

自動化調整雲端Spark 異常流量偵測系統

許時準、周小慧
國立中央大學 電算中心

論文發表於 TANET2016研討會

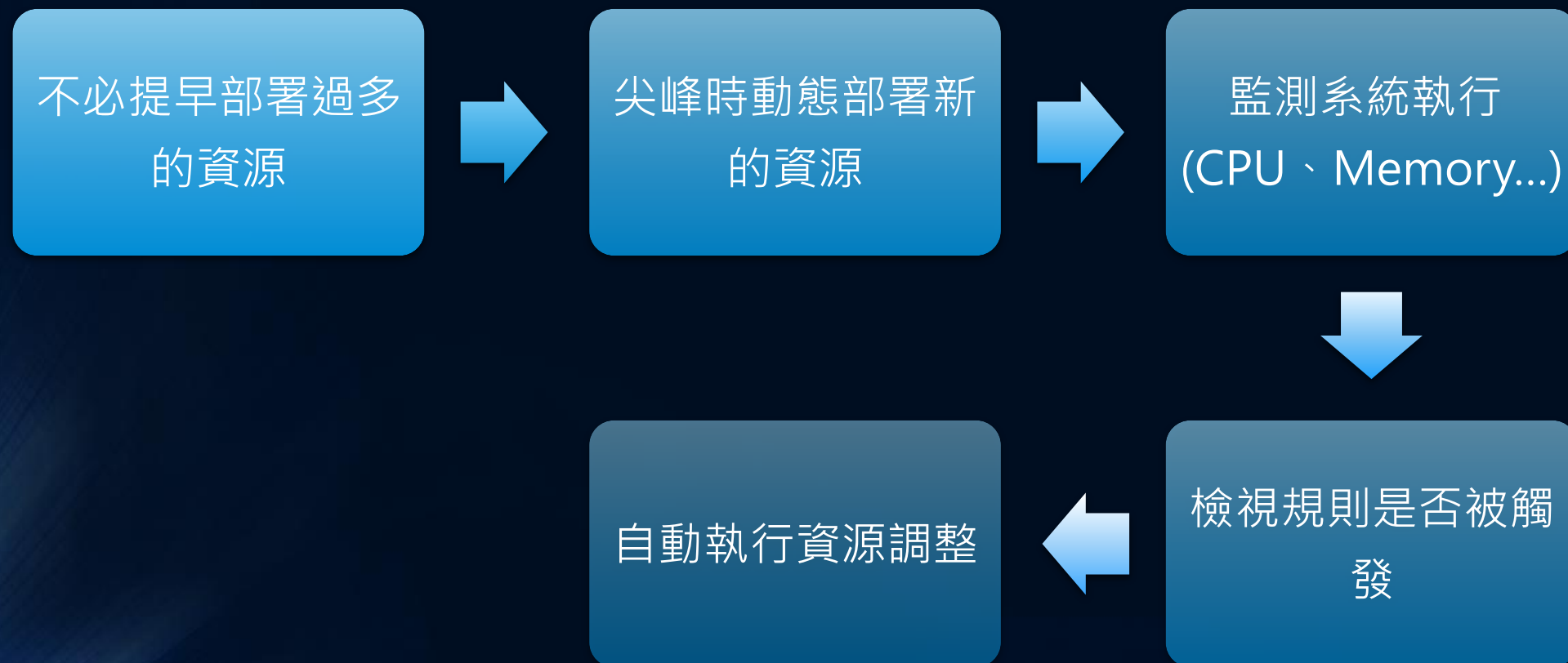
報告大綱

- 系統目標
- Auto-Scaling 相關研究
- Auto-Scaling Spark偵測系統架構
- Spark Cluster 設計
- 系統測試
- 結論

系統目標

- 因應台灣學術網路骨幹頻寬由10G提升至100G，但帶來之網路攻擊，其規模及強度也將大幅增加。
- 以自動化調整(auto-scaling)雲端架構搭配動態部署的Spark Cluster網路異常流量偵測系統，依照網路流量之大小自動調整Spark Cluster的計算節點數量。

