網路硬體管理與監控

- Librenms學習筆記
- pfsense學習筆記

Librenms學習筆記

Librenms指令

檢查服務狀態

```
./validate.php
```

備註: 使用者需要是**librenms**

LibreNMS 告警模板

萬用模板

```
@if ($alert-> state == 0) ℹ恢復ℹ @endif
@if ($alert-> state == 1) ⚠告警⚠ @endif

標題: {{ $alert->title }}
規則: {{ $alert->name }}

設備名稱: {{ $alert->sysName }}
設備位址: {{ $alert->hostname }}
作業系統: {{ $alert->os }}
警示層級: {{ $alert->severity }}
警示時間: {{ $alert->timestamp }}
@if ($alert->state == 0)
經過時間: {{ $alert->elapsed }}
@endif
運行時間: {{ $alert->uptime_short }}
設備所在位置: {{ $alert->location }}
備註: {{ $alert->notes }}

@if ($alert->faults)
@foreach ($alert->faults as $key => $value)
服務: {{ $value['service_desc'] }}
類別: {{ $value['service_type'] }}
```

訊息: {{ $value['service_message'] }}

參數: {{ $value['service_param'] }}

@endforeach

@Endif

離線超過五分鐘（需搭萬用模板）

```
SELECT * FROM devices WHERE (devices.device_id = ?) AND (devices.status = 0 && (devices.disabled = 0 && devices.ignore = 0)) = 1 AND TIME_TO_SEC(timediff(now(), last_polled)) > 300;
```

設備重新啟動（需搭萬用模板）

```
SELECT * FROM devices WHERE (devices.device_id = ?) AND devices.uptime < 300 AND (devices.disabled = 0 && devices.ignore = 0) = 1
```

Windows 記憶體使用率過高

```
SELECT * FROM devices,mempools WHERE (devices.device_id = ? AND devices.device_id = mempools.device_id) AND mempools.mempool_perc > 90 AND devices.os LIKE '%Windows%' AND mempools.mempool_descr REGEXP "Physical.*"
```

@if ($alert-> state == 0) ℹ恢復ℹ @endif

@if ($alert-> state == 1) ⚠告警⚠ @endif

標題: {{ $alert->title }}

設備名稱: {{ $alert->sysName }}

設備位址: {{ $alert->hostname }}

警示嚴重: {{ $alert->severity }}

運行時間: {{ $alert->uptime_short }}

@if ($alert->state == 0)

經過時間: {{ $alert->elapsed }}

@endif

警示時間: {{ $alert->timestamp }}

設備所在位置: {{ $alert->location }}

備註: {{ $alert->notes }}

設備名稱: {{ $alert->sysName }}

@foreach ($alert->faults as $key => $value)

描述: {{ $value['mempool_descr'] }}

使用率: {{ $value['mempool_perc'] }}%

大小: {{ number_format(round(($value['mempool_total']/2**30),2,PHP_ROUND_HALF_DOWN),2) }} GB

已使用: {{ number_format(round(($value['mempool_used']/2**30),2,PHP_ROUND_HALF_DOWN),2) }} GB

未使用: {{ number_format(round(($value['mempool_free']/2**30),2,PHP_ROUND_HALF_DOWN),2) }} GB

@endforeach

Windows 磁碟空間不足

```
SELECT * FROM devices,storage WHERE (devices.device_id = ? AND devices.device_id = storage.device_id) AND storage.storage_perc > 90 AND devices.os LIKE '%Windows%'
```

```
@if ($alert-> state == 0) ℹ恢復ℹ @endif
@if ($alert-> state == 1) ⚠告警⚠ @endif

標題: {{ $alert->title }}

設備名稱: {{ $alert->sysName }}
設備位址: {{ $alert->hostname }}
警示層級: {{ $alert->severity }}
運行時間: {{ $alert->uptime_short }}
@if ($alert->state == 0)
經過時間: {{ $alert->elapsed }}
@endif
警示時間: {{ $alert->timestamp }}
設備所在位置: {{ $alert->location }}
備註: {{ $alert->notes }}

設備名稱: {{ $alert->sysName }}
@foreach ($alert->faults as $key => $value)
磁碟: {{ $value['storage_descr'] }}
容量: {{ number_format($value['storage_size']/1073741824,2) }} GB
使用率: {{ $value['storage_perc'] }}%
使用: {{ number_format($value['storage_used']/1073741824,2) }} GB
剩餘: {{ number_format($value['storage_free']/1073741824,2) }} GB

@endforeach
```

