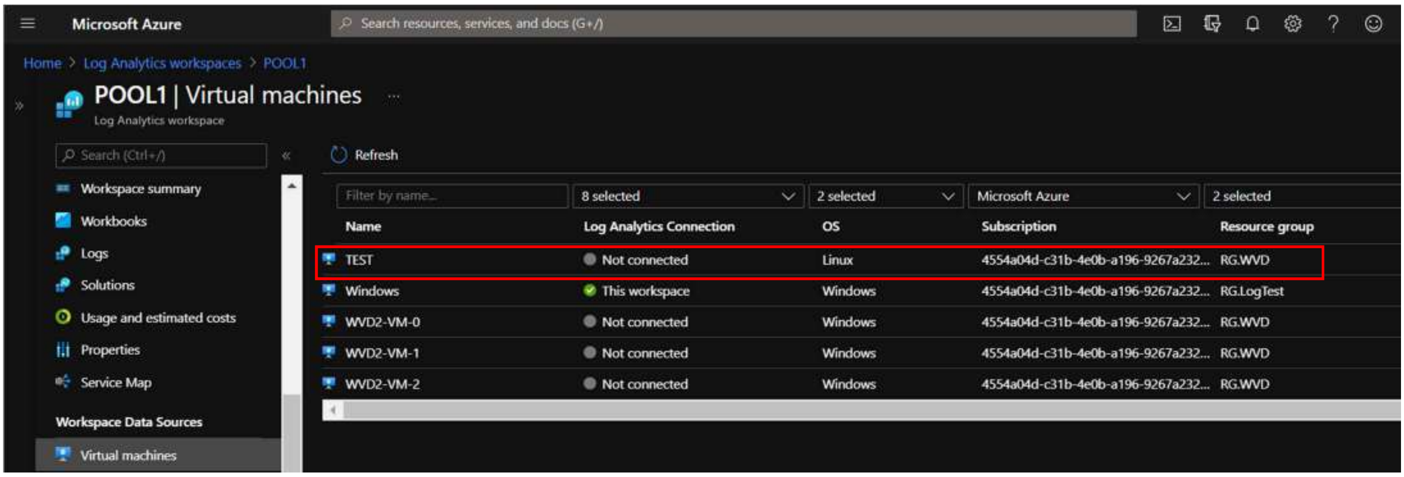
配置完成呈現 Validation passed 則表示驗證功過可以創建。


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Log Analytics Workspace >
Create Log Analytics workspace
Validation passed
Basics
Pricing tier
Tags
Review + Create
Log Analytics workspace
by Microsoft

2. 連線被監控主機

- 方法 A

開啟 Log Analytics 資源，進到 Virtual machines，選擇要連線的機器進行連線。

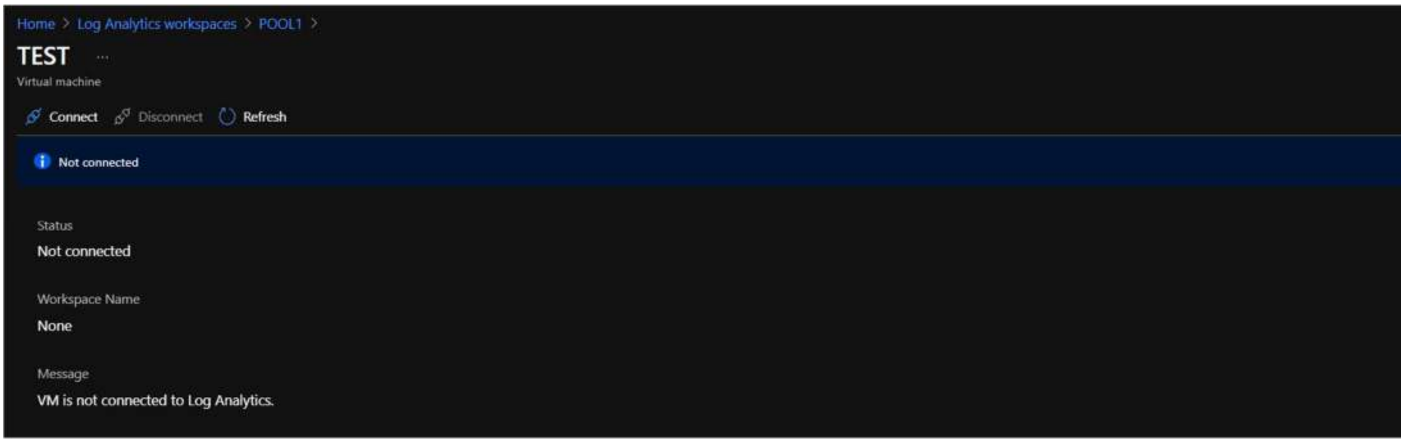


Home > Log Analytics workspaces > POOL1

POOL1 | Virtual machines

Log Analytics workspace

Name	Log Analytics Connection	OS	Subscription	Resource group
TEST	Not connected	Linux	4554a04d-c31b-4e0b-a196-9267a232...	RG.WVD
Windows	This workspace	Windows	4554a04d-c31b-4e0b-a196-9267a232...	RG.LogTest
WVD2-VM-0	Not connected	Windows	4554a04d-c31b-4e0b-a196-9267a232...	RG.WVD
WVD2-VM-1	Not connected	Windows	4554a04d-c31b-4e0b-a196-9267a232...	RG.WVD
WVD2-VM-2	Not connected	Windows	4554a04d-c31b-4e0b-a196-9267a232...	RG.WVD



Home > Log Analytics workspaces > POOL1 >

TEST

Virtual machine

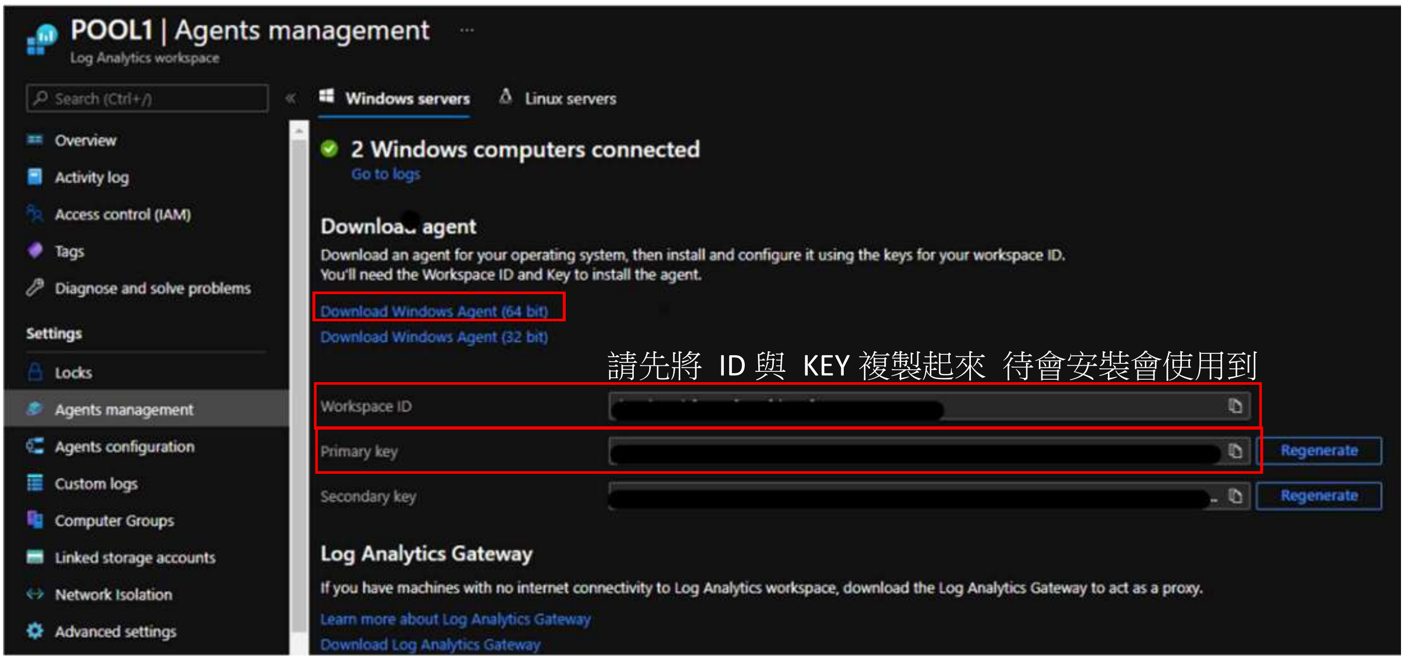
Not connected

Status
Not connected

Workspace Name
None

Message
VM is not connected to Log Analytics.