Auto-Scaling相關研究(1)

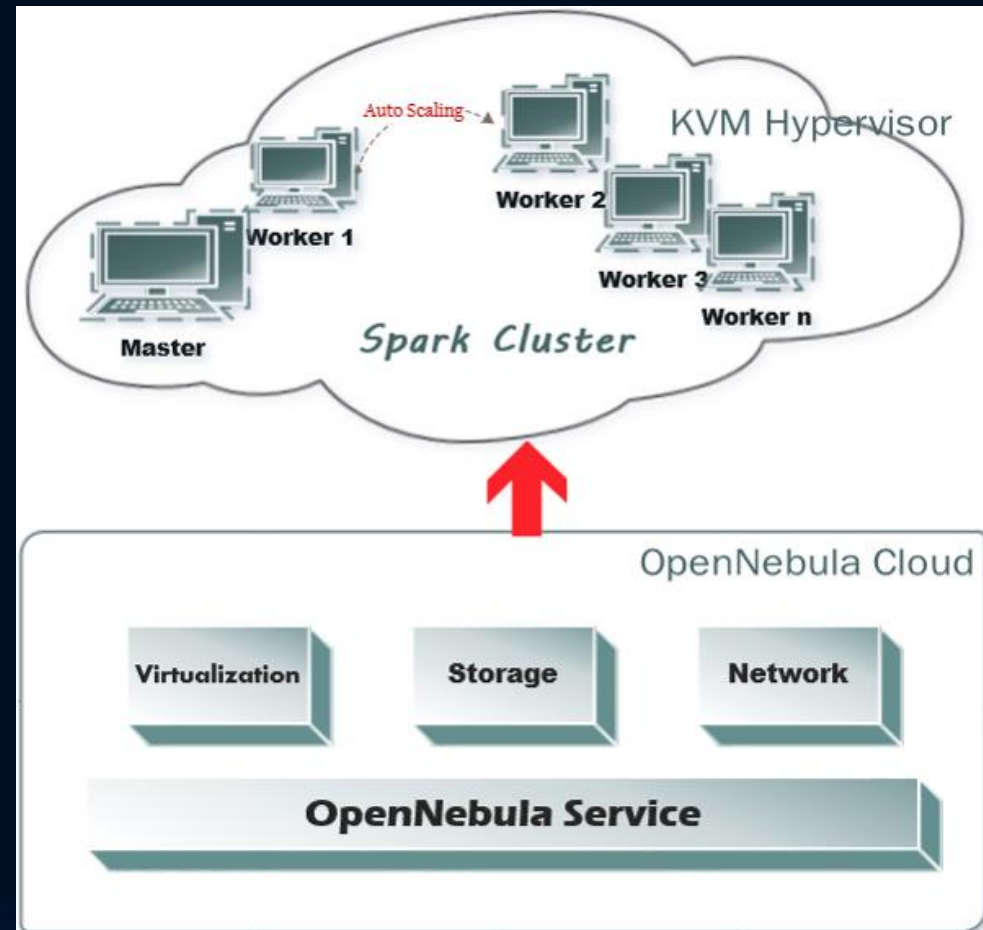


Auto-Scaling相關研究(2)

