N Cloud

The smartest syslog reporter in the world

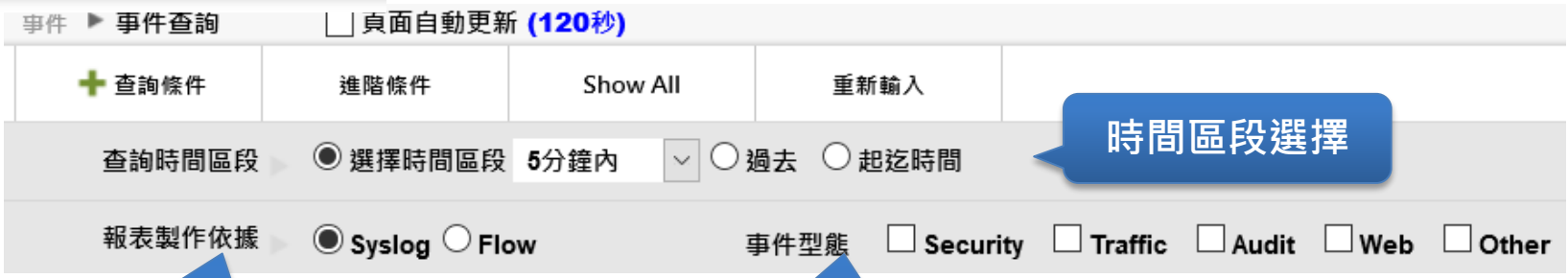
Training Material- 事件

Henry Yu
henry@npartnertech.com

N-Partner
Next Generation Technologies & Security of Network

事件 – 功能一覽

- 事件查詢
  - ✓ 查詢syslog事件和flow紀錄
  - ✓ 關聯
  - ✓ 支援 action
- 已儲存查詢條件
  - ✓ 儲存的查詢條件
  - ✓ 使用簡單



時間區段選擇

調整查詢依據為syslog事件或flow紀錄.
可以從[系統管理 >偏好設定]調整預設值

事件型態

進階條件

基本條件

事件 ▶ 事件查詢　頁面自[illegible]新 (120秒)

查詢條件 | 進階條件 | Show All

查詢時間區段 ◉ 選擇時間區段 5分鐘內 ○ 過[illegible]

◉ Syslog ○ Flow　事[illegible]rity ☐ Traffic ☐ Audit ☐ Web ☐ Other

- 設備
- 事件關鍵字
- IP過濾
- Port 過濾
- 動作
- 等級

- 應用服務
- 使用者名稱
- 時間範圍
- Policy ID
- Protocol
- 區域過濾
- 流量過濾
- 封包大小
- 主機名稱
- 寄件者
- 收件者
- MAC
- 介面過濾
- 路徑
- 作業系統
- 分類
- 狀態
- 無線基地台
- AP SSID
- Session ID


顯示所有條件
事件 ▶ 事件查詢
頁面自動更新 (120秒
查詢條件
進階條件
Show All
重新輸入
查詢時間區段
選擇時間區段
5分鐘內
過去
起迄時間
桃園市政府教育局
slog
Flow
affic
Audit
Web
Other
事件
事件查詢
已儲存查詢
支援邏輯判斷式, [+] 代表 or, [!] 代表not
事件關鍵字
查詢空事件
應用服務
使用者名稱
Policy ID
主機名稱
寄件者
收件者
MAC
URL, 檔案路徑
路徑
作業系統
分類
無線基地台
狀態
AP SSID
Session ID
查詢條件留空代表查詢any


顯示所有條件
事件 ▶ 事件查詢
頁面自動更新 (120秒
查詢條件
進階條件
Show All
重新輸入
點擊
7
查詢時間區段
選擇時間區段
5分鐘內
過去
起迄時間
Start Query
桃園市政府教育局
slog
Flow
事件型態
Security
Traffic
Audit
Web
Other
事件
事件查詢
已儲存查
使用者名稱
1
查詢指定IP
Protocol
N/A
2
點這
來源IP
目的IP
IP過濾
同時判定來源與目的IP
判定來源或目的IP
Port 過濾
同時判定來源與目的Port
判定來源或目的Port
區域過濾
同時判定來源與目的區域
判定來源或
介面過濾
同時判定流入與流出介面
判定流入或
流量過濾
流量(bytes)
>
封
封包大小
時間範圍
輸入IP
3
IP網段過濾條件
單一IP或網段:
IP 範圍:
IP名稱解析:
----------Network Domain----
3
使用名稱解析
[+] 代表新增,
[!] 代表排除
4
Home
[I]192.168.0.1
指定設備
6
設備
Global - Cisco6509-A
Global - Cisco6509-B
確定
取消
OK
5