如果需要監控的系統不在Azure上，則需要在系統上安裝Agent 以下以Windows為例。首先在 Agent Management 的地方找到並下載 Download Windows Agent (64 bit)



POOL1 | Agents management

Log Analytics workspace

2 Windows computers connected

Go to logs

Downloa agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

Download Windows Agent (64 bit)

Download Windows Agent (32 bit)

請先將 ID 與 KEY 複製起來 待會安裝會使用到

Workspace ID [redacted]

Primary key [redacted] Regenerate

Secondary key [redacted] Regenerate

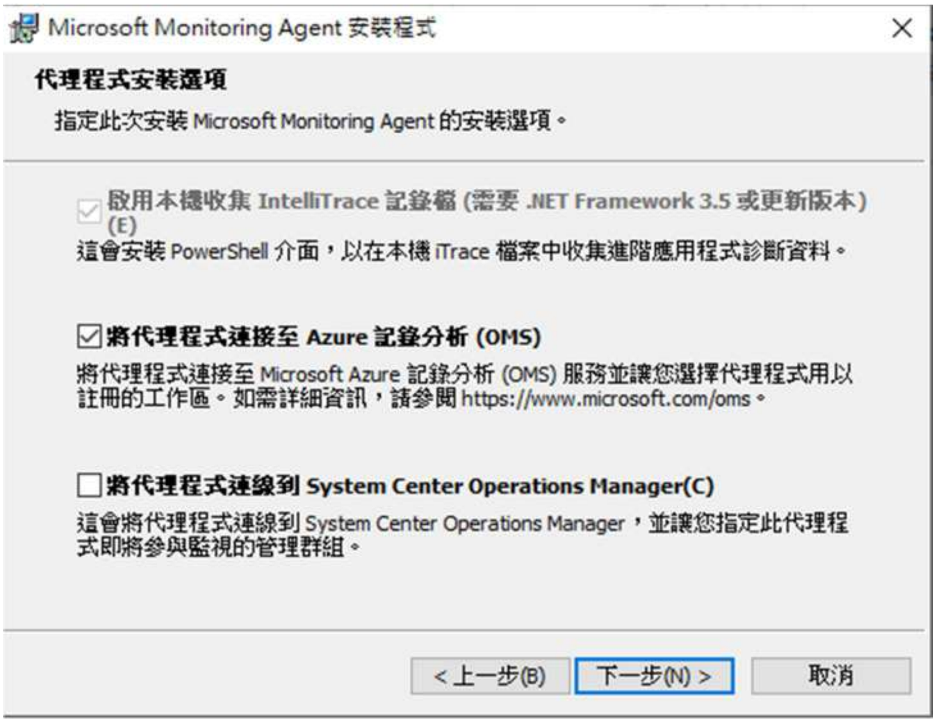
Log Analytics Gateway

If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy.

Learn more about Log Analytics Gateway

Download Log Analytics Gateway

檔案下載完成後,在需要監控的 Windows 系統上執行安裝 Agent 安裝檔，注意安裝時需要將 OMS 打勾如下圖。


Microsoft Monitoring Agent 安裝程式

代理程式安裝選項

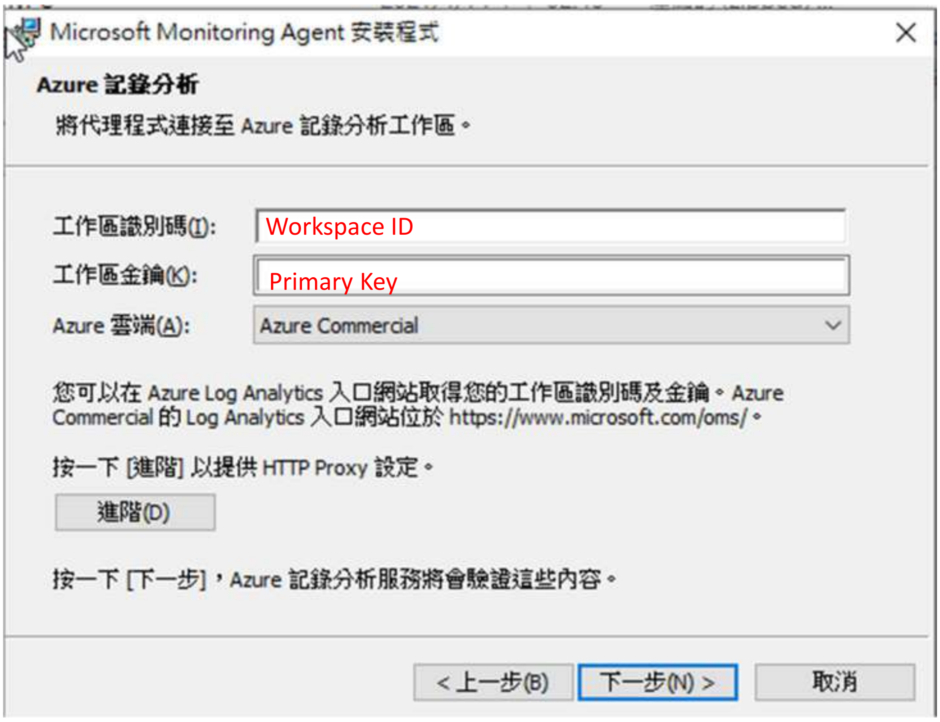
指定此次安裝 Microsoft Monitoring Agent 的安裝選項。

☑ 啟用本機收集 IntelliTrace 記錄檔 (需要 .NET Framework 3.5 或更新版本)(E)
這會安裝 PowerShell 介面，以在本機 iTrace 檔案中收集進階應用程式診斷資料。

☑ **將代理程式連接至 Azure 記錄分析 (OMS)**
將代理程式連接至 Microsoft Azure 記錄分析 (OMS) 服務並讓您選擇代理程式用以註冊的工作區。如需詳細資訊，請參閱 https://www.microsoft.com/oms。

□ **將代理程式連線到 System Center Operations Manager(C)**
這會將代理程式連線到 System Center Operations Manager，並讓您指定此代理程式即將參與監視的管理群組。

再來需要將剛剛複製的 Workspace ID 與 Primary Key 貼上後直接安裝即可。


Microsoft Monitoring Agent 安裝程式

Azure 記錄分析

將代理程式連接至 Azure 記錄分析工作區。

工作區識別碼(I): Workspace ID

工作區金鑰(K): Primary Key

Azure 雲端(A): Azure Commercial

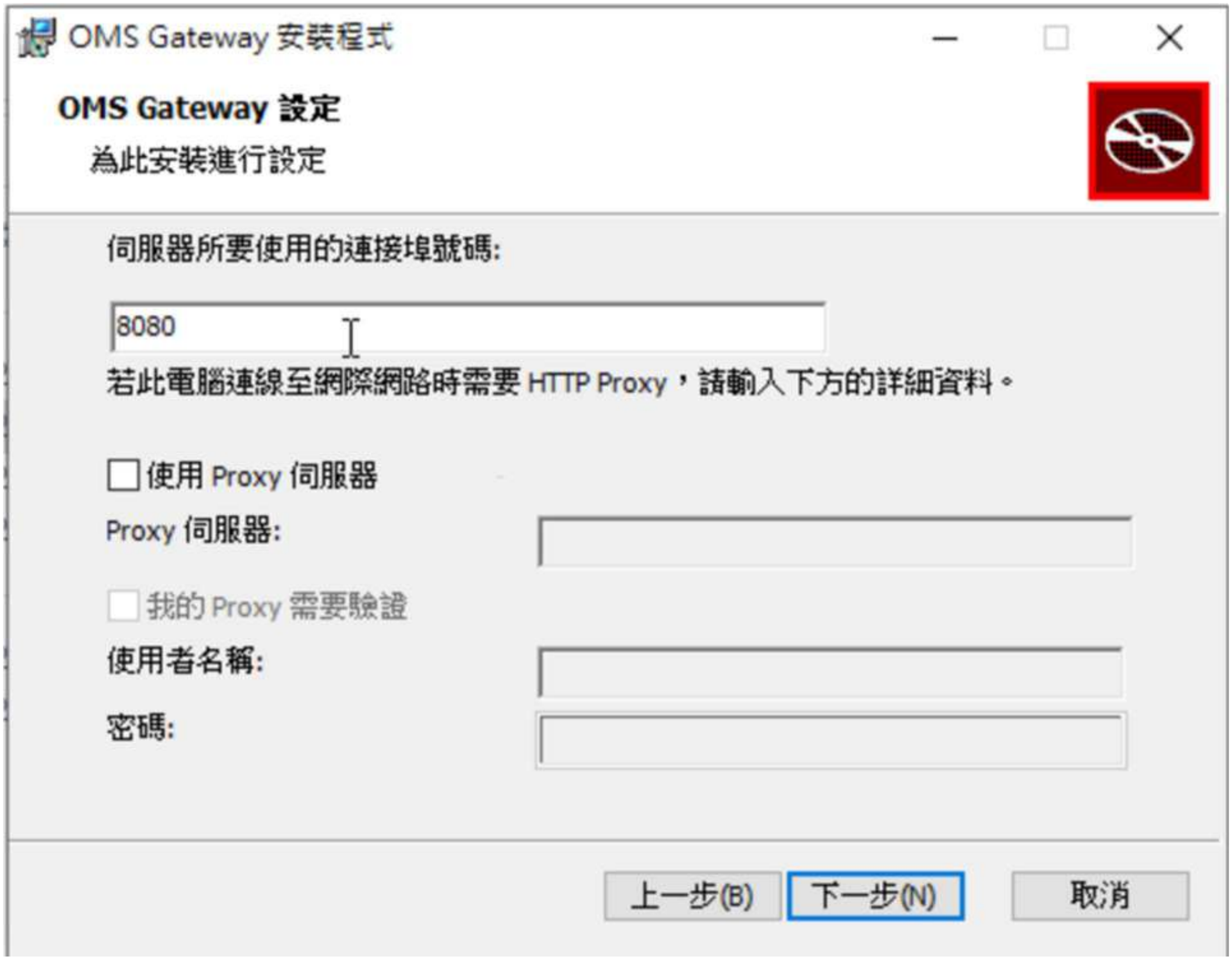
您可以在 Azure Log Analytics 入口網站取得您的工作區識別碼及金鑰。Azure Commercial 的 Log Analytics 入口網站位於 https://www.microsoft.com/oms/。

按一下 [進階] 以提供 HTTP Proxy 設定。

按一下 [下一步]，Azure 記錄分析服務將會驗證這些內容。

- 方法 B

準備一台可以對外連線主機扮演 Gateway 角色，安裝 Log Analytics，安裝方式與方法 A 相同，另額外安裝 OMS Gateway，安裝過程皆使用預設安裝即可



OMS Gateway 設定

為此安裝進行設定

伺服器所要使用的連接埠號碼:

8080

若此電腦連線至網際網路時需要 HTTP Proxy，請輸入下方的詳細資料。

☐ 使用 Proxy 伺服器

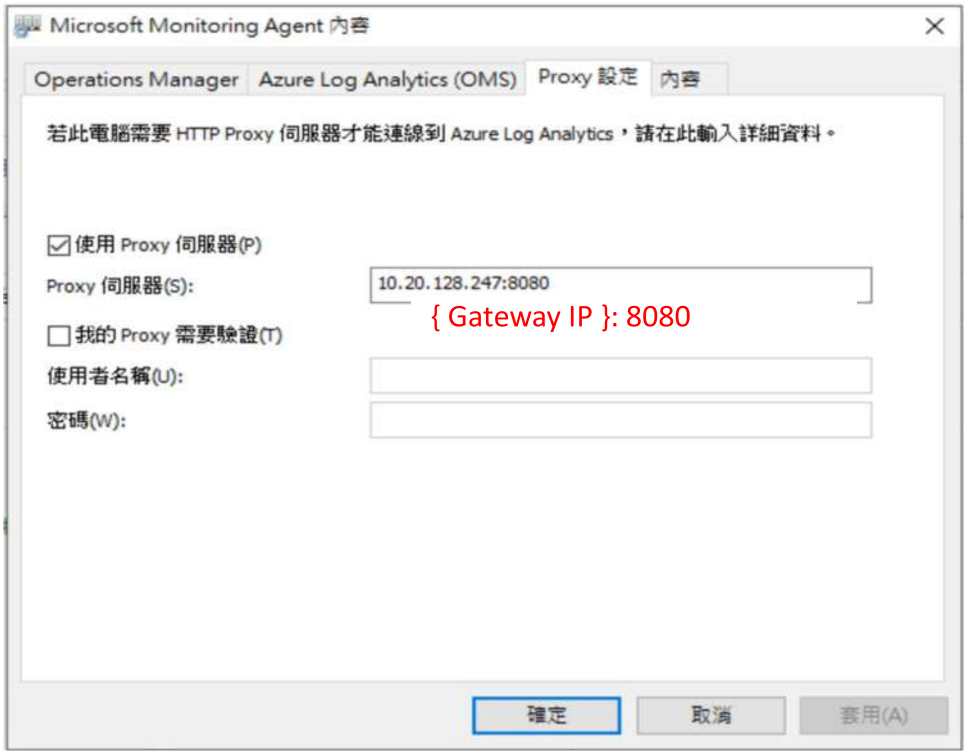
Proxy 伺服器:

☐ 我的 Proxy 需要驗證

使用者名稱:

密碼:

於其他被監控主機上安裝安裝 Log Analytics，安裝方式與方法 A 相同，接下來設定 Proxy，進到 控制台 > Microsoft Monitoring Agent > Proxy 設定，將前述 Gateway 主機 IP 輸入，後面接上:8080 即可。



Microsoft Monitoring Agent 內容

若此電腦需要 HTTP Proxy 伺服器才能連線到 Azure Log Analytics，請在此輸入詳細資料。

☑ 使用 Proxy 伺服器(P)

Proxy 伺服器(S): 10.20.128.247:8080

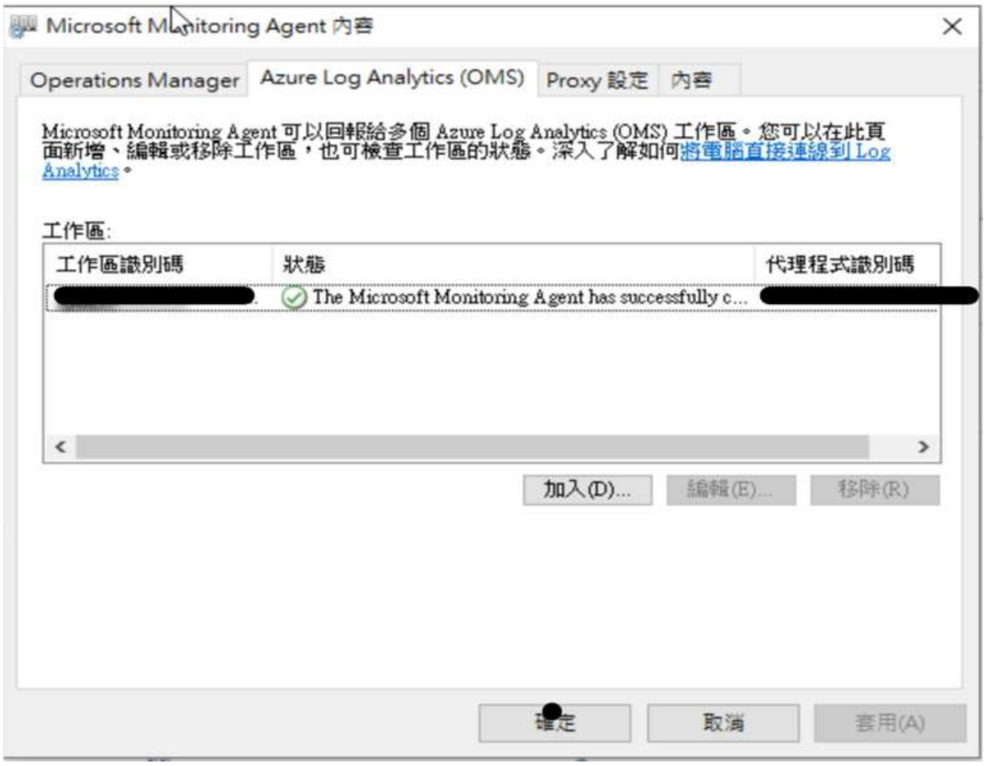
{ Gateway IP }: 8080

□ 我的 Proxy 需要驗證(T)

使用者名稱(U):

密碼(W):

確認連線狀態，如果狀態為綠色勾勾代表完成，若沒出現綠色勾勾則再重新編輯設定一次連線即可。



Microsoft Monitoring Agent 內容

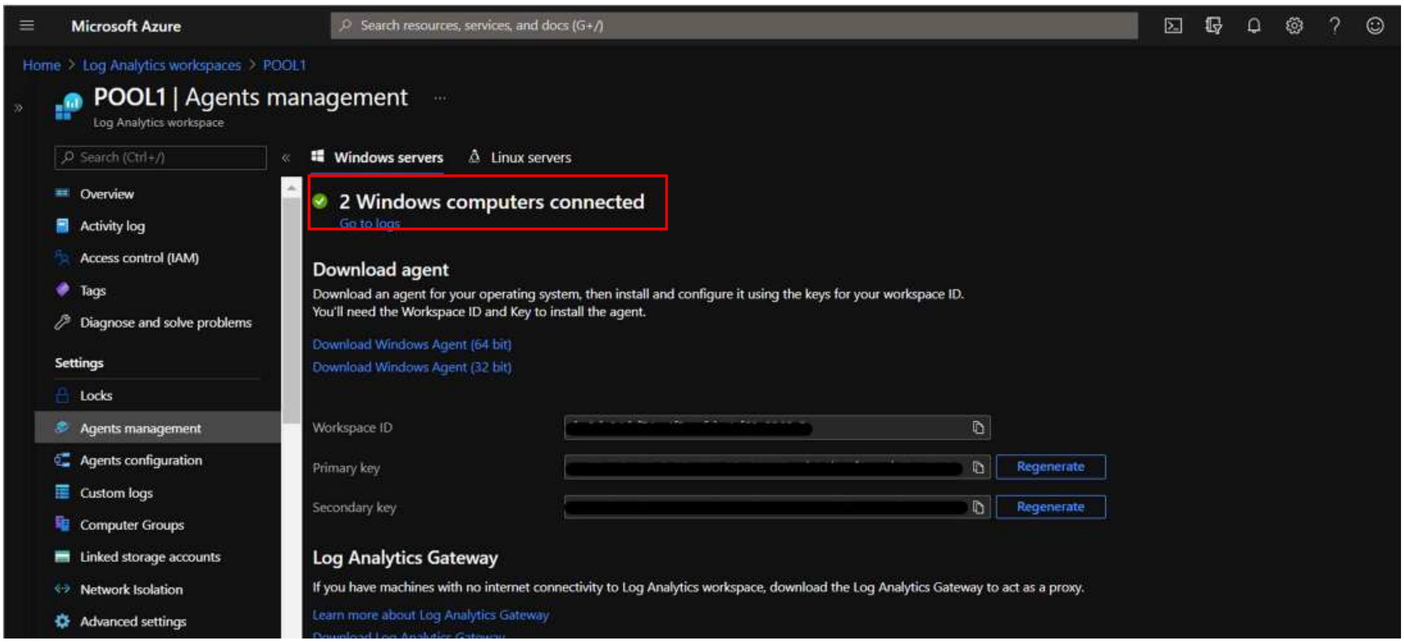
Microsoft Monitoring Agent 可以回報給多個 Azure Log Analytics (OMS) 工作區。您可以在此頁面新增、編輯或移除工作區，也可檢查工作區的狀態。深入了解如何將電腦直接連線到 Log Analytics。

工作區:

工作區識別碼	狀態	代理程式識別碼
[redacted]	✓ The Microsoft Monitoring Agent has successfully c...	[redacted]

3. 確認連線是否成功

進入 Agents Management 查看 Windows server or Linux server，若畫面上顯示綠色勾勾代表連線成立 (勾勾後方數字為連線機器數量)。



✓ 2 Windows computers connected

Download agent

Download an agent for your operating system, then install and configure it using the keys for your workspace ID. You'll need the Workspace ID and Key to install the agent.