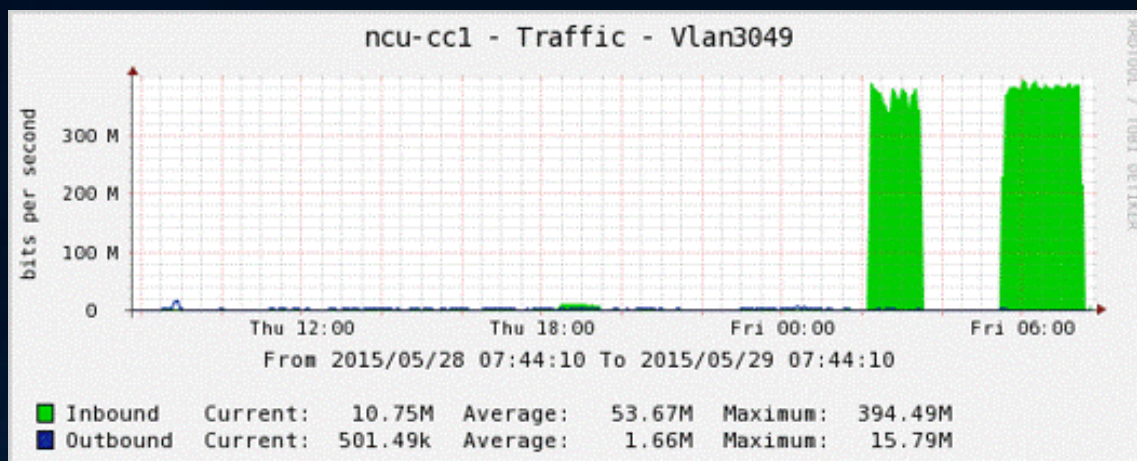
	Open Source Clouds	Auto-Scaling
1	OpenNebula	OneFlow service
2	OpenStack	Heat service
3	CloudStack	NetScaler
4	Eucalyptus	Auto scaling service

Auto-Scaling Spark異常流量偵測系統架構

- OpenNebula雲端運算平台，透過Front-End管理平台對hypervisor管理，系統可以建置、管理每一個VM的生命週期。
- 利用OneFlow 服務提供 auto-scaling。
- Spark Cluster 異常流量偵測系統使用KVM Hypervisor。



網路異常流量偵測(1)



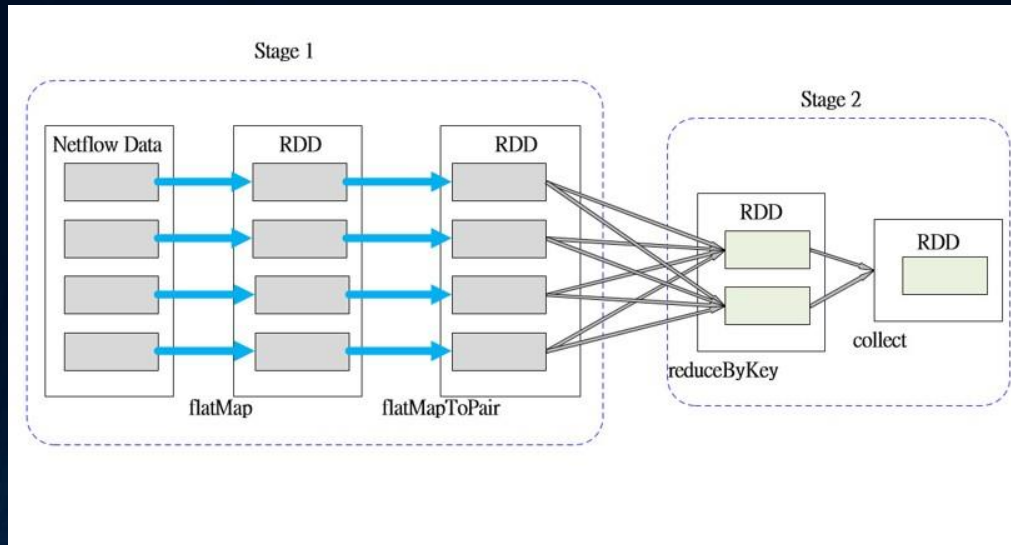
srcIP	dstIP	prot	srcPort	dstPort	octets	packets
220.123.30.252	140.115.222.75	17	24933	8322	321	1
180.153.97.14	140.115.1.31	17	53	59354	203	1
59.115.225.220	140.115.153.235	6	2227	12149	92	2
74.125.203.102	140.115.189.67	6	80	2453	20410	27
168.95.1.1	140.115.126.250	17	53	13080	179	1
222.59.54.193	140.115.41.95	6	3549	59574	314	5
74.125.23.138	140.115.236.202	6	443	2663	4759	11
74.125.203.138	140.115.65.206	6	443	33026	1335	4
123.223.24.109	140.115.56.160	6	27546	8265	52	1