VMware ESXI 記憶體使用超過 85%

```
SELECT * FROM devices,mempools WHERE (devices.device_id = ? AND devices.device_id = mempools.device_id) AND mempools.mempool_perc > 85 AND devices.os LIKE '%VMware%' AND mempools.mempool_descr REGEXP "Real.*"
```

```
@if ($alert-> state == 0) ℹ恢復ℹ @endif
@if ($alert-> state == 1) ⚠告警⚠ @endif

標題: {{ $alert->title }}

設備名稱: {{ $alert->sysName }}
設備位址: {{ $alert->hostname }}
警示層級: {{ $alert->severity }}
運行時間: {{ $alert->uptime_short }}
@if ($alert->state == 0)
經過時間: {{ $alert->elapsed }}
@endif
警示時間: {{ $alert->timestamp }}
設備所在位置: {{ $alert->location }}
備註: {{ $alert->notes }}

設備名稱: {{ $alert->sysName }}
@foreach ($alert->faults as $key => $value)
描述: {{ $value['mempool_descr'] }}
使用率: {{ $value['mempool_perc'] }}%
大小: {{ number_format(round(($value['mempool_total']/2**30),2,PHP_ROUND_HALF_DOWN),2) }} GB
已使用: {{ number_format(round(($value['mempool_used']/2**30),2,PHP_ROUND_HALF_DOWN),2) }} GB
未使用: {{ number_format(round(($value['mempool_free']/2**30),2,PHP_ROUND_HALF_DOWN),2) }} GB
@endforeach
```

VMware ESXI 儲存空間不足

```
SELECT * FROM devices,storage WHERE (devices.device_id = ? AND devices.device_id = storage.device_id) AND storage.storage_perc > 90 AND devices.os LIKE '%VMware%'
```

```
@if ($alert-> state == 0) ℹ恢復ℹ @endif
@if ($alert-> state == 1) ⚠告警⚠ @endif

標題: {{ $alert->title }}

設備名稱: {{ $alert->sysName }}
```

設備位址: {{ $alert->hostname }}

警示層級: {{ $alert->severity }}

運行時間: {{ $alert->uptime_short }}

@if ($alert->state == 0)

經過時間: {{ $alert->elapsed }}

@endif

警示時間: {{ $alert->timestamp }}

設備所在位置: {{ $alert->location }}

備註: {{ $alert->notes }}

設備名稱: {{ $alert->sysName }}

@foreach ($alert->faults as $key => $value)