Workspace ID [redacted]

Primary key [redacted]

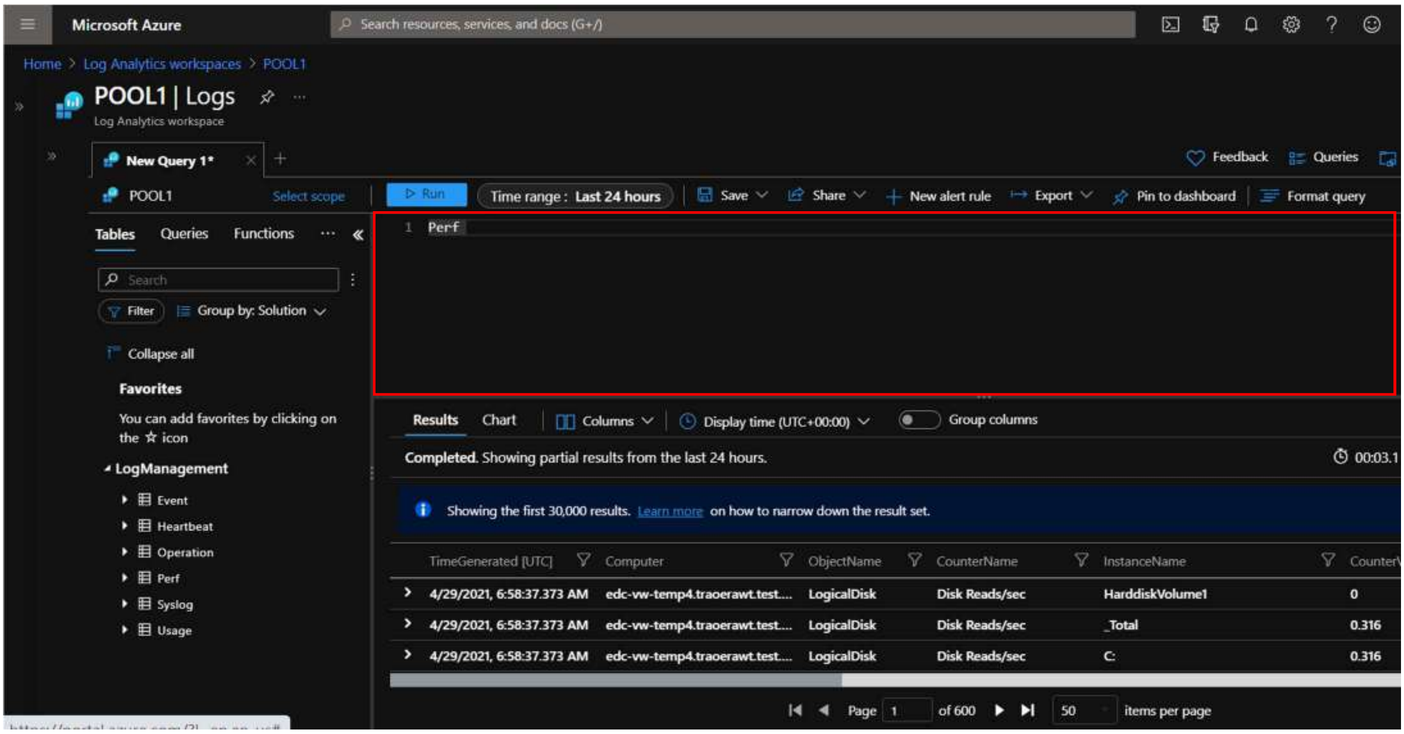
Secondary key [redacted]

Log Analytics Gateway

If you have machines with no internet connectivity to Log Analytics workspace, download the Log Analytics Gateway to act as a proxy.

4. Log 查詢

進到 Logs 內可以輸入想要查詢的資料，並且點下 Run，下方會顯示出查詢的結果，如下圖我們在 Query 的地方輸入 Perf 關鍵字，系統會搜尋出所有關於 performance 的資訊。



```
1   Perf
```

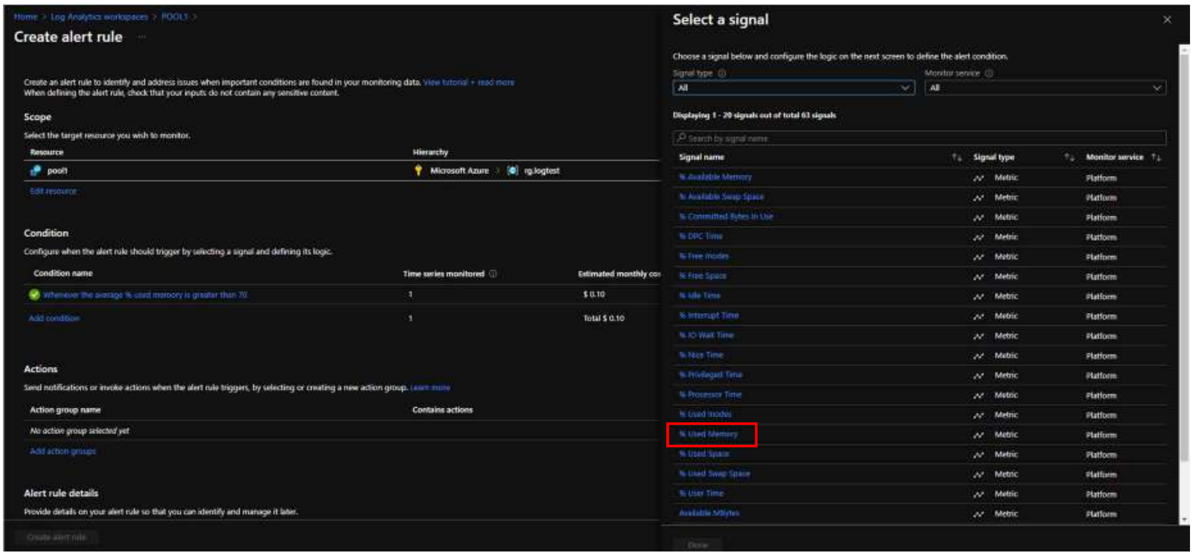
Completed. Showing partial results from the last 24 hours.

Showing the first 30,000 results. Learn more on how to narrow down the result set.

TimeGenerated [UTC]	Computer	ObjectName	CounterName	InstanceName	CounterV
4/29/2021, 6:58:37.373 AM	edc-vw-temp4.traoerawt.test....	LogicalDisk	Disk Reads/sec	HarddiskVolume1	0
4/29/2021, 6:58:37.373 AM	edc-vw-temp4.traoerawt.test....	LogicalDisk	Disk Reads/sec	_Total	0.316
4/29/2021, 6:58:37.373 AM	edc-vw-temp4.traoerawt.test....	LogicalDisk	Disk Reads/sec	C:	0.316

5. 配置警告

進入 Alert > 在 condition 的地方建立想要產生報警的內容。建立成功後，在 condition name 的地方會有綠色的勾勾。我們在此配置當系統的記憶體使用率平均超過 70%，則透過 Email 發出警告信件作為範例。



Create an alert rule to identify and address issues when important conditions are found in your monitoring data. View tutorial + read more
When defining the alert rule, check that your inputs do not contain any sensitive content.

Scope

Select the target resource you wish to monitor.

Resource	Hierarchy
pool1	Microsoft Azure > rg.logtest

Condition

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Condition name	Time series monitored	Estimated monthly cos
✓ Whenever the average % used memory is greater than 70	1	$ 0.10
Add condition	1	Total $ 0.10

Actions

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group. Learn more

Action group name	Contains actions
No action group selected yet	

Alert rule details

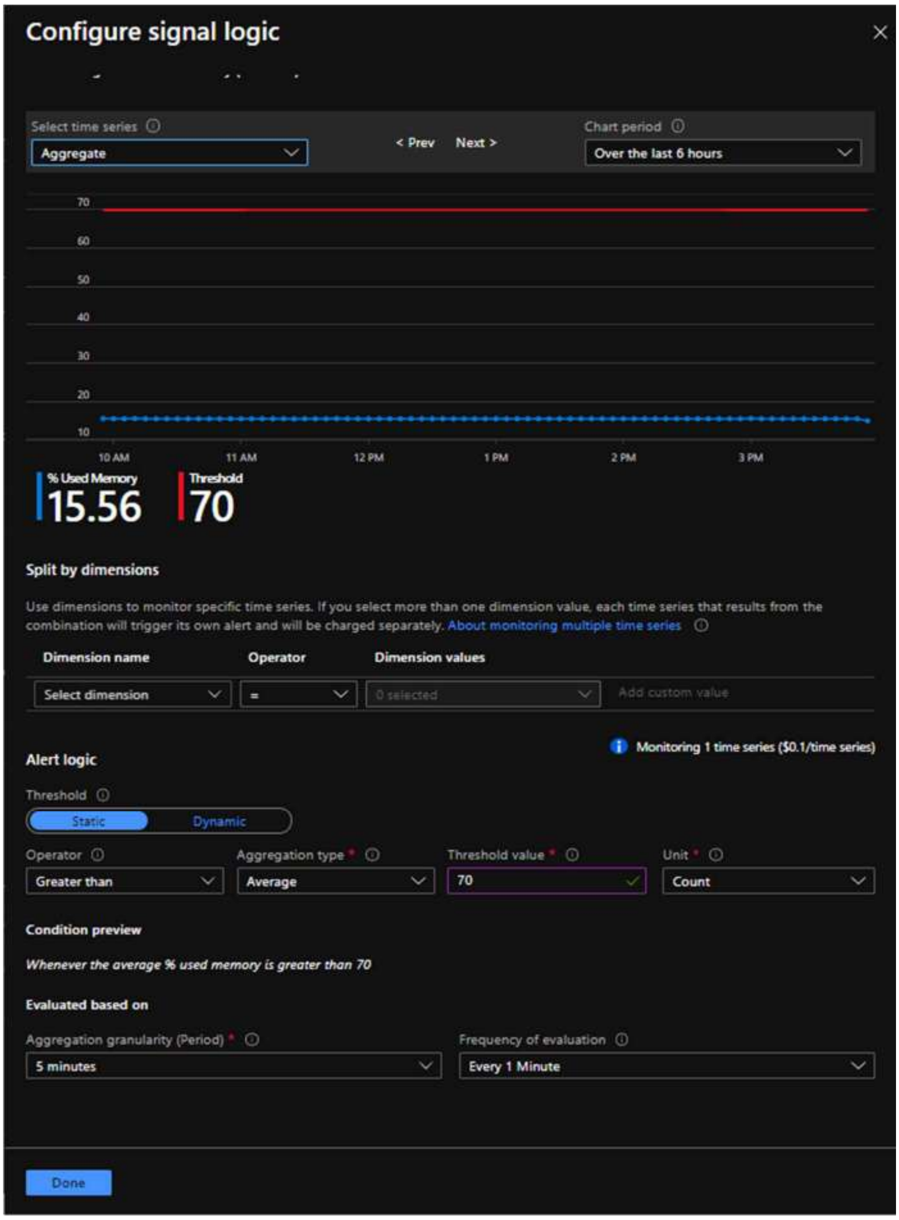
Provide details on your alert rule so that you can identify and manage it later.