網路異常流量偵測(2)

srcIP@prot	sum_in:sum_out:cnt_in:cnt_out:pkt_in:pkt_out
74.125.203.136@17	0:2836185:0:112:0:2958
74.125.203.136@6	0:1867105:0:413:0:3793
74.125.203.138@17	0:14560853:0:630:0:17070
74.125.203.138@6	0:22674792:0:2009:0:31098
74.125.203.139@17	0:17421876:0:625:0:18890
74.125.203.139@6	0:14348897:0:1945:0:24920
74.125.203.141@17	0:15936:0:6:0:21

- srcIP@prot(來源IP及協定)
- sum_in(輸入位元數)， sum_out(輸出位元數)
- cnt_in(輸入連接量)， cnt_out(輸出連接量)
- pkt_in(輸入封包量)， pkt_out(輸出封包量)

網路異常流量處理(3)



The screenshot shows the Spark UI interface for Job 0. The job is in a 'RUNNING' state with 1 active stage and 1 completed stage.

Details for Job 0

Status: RUNNING
Active Stages: 1
Completed Stages: 1

Active Stages (1)

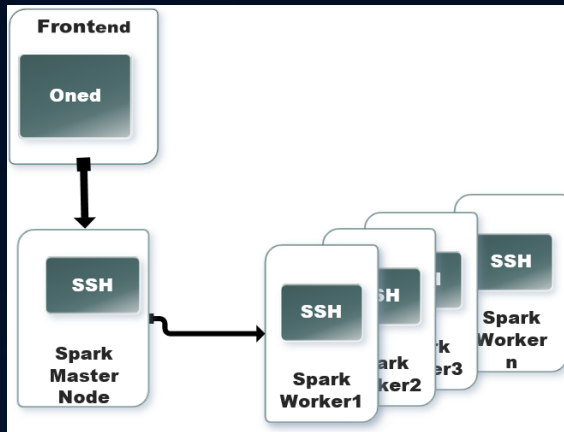
Stage Id	Description	Submitted	Duration	Tasks: Succeeded/Total	Input	Output	Shuffle Read	Shuffle Write
1	sortByKey at SparkPscan_min.java:138 (kill) +details	2016/08/19 06:00:36	4 s	2/12			24.0 MB	

Completed Stages (1)

Stage Id	Description	Submitted	Duration	Tasks: Succeeded/Total	Input	Output	Shuffle Read	Shuffle Write
0	flatMapToPair at SparkPscan_min.java:126 +details	2016/08/19 06:00:08	29 s	12/12	361.7 MB			144.1 MB

- Spark 處理流程第一階段：
透過 flatMap 及 flatMapToPair，將資料轉換為 key/value pairs 的 RDD。
- Spark 處理流程第二階段：
相同 key 值的 pairs 以 reduceByKey 轉為 counts RDD，再將符合異常網路流量特徵的 RDD 過濾出來。

Multi-tier Application 設計



- OneFlow 模組提供使用者定義、執行、管理 multi-tiered application。
- 各個虛擬機依照相依性進行部署。箭頭代表任務間的相依性，只有當 parent VM 開始執行後，child VM 才會開始被部署。