磁碟: {{ $value['storage_descr'] }}

容量: {{ number_format($value['storage_size']/1073741824,2) }} GB

使用率: {{ $value['storage_perc'] }}%

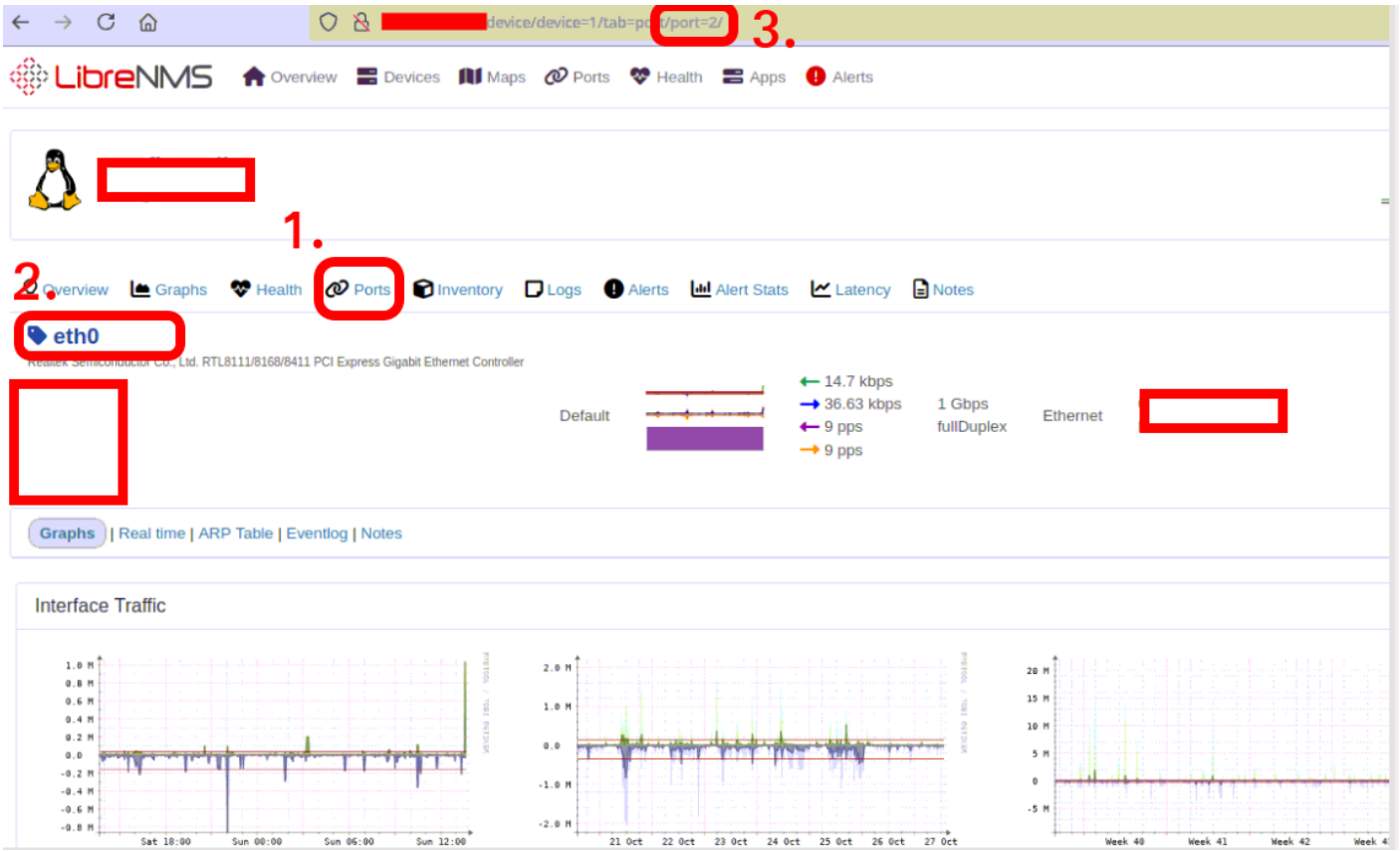
使用: {{ number_format($value['storage_used']/1073741824,2) }} GB

剩餘: {{ number_format($value['storage_free']/1073741824,2) }} GB

@endforeach

網路流量異常告警

先找到想要監控的Port ID, 可以去裝置→連接埠→點進去想要監控的埠→網址的位置就可以找到Port ID。



設定告警

ports.ifInOctets_rate 為流入的速率 (LibreNMS 已經先除以8了)