Choose a signal below and configure the logic on the next screen to define the alert condition.

Signal type: All
Monitor service: All

Displaying 1 - 20 signals out of total 63 signals

Signal name	Signal type	Monitor service
% Available Memory	Metric	Platform
% Available Swap Space	Metric	Platform
% Committed Bytes In Use	Metric	Platform
% DPC Time	Metric	Platform
% Free Inodes	Metric	Platform
% Free Space	Metric	Platform
% Idle Time	Metric	Platform
% Interrupt Time	Metric	Platform
% IO Wait Time	Metric	Platform
% Nice Time	Metric	Platform
% Privileged Time	Metric	Platform
% Processor Time	Metric	Platform
% Used Inodes	Metric	Platform
% Used Memory	Metric	Platform
% Used Space	Metric	Platform
% Used Swap Space	Metric	Platform
% User Time	Metric	Platform
Available MBytes	Metric	Platform



Configure signal logic

Select time series: Aggregate

< Prev   Next >

Chart period: Over the last 6 hours

% Used Memory 15.56

Threshold 70

Split by dimensions

Use dimensions to monitor specific time series. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately. About monitoring multiple time series

Dimension name	Operator	Dimension values	
Select dimension	=	0 selected	Add custom value

Monitoring 1 time series ($0.1/time series)

Alert logic

Threshold: Static | Dynamic

Operator: Greater than

Aggregation type *: Average

Threshold value *: 70

Unit *: Count

Condition preview

Whenever the average % used memory is greater than 70

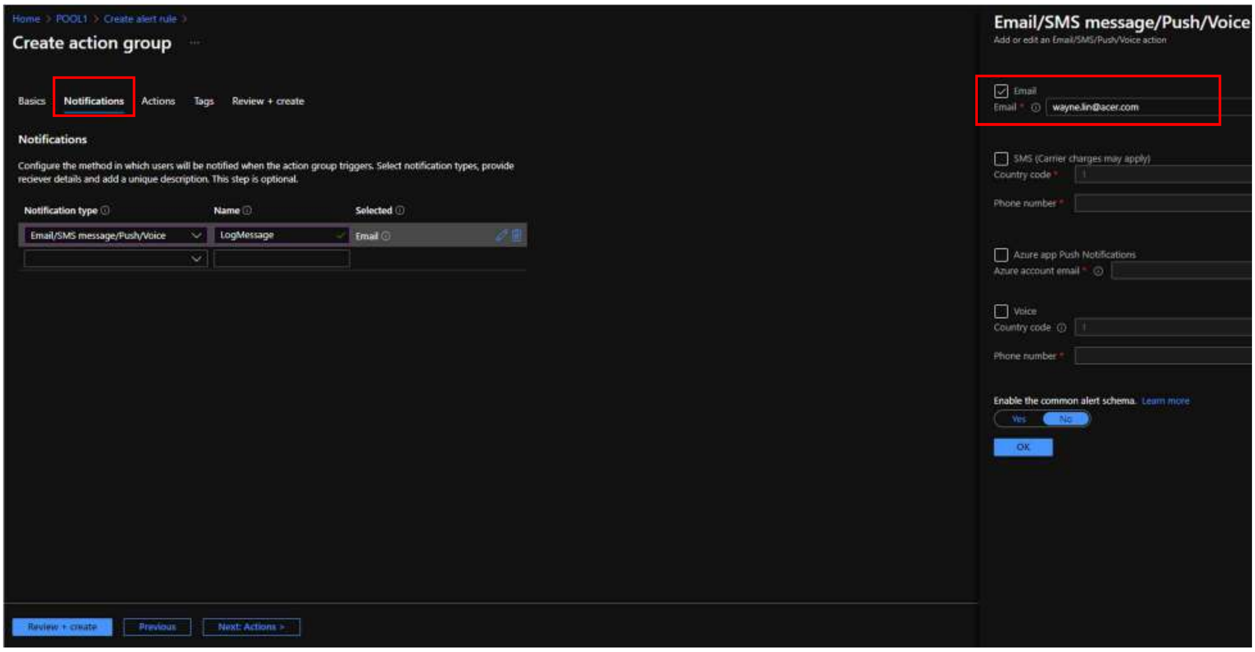
Evaluated based on

Aggregation granularity (Period) *: 5 minutes

Frequency of evaluation: Every 1 Minute

Done

接下來到 Action 的地方，配置警報發生後要發送 mail 告知管理人員的配置。



Create action group

Notifications

Configure the method in which users will be notified when the action group triggers. Select notification types, provide reciever details and add a unique description. This step is optional.

Notification type	Name	Selected
Email/SMS message/Push/Voice	LogMessage	Email

Email/SMS message/Push/Voice

Add or edit an Email/SMS/Push/Voice action

☑ Email
Email * wayne.lin@acer.com

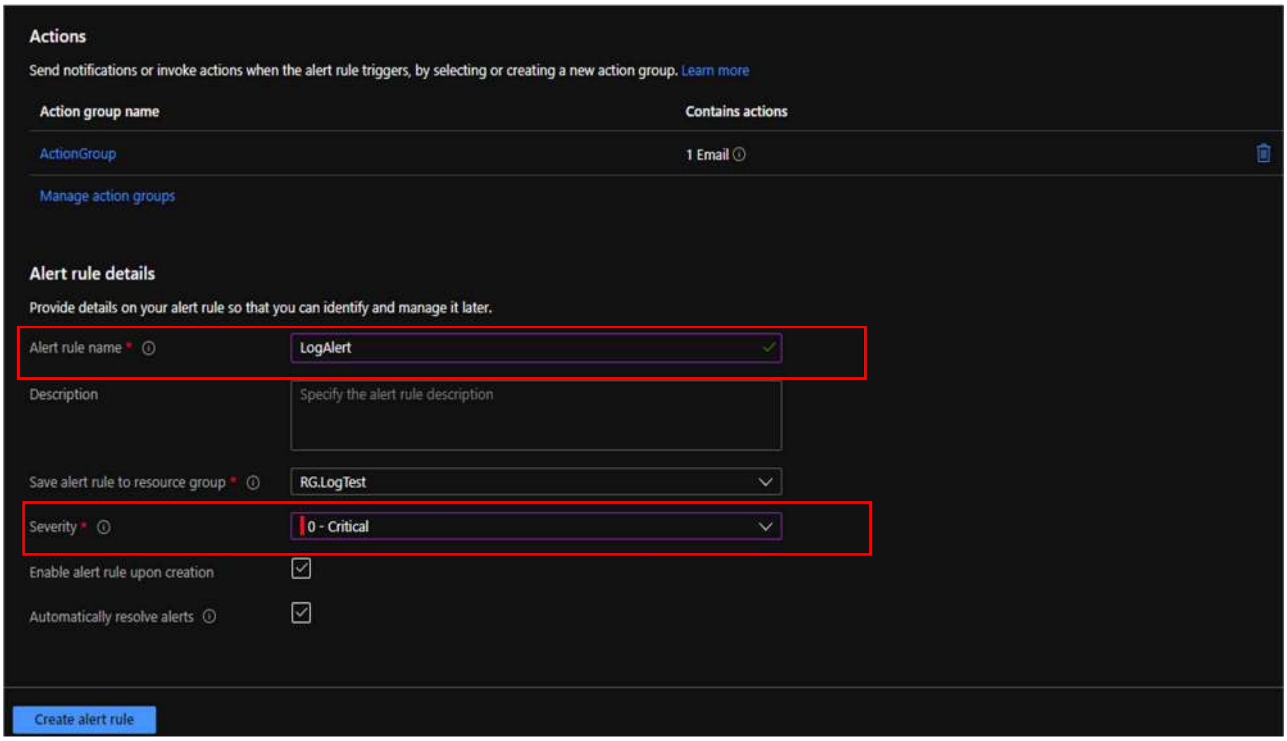
☐ SMS (Carrier charges may apply)
Country code * 1
Phone number *

☐ Azure app Push Notifications
Azure account email *

☐ Voice
Country code 1
Phone number *

Enable the common alert schema. Learn more
Yes [✓ No]

設定完 Action 的 Notifications 就可以執行 Create，創建完 Action 後為 Alert Rule 命名，再選取該警報的 Severity 等級即可完成警告配置。



Actions

Send notifications or invoke actions when the alert rule triggers, by selecting or creating a new action group. Learn more

Action group name	Contains actions
ActionGroup	1 Email

Alert rule details

Provide details on your alert rule so that you can identify and manage it later.