時間區段

你可以從[系統管理>偏好設定]
改變欄位內容和順序

資料時間範圍: 2016/05/18 16:45:41 ~ 2016/05/19 16:01:10 總

事件	時間	次數	設備
%S d from console by systex on vty0 (127.0.0.3)	2016/05/19 16:01:10	1	Cisco 3750G aluster
%L ne protocol on Interface Vlan1, changed state to down	2016/05/19 15:57:16	1	Cisco 3750G aluster
%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down	2016/05/19 15:57:16	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured fro			50G aluster
%SYS-5-CONFIG_I: Configured fro			50G aluster
%SYS-5-CONFIG_I: Configured fro			50G aluster
%LINEPROTO-5-UPDOWN: Line pr			50G aluster
% -3-UPD I: Interface Giga			50G aluster
% terface Giga			50G aluster
% nterface Giga			50G aluster
%LINEPROTO-5-UPDOWN: Line pr			

事件內容

1 點擊事件

2 事件詳細內容

事件：	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/17, changed state to up		
時間：	2016/05/19 15:27:31	等級：	
動作：		次數：	1
來源IP：		目的IP：	
來源Port：	0	目的Port：	0
來源IP名稱解析：		目的IP名稱解析：	
來源Port解析：		目的Port解析：	
來源區域：		目的區域：	
Session：	0	Packets：	0
Bytes：	0	Protocol：	
來源使用者：		目的使用者：	
來源MAC：		目的MAC：	
NAT 來源IP：		NAT 目的IP：	
NAT 來源Port：	0	NAT 目的Port：	0
源IP所屬交換機/介面：		目的IP所屬交換機/介面：	
流入介面：		流出介面：	
主機名稱：		目的主機名稱：	
寄件者：		收件者：	
事件型態：	other	TCP Flag：	------
Policy ID：		Session ID：	
udit User：		狀態：	
設備：	Cisco 3750G aluster	路徑：	
參數：		應用服務：	
AP SSID：		無線基地台：	
作業系統：		分類：	

所有事件欄位

資料時間範圍: 2016/05/18 16:45:41 ~ 2016/05/19 16:01:10　總筆數: 122

事件	時間	次數	設備
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	2016/05/19 16:01:10	1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down	2016/05/19 15:57:16	1	Cisco 3750G aluster
%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down	2016/05/19 15:57:16	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by sys	2016/05/19 15:56:27	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by sys	2016/05/19 15:54:44	1	Cisco 3750G aluster
%S -CONFIG : Configured from console by systex on vty			
%L WN: Line pr			et2/0/17, cha
%L			
%LINK-3-UPDOWN: Interface Giga			o up
%LINK-3-UPDOWN: Interface Giga			to down
%LINEPROTO-5-UPDOWN: Line pr			et2/0/5, chan

1 在事件上點擊右鍵

2 Click here

- 分項統計
- 過濾條件加入此事件
- 過濾條件排除此事件
- 過濾條件加入來源IP
- 過濾條件排除來源IP
- 過濾條件加入目的IP
- 過濾條件排除目的IP
- 阻擋來源IP
- 阻擋目的IP