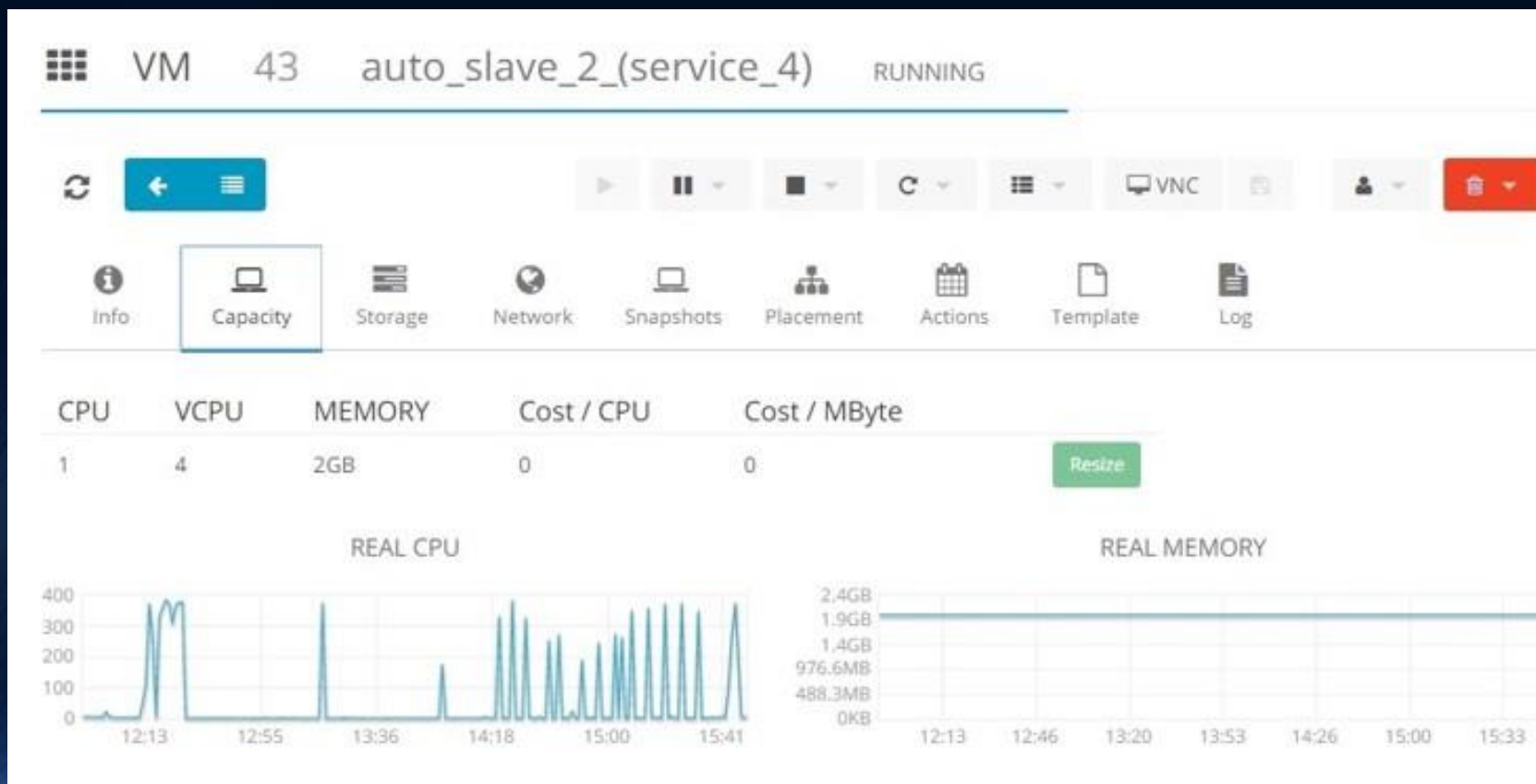
```
{
  "name": "Auto_Scaling",
  "deployment": "straight",
  "roles": [
    {
      "name": "auto_master",
      "vm_template": 4,
      "cardinality": 1
    },
    {
      "name": "auto_slave",
      "parents": [
        "auto_master"
      ],
      "cardinality": 1,
      "vm_template": 5,
      "min_vms": 1,
      "max_vms": 5,
    }
  ]
}
```

OneFlow Auto-Scaling設計(1)

- Auto-Scaling規則可依照系統服務性質定義，詳細分析系統特性及觀察系統執行效率。
- 本系統採用Spark in-memory 計算大量之資料，當系統執行大量運算時，CPU的使用率也到達高峰，因此規則定義依據CPU 使用率增加或減少計算節點(VM)。

```
"elasticity_policies": [  
  {  
    "expression": "CPU > 70",  
    "type": "CHANGE",  
    "adjust": 1,  
    "period_number": 4,  
    "period": 30  
  },  
  {  
    "expression": "CPU < 30",  
    "type": "CHANGE",  
    "adjust": -1,  
    "period_number": 6,  
    "period": 30  
  }  
]
```