Alert rule name * LogAlert

Description Specify the alert rule description

Save alert rule to resource group * RG.LogTest

Severity * 0 - Critical

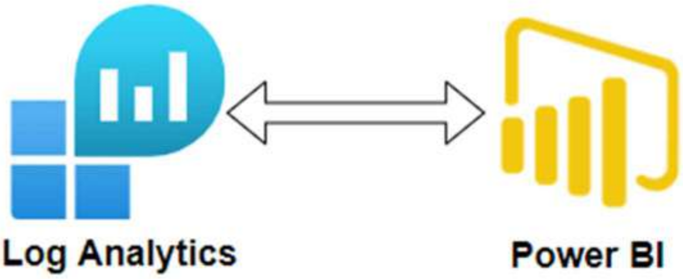
Enable alert rule upon creation ☑

Automatically resolve alerts ☑

到此已經完成整個 **Log Analytics** 的配置

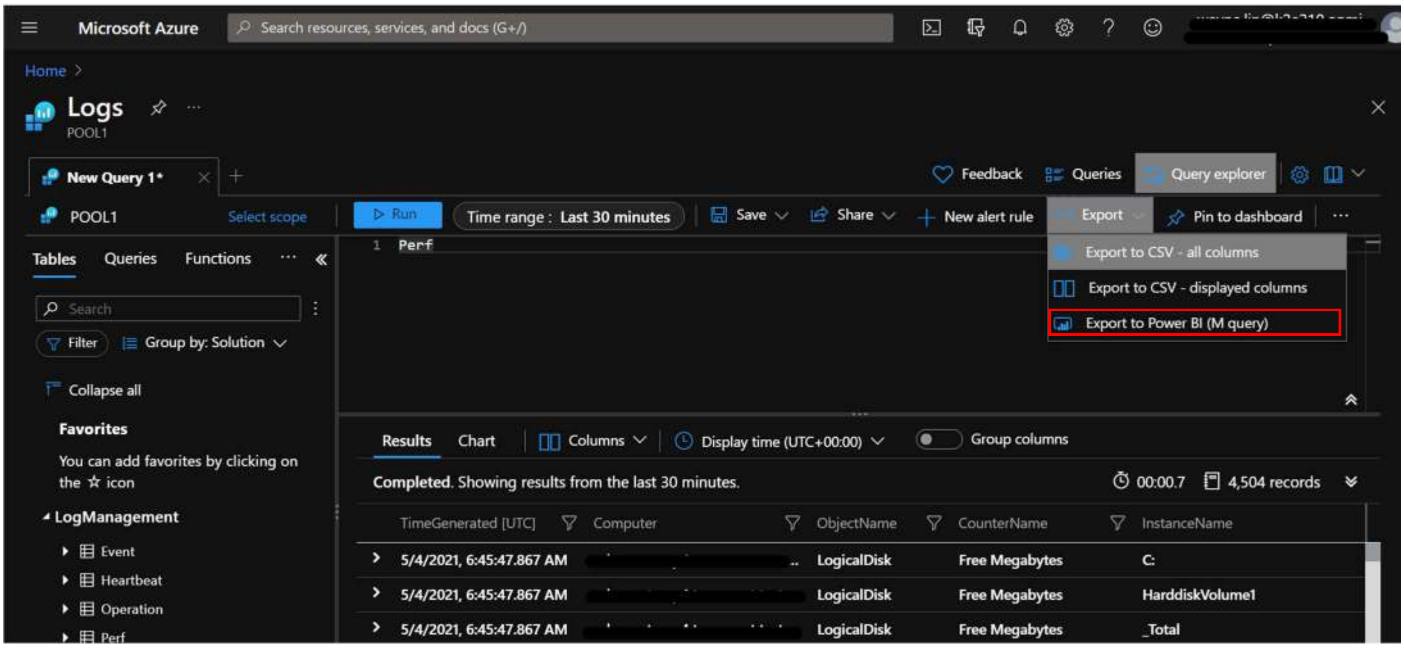
Log Analytics 整合 Power BI

這裡我們要將 Log Analytics 所接收到的所有關於效能的資訊傳送到 Power BI，再由 Power BI 整理出更加視覺化的內容。



1. 匯出 LOG

透過 Analytics Log 將所需要的 LOG 匯出。這邊匯出會是一個檔案，需要將檔案的內容複製。



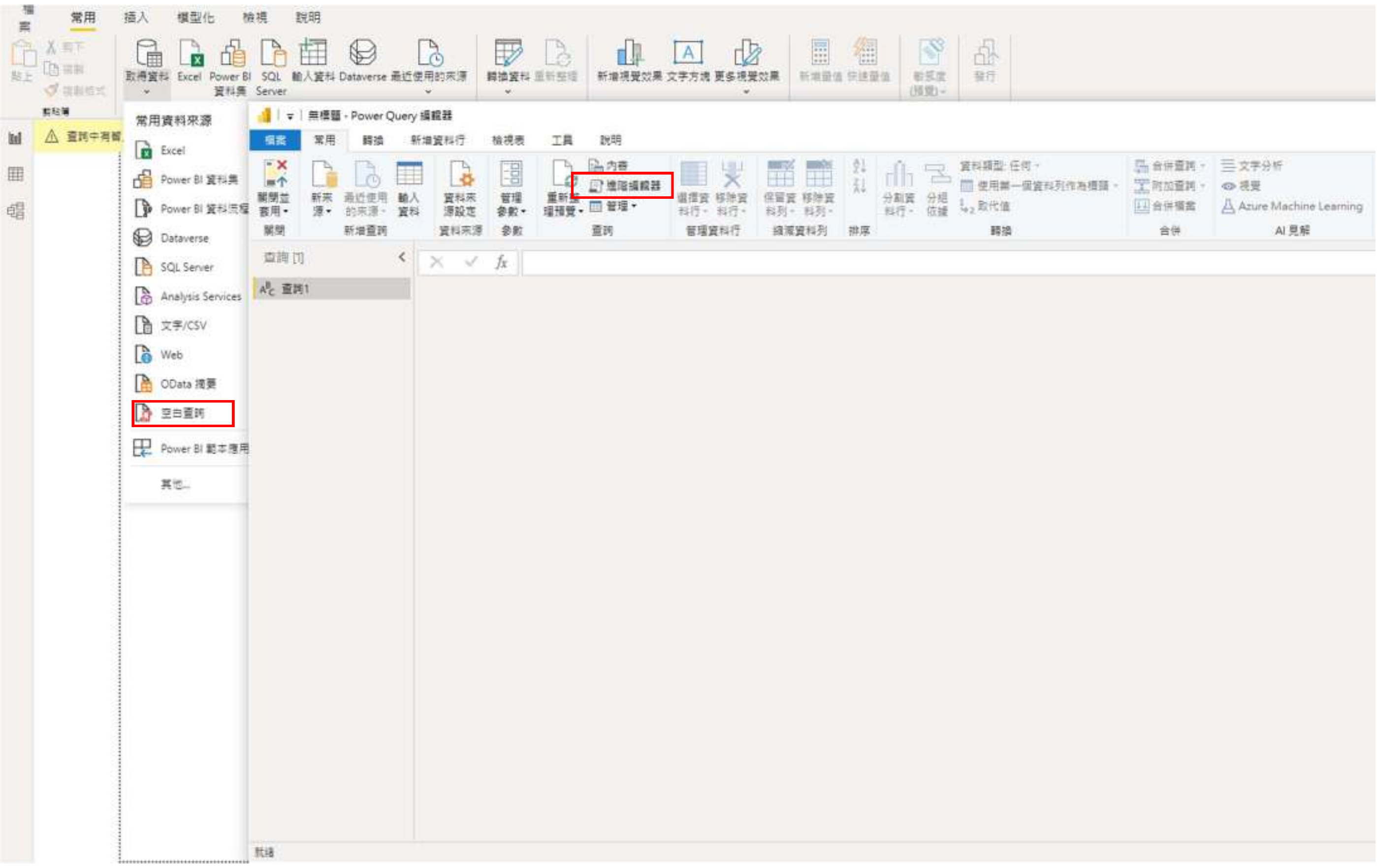
```
Perf
```

Completed. Showing results from the last 30 minutes.

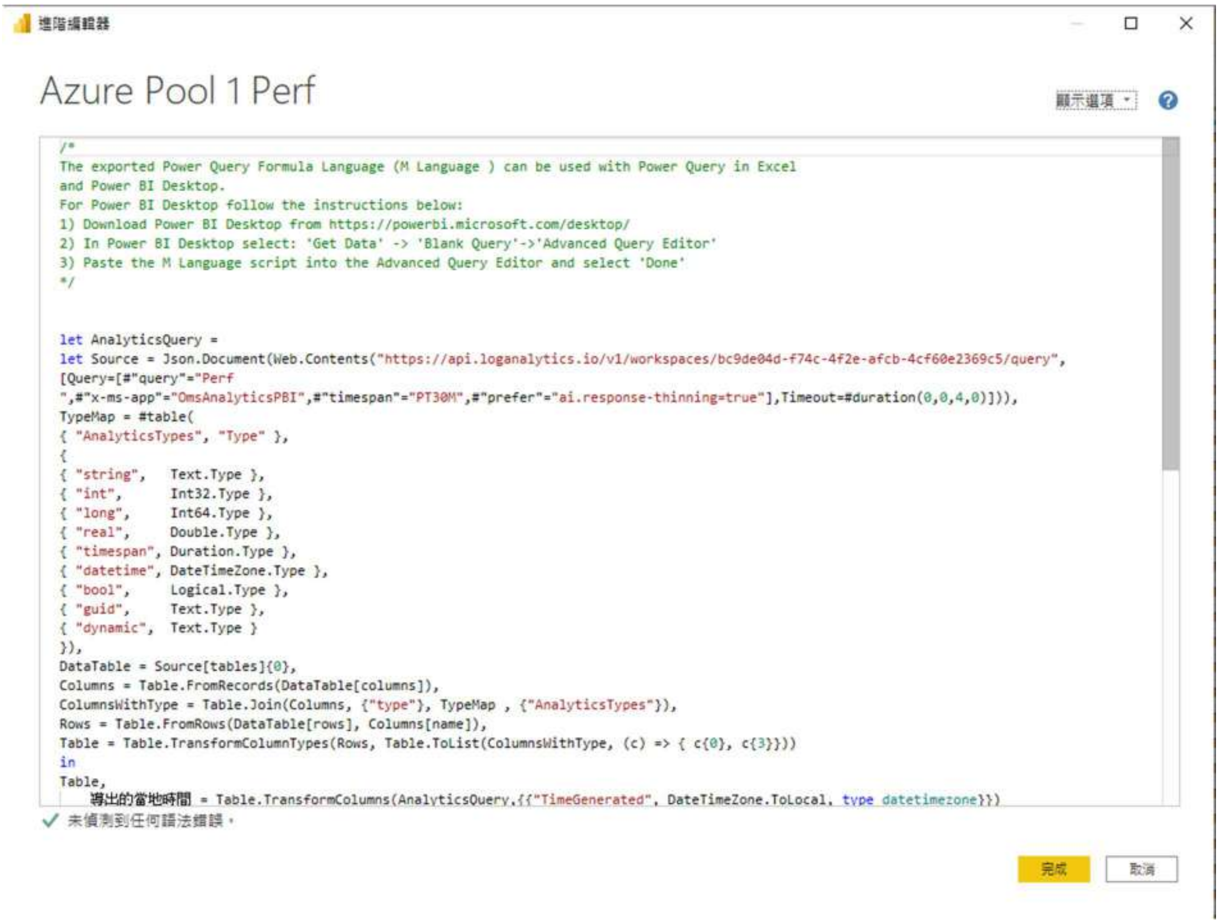
TimeGenerated [UTC]	Computer	ObjectName	CounterName	InstanceName
5/4/2021, 6:45:47.867 AM	[redacted]	LogicalDisk	Free Megabytes	C:
5/4/2021, 6:45:47.867 AM	[redacted]	LogicalDisk	Free Megabytes	HarddiskVolume1
5/4/2021, 6:45:47.867 AM	[redacted]	LogicalDisk	Free Megabytes	_Total