3 選擇欄位。N-Cloud 會統計所有事件的次數

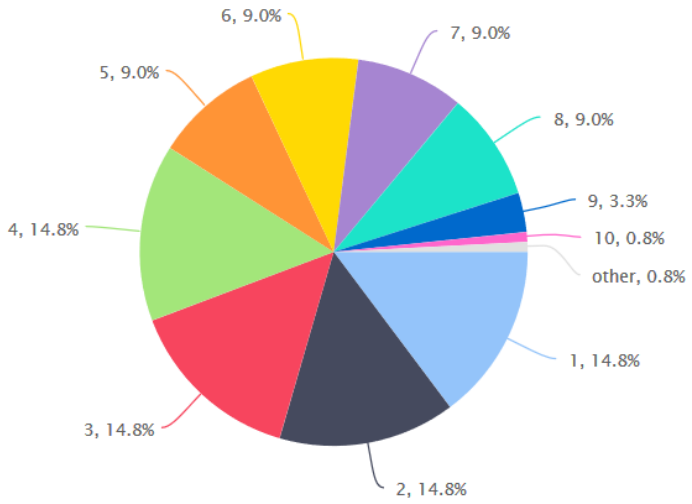
OK 4

從查詢結果產生TopN報表

資料時間範圍: 2016/05/18 16:45:41 ~ 2016/05/19 16:01:10　　總筆數: 122

事件	時間	次數	設備
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	2016/05/19 :01:10	1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down	2016/05 15:57:16	1	Cisco 3750G aluster
%LINK-5-CHANGED: Interface Vlan1, changed state to administratively down	2016 /19 15:57:16	1	Cisco 3750G aluster

Top 100 HitCount
2016/5/16 18:57 ~ 2016/5/23 18:57



總筆數: 11

NO	事件	Hit Count
1	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/5, changed state to up	18
2	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/17, changed state to up	18
3	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/17, changed state to down	18
4	%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/5, changed state to down	18
5	%LINK-3-UPDOWN: Interface GigabitEthernet2/0/17, changed state to up	11

1 匯出事件查詢結果

資料時間範圍: 2016/05/18 16:45:41 ~ 2016/05/19 16:01:10　總筆數: 122

事件		次數	設備
%SYS-5-CONFIG_I: Configured from console by systex on vty		1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan		1	Cisco 3750G aluster
%LINK-5-CHANGED: Interface Vlan1, changed state to adm		1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	201 :27	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	2016/05/19 1 4	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured	016/05/19 15:52:39	1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Li	016/05/19 15:27:31	1	Cisco 3750G aluster
%LINK-3-UPDOWN: Interface	016/05/19 15:27:31	1	Cisco 3750G aluster
%LINK-3-UPDOWN: Interface	016/05/19 15:27:31	1	Cisco 3750G aluster
%LINK-3-UPDOWN: Interface	016/05/19 15:27:29	1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Li	016/05/19 15:27:28	1	Cisco 3750G aluster

匯出報表

資料格式: ◉ PDF ○ CSV ○ XML

2 選擇輸出格式

確定　取消

OK

3

開啟中: Report_manual_2016_0516_1857.csv

您已決定開啟:

Report_manual_2016_0516_1857.csv

檔案類型: Micros cel 逗點分隔值檔案 (1.3 KB)

從: http://163.30 9

4 下載檔案

Firefo

Excel (預設)

◉ 儲存檔案 (S)

對此類檔案自動採用此處理方式。 (A)

確定　取消

資料時間範圍: 2016/05/18 16:45:41 ~ 2016/05/19 16:01:10　總筆數: 122

事件		次數	設備
%SYS-5-CONFIG_I: Configured from console by systex on		1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vla		1	Cisco 3750G aluster
%LINK-5-CHANGED: Interface Vlan1, changed state to ad		1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	9 15:56:27	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	:54:44	1	Cisco 3750G aluster
%SYS-5-CONFIG_I: Configured from console by systex on vty0 (127.0.0.3)	2016/05/19 15:52:39	1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/17, changed state to up	2016/05/19 15:27:31	1	Cisco 3750G aluster
%LINK-3-UPDOWN: Interface GigabitEthernet2/0/17, changed state to up	2016/05/19 15:27:31	1	Cisco 3750G aluster
%LINK-3-UPDOWN: Interface GigabitEthernet2/0/5, changed state to up	2016/05/19 15:27:31	1	Cisco 3750G aluster
%LINK-3-UPDOWN: Interface GigabitEthernet2/0/17, changed state to down	2016/05/19 15:27:29	1	Cisco 3750G aluster
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet2/0/5, changed state to up	2016/05/19 15:27:28	1	Cisco 3750G aluster


桃園市政府教育局
事件
事件查詢
已儲存查詢條件
搜尋已儲存條件名稱
事件 ▶ 已儲存查詢條件
已儲存條件名稱
事件種類
編輯查詢條件
查詢條件名稱
查詢依據
來源或目的為大陸地區
Flow
對內部連線狀態查詢
Flow
對外連線狀態查詢
Flow
網路設備事件查詢
Syslog
點擊名稱可用已存條件來查詢事件
刪除

Practice

N-Partner

Next Generation Technologies & Security of Network