OneFlow Auto-Scaling設計(2)



Contextualization 設計

- Contextualization 在新建立虛擬機時自動設定網路相關設定值，包括自動設定IP，定義虛擬機 HostName 及使用之網路介面及網段。
- 新建虛擬機與Spark主節點之間的自動連接，可以設定 SSH_PUBLIC_KEY，因此自動建立的計算節點可利用此參數而達到自動加入 Cluster。

The screenshot displays the OpenNebula web interface. On the left is a sidebar menu with categories like Dashboard, System, Virtual Resources, Infrastructure, Marketplace, OneFlow, Settings, and Support. The main area shows the configuration for a template named 'CentOS-6.5-slave0'. It includes tabs for 'Info' and 'Template', with the 'Template' tab selected. Below the tabs is a 'CONTEXT' section containing a list of configuration parameters and their values.

Parameter	Value
SET_HOSTNAME	slave\$VMID
SSH_PUBLIC_KEY	ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAu0/2vxx11D3NhHDLrW5QW5fZ4xEoLS9Mf9VyAdCj69mqI7Aefu7...
CPU	2.0
DISK	
IMAGE	auto_slave0_image
GRAPHICS	
LISTEN	0.0.0.0
TYPE	vnc
MEMORY	3072
NIC	
NETWORK	private1
OS	
ARCH	x86_64
VCPU	4

系統測試(1)

The screenshot displays the OpenNebula web interface. The left sidebar contains navigation menus for Dashboard, System, Virtual Resources, Infrastructure, Marketplace, OneFlow, and Support. The main content area shows the configuration for 'OneFlow - Service 4 Auto_Scaling_Experiment' in a 'RUNNING' state. It includes buttons for 'Shutdown' and 'Recover', and tabs for 'Info', 'Roles', and 'Log'. A 'Scale' button is visible. Below this, a table lists the roles and their cardinality:

Name	State	Cardinality	VM Template	Parents
auto_slave	RUNNING	1	5	auto_master
auto_master	RUNNING	1	4	-

Below the table, the 'Role - auto_master' section shows its configuration, including 'Shutdown action', 'Cooldown', 'Min VMs', and 'Max VMs'. The 'Virtual Machines' section at the bottom shows a list of VMs with columns for ID, Owner, Group, Name, Status, Host, and IPs.