2. 將 LOG 匯入 Power BI

將匯出的 M Query 內容輸入到 Power BI，以作為資料來源。Power BI 介面選到 新來源 > 空白查詢 > 進階編輯器



將剛剛所匯出的內容輸入至進階編輯器。



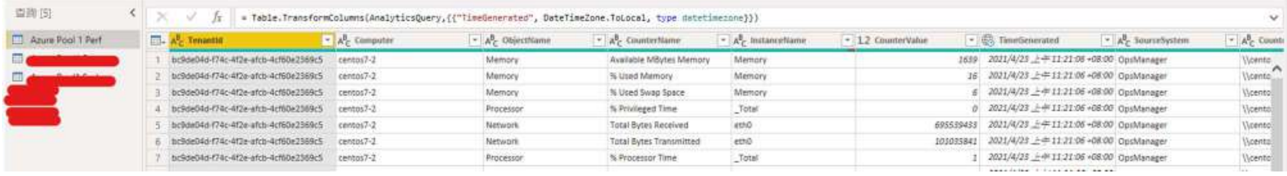
Azure Pool 1 Perf

```
/*
The exported Power Query Formula Language (M Language ) can be used with Power Query in Excel
and Power BI Desktop.
For Power BI Desktop follow the instructions below:
1) Download Power BI Desktop from https://powerbi.microsoft.com/desktop/
2) In Power BI Desktop select: 'Get Data' -> 'Blank Query'->'Advanced Query Editor'
3) Paste the M Language script into the Advanced Query Editor and select 'Done'
*/


let AnalyticsQuery =
let Source = Json.Document(Web.Contents("https://api.loganalytics.io/v1/workspaces/bc9de04d-f74c-4f2e-afcb-4cf60e2369c5/query",
[Query=[#"query"="Perf
",#"x-ms-app"="OmsAnalyticsPBI",#"timespan"="PT30M",#"prefer"="ai.response-thinning=true"],Timeout=#duration(0,0,4,0)])),
TypeMap = #table(
{ "AnalyticsTypes", "Type" },
{
{ "string",   Text.Type },
{ "int",      Int32.Type },
{ "long",     Int64.Type },
{ "real",     Double.Type },
{ "timespan", Duration.Type },
{ "datetime", DateTimeZone.Type },
{ "bool",     Logical.Type },
{ "guid",     Text.Type },
{ "dynamic",  Text.Type }
}),
DataTable = Source[tables]{0},
Columns = Table.FromRecords(DataTable[columns]),
ColumnsWithType = Table.Join(Columns, {"type"}, TypeMap , {"AnalyticsTypes"}),
Rows = Table.FromRows(DataTable[rows], Columns[name]),
Table = Table.TransformColumnTypes(Rows, Table.ToList(ColumnsWithType, (c) => { c{0}, c{3}}))
in
Table,
    導出的當地時間 = Table.TransformColumns(AnalyticsQuery,{{"TimeGenerated", DateTimeZone.ToLocal, type datetimezone}})
```

✓ 未偵測到任何語法錯誤。

點選完成後將呈現出以下表格，呈現出此表，代表匯出完成。

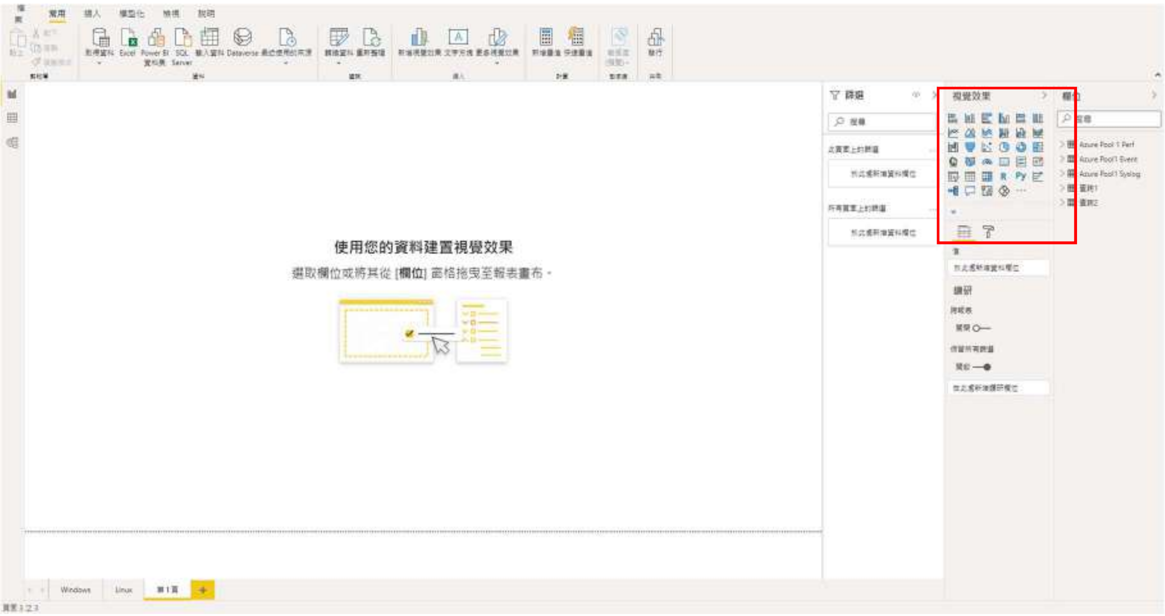


```
= Table.TransformColumns(AnalyticsQuery,{{"TimeGenerated", DateTimeZone.ToLocal, type datetimezone}})
```

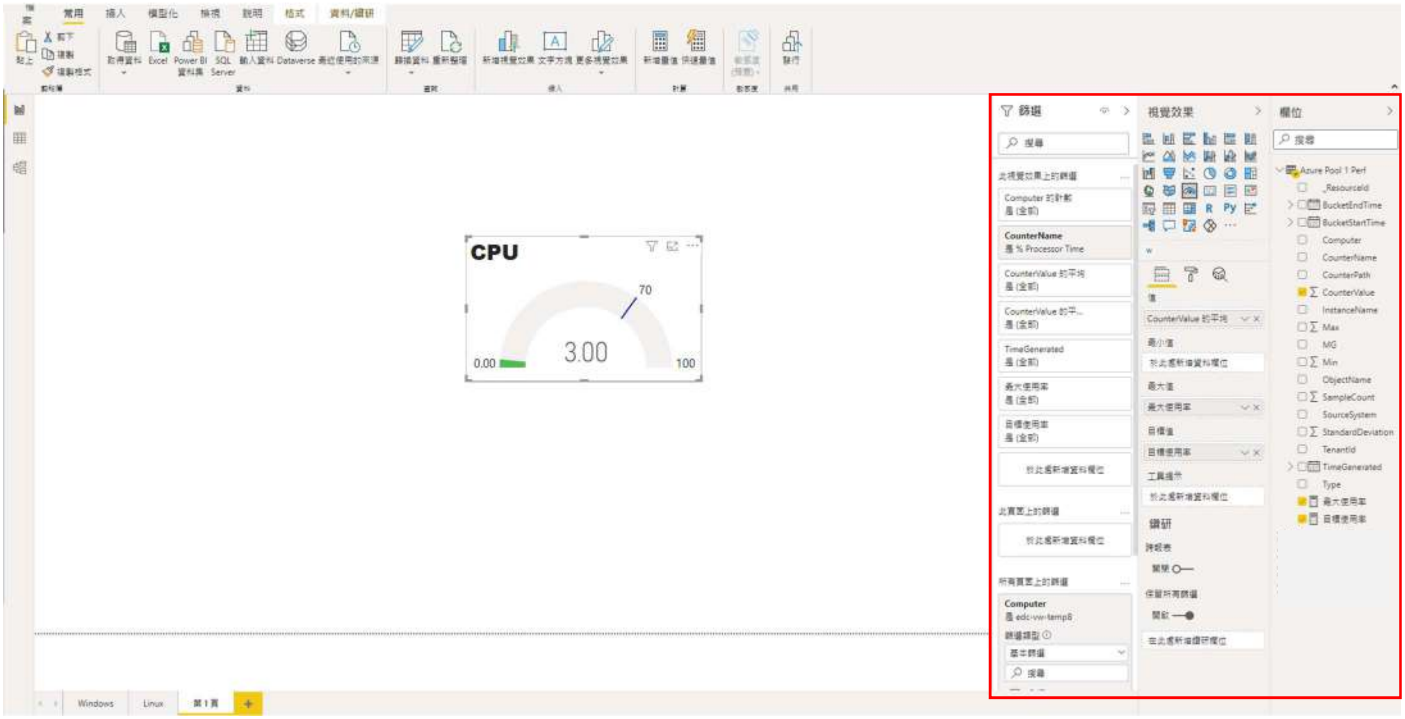
	TenantId	Computer	ObjectName	CounterName	InstanceName	CounterValue	TimeGenerated	SourceSystem	Count
1	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Memory	Available MBytes Memory	Memory	1639	2021/4/23 上午 11:21:08 +08:00	OpsManager	\\cento
2	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Memory	% Used Memory	Memory	16	2021/4/23 上午 11:21:06 +08:00	OpsManager	\\cento
3	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Memory	% Used Swap Space	Memory	6	2021/4/23 上午 11:21:06 +08:00	OpsManager	\\cento
4	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Processor	% Privileged Time	_Total	0	2021/4/23 上午 11:21:06 +08:00	OpsManager	\\cento
5	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Network	Total Bytes Received	eth0	695539433	2021/4/23 上午 11:21:06 +08:00	OpsManager	\\cento
6	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Network	Total Bytes Transmitted	eth0	101035841	2021/4/23 上午 11:21:06 +08:00	OpsManager	\\cento
7	bc9de04d-f74c-4f2e-afcb-4cf60e2369c5	centos7-2	Processor	% Processor Time	_Total	1	2021/4/23 上午 11:21:06 +08:00	OpsManager	\\cento