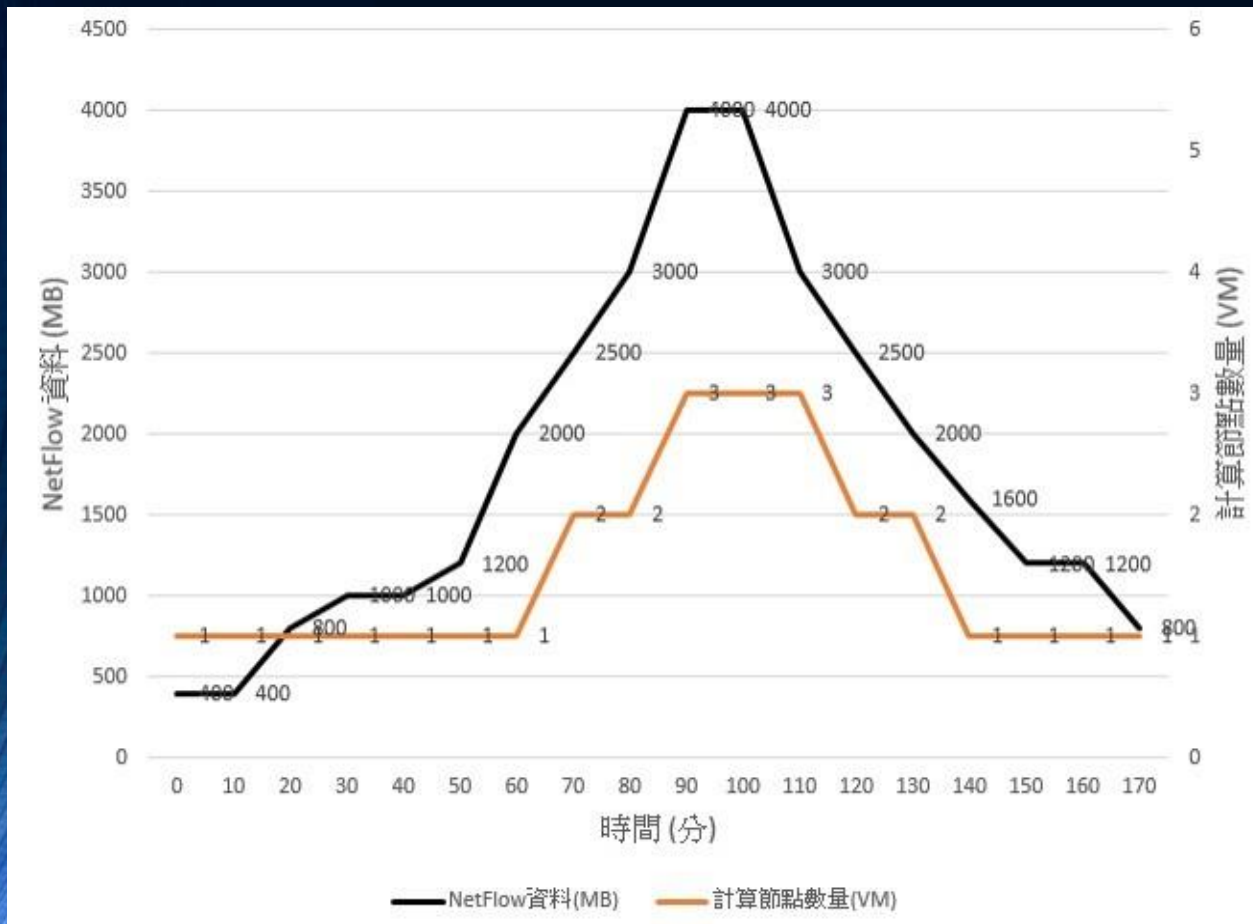
ID	Owner	Group	Name	Status	Host	IPs
40	oneadmin	oneadmin	auto_master_0(service_4)	RUNNING	163.25.251.65	192.168.122.26

➤ 初始配置1個主節點及1個計算節點。

➤ 初始資料量為每10分鐘400MB。

➤ 測試逐步提升資料量至每10分鐘4GB (初始量的10倍)。

系統測試(2)



➤ 資料量提升至每10分鐘2GB (初始量的5倍)，系統自動執行由1個計算節點增加為2個。

➤ 到達每10分鐘處理3.5GB 時，系統自動執行由2個計算節點增加為3個節點

```
10:06:55 18/08/2016 [I] Role auto_slave scaling up from 1 to 2 nodes
10:06:55 18/08/2016 [I] New state: SCALING
10:31:22 18/08/2016 [I] Role auto_slave scaling up from 2 to 3 nodes
10:31:22 18/08/2016 [I] New state: SCALING
10:57:51 18/08/2016 [I] Role auto_slave scaling down from 3 to 2 nodes
10:57:51 18/08/2016 [I] New state: SCALING
11:07:59 18/08/2016 [I] Role auto_slave scaling down from 2 to 1 nodes
11:07:59 18/08/2016 [I] New state: SCALING
```

結論

Auto-Scaling

- 使用OpenNebula 的Auto-Scaling 功能彈性調整系統資源。當流量異常增加時，系統自動增加計算節點。當流量減少時，也能自動減少計算節點。

Dynamic Resource Allocation

- Spark Cluster 透過Contextualization在新建立虛擬機時，自動設定相關設定值。並利用Spark Cluster 的動態資源配置，協調新計算節點加入Cluster共同處理。

Without any Human Operator Involvement

- 網管人員無需24小時人力介入，就可透過Auto-Scaling 的功能彈性調整 Cluster 計算資源。

The End