匯入完成後我們到報表的介面開始製作屬於我們的監控畫面。

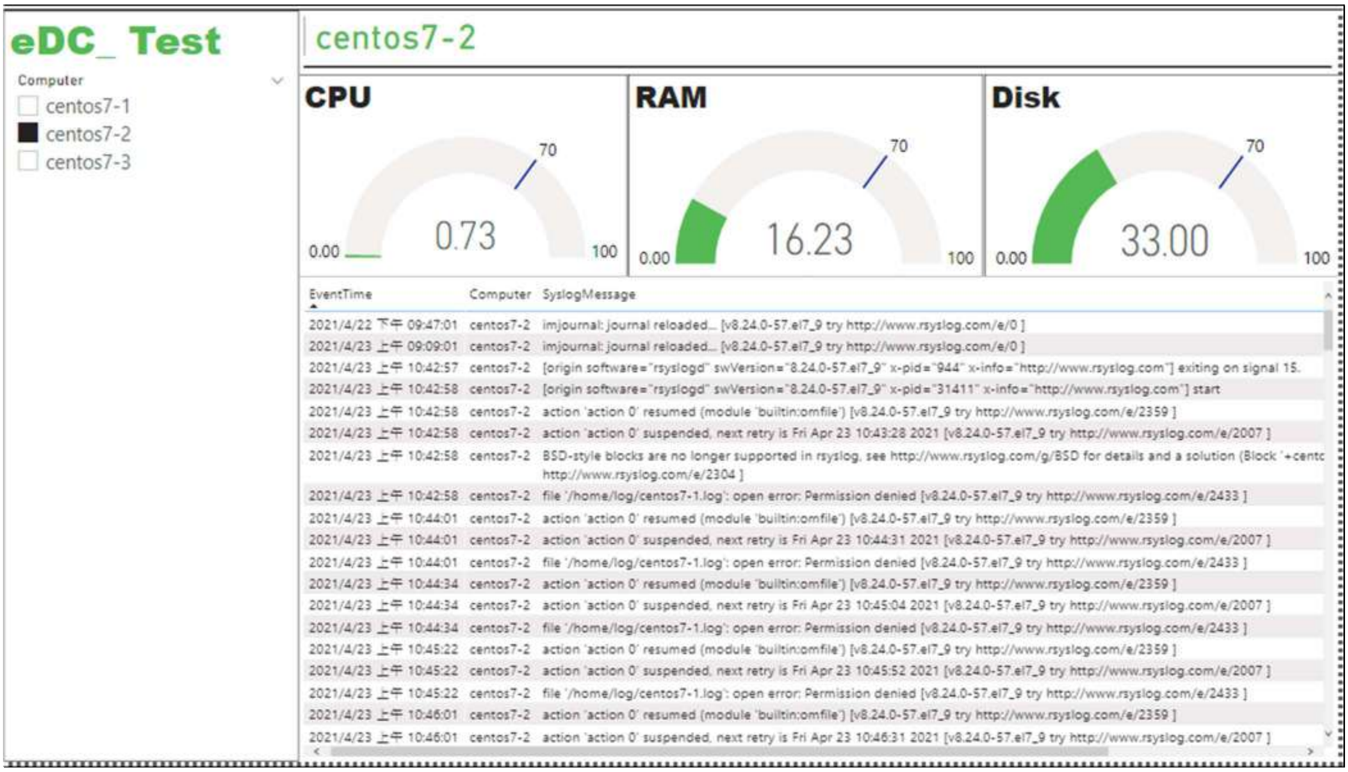
在紅色框框的地方可以選擇適合自己的效果。



之後在欄位的地方輸入自己想要的數據，即可產出一份屬於自己的報表。



下面這張圖是根據 CPU 與記憶體以及硬碟所整理出來的報表，這樣對 IT 人員在監控系統顯得非常容易，也可以更快的發現問題。



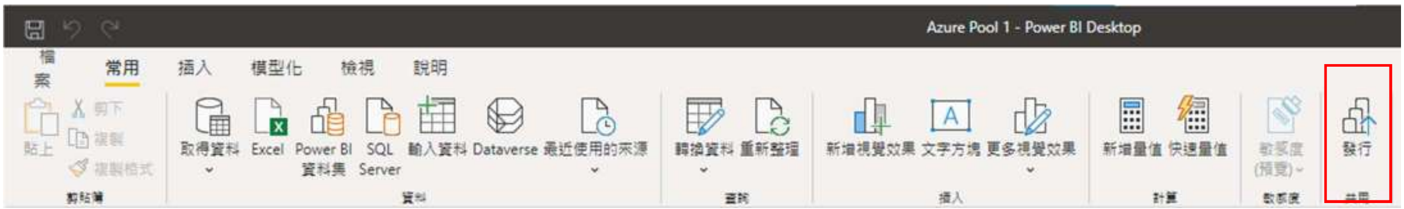
EventTime	Computer	SyslogMessage
2021/4/22 下午 09:47:01	centos7-2	imjournal: journal reloaded... [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/0]
2021/4/23 上午 09:09:01	centos7-2	imjournal: journal reloaded... [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/0]
2021/4/23 上午 10:42:57	centos7-2	[origin software="rsyslogd" swVersion="8.24.0-57.el7_9" x-pid="944" x-info="http://www.rsyslog.com"] exiting on signal 15.
2021/4/23 上午 10:42:58	centos7-2	[origin software="rsyslogd" swVersion="8.24.0-57.el7_9" x-pid="31411" x-info="http://www.rsyslog.com"] start
2021/4/23 上午 10:42:58	centos7-2	action 'action 0' resumed (module 'builtin:omfile') [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2359]
2021/4/23 上午 10:42:58	centos7-2	action 'action 0' suspended, next retry is Fri Apr 23 10:43:28 2021 [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2007]
2021/4/23 上午 10:42:58	centos7-2	BSD-style blocks are no longer supported in rsyslog, see http://www.rsyslog.com/g/BSD for details and a solution (Block '+centc http://www.rsyslog.com/e/2304]
2021/4/23 上午 10:42:58	centos7-2	file '/home/log/centos7-1.log': open error: Permission denied [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2433]
2021/4/23 上午 10:44:01	centos7-2	action 'action 0' resumed (module 'builtin:omfile') [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2359]
2021/4/23 上午 10:44:01	centos7-2	action 'action 0' suspended, next retry is Fri Apr 23 10:44:31 2021 [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2007]
2021/4/23 上午 10:44:01	centos7-2	file '/home/log/centos7-1.log': open error: Permission denied [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2433]
2021/4/23 上午 10:44:34	centos7-2	action 'action 0' resumed (module 'builtin:omfile') [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2359]
2021/4/23 上午 10:44:34	centos7-2	action 'action 0' suspended, next retry is Fri Apr 23 10:45:04 2021 [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2007]
2021/4/23 上午 10:44:34	centos7-2	file '/home/log/centos7-1.log': open error: Permission denied [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2433]
2021/4/23 上午 10:45:22	centos7-2	action 'action 0' resumed (module 'builtin:omfile') [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2359]
2021/4/23 上午 10:45:22	centos7-2	action 'action 0' suspended, next retry is Fri Apr 23 10:45:52 2021 [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2007]
2021/4/23 上午 10:45:22	centos7-2	file '/home/log/centos7-1.log': open error: Permission denied [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2433]
2021/4/23 上午 10:46:01	centos7-2	action 'action 0' resumed (module 'builtin:omfile') [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2359]
2021/4/23 上午 10:46:01	centos7-2	action 'action 0' suspended, next retry is Fri Apr 23 10:46:31 2021 [v8.24.0-57.el7_9 try http://www.rsyslog.com/e/2007]

整合進 Power BI 可以透過 Power BI 產出 LOG Analytics 的所有資訊，並且將資訊相互關聯，如上圖所示，如果要觀看單一系統的資訊，可以篩選想觀看的系統名稱 Power BI 將會呈現您所選取的系統上所有相關資訊報表。

簡單來說就是可以更加值觀並快速的知道所有系統的資訊狀況，這樣做可以不必透過繁瑣的 Query 過程，就能夠查看所有系統的資訊。

3. 發佈至雲端

Power BI 也可以同步上傳至 WEB，點按下圖之發行鈕，就可以將在 Power BI Desktop 上製作的報表上傳至帳戶上的雲端工作區，這樣就可以隨時隨地監控系統的所有狀況，不管是在公司還是在外地出差，都可以透過瀏覽器第一時間知道系統狀況，如果是 Mobile 平台則可以透過 Power BI APP 查看。



至此我們已經利用 Azure Log Analytics 及 Power BI 快速完成一套簡單的雲端日誌收集及分析系統。