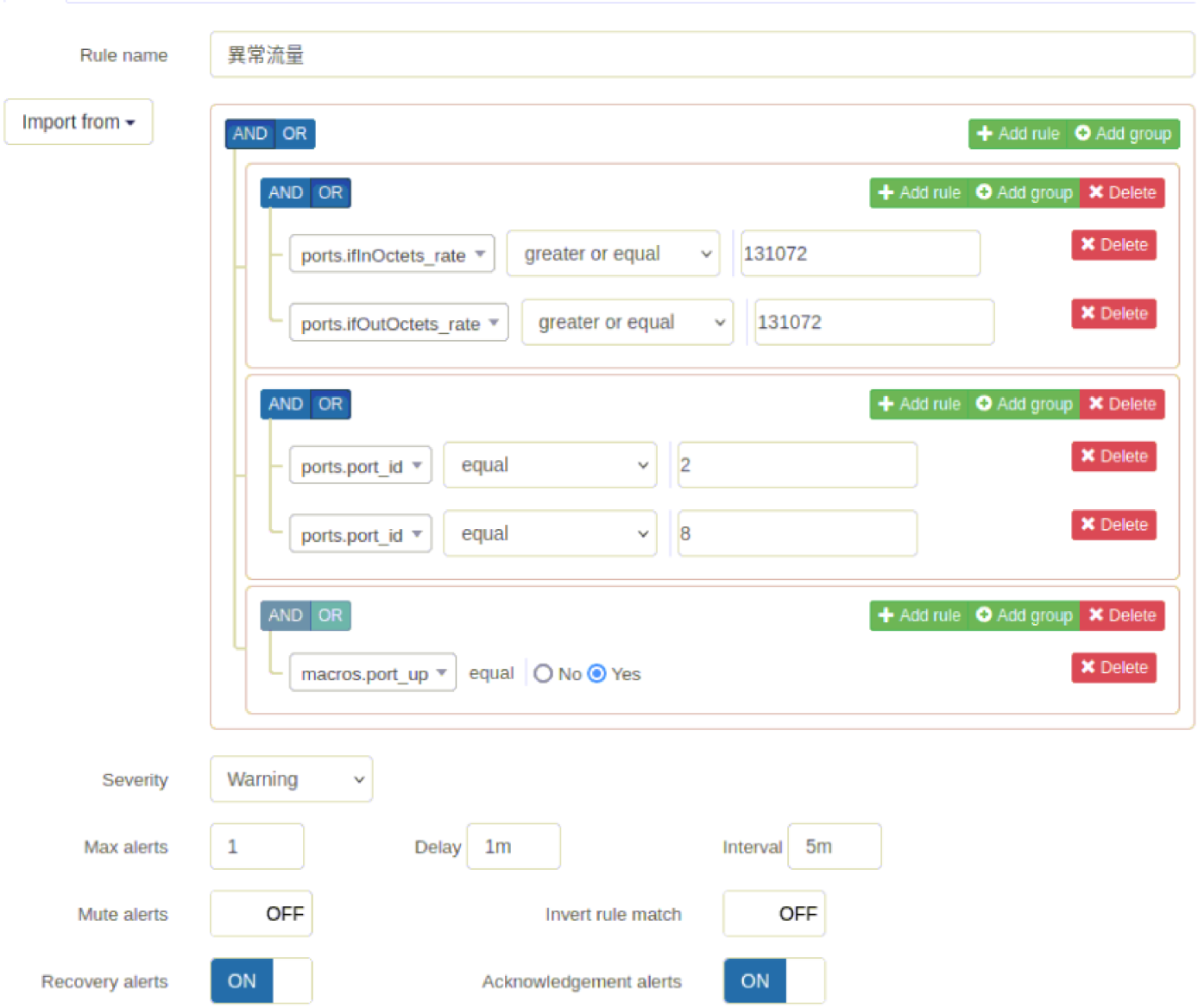
ports. ifOutOctets_rate 為流出速率 (LibreNMS 已經先除以8了)

速率計算方式 = X *1024* 1024 / 8

10M = 10 *1024* 1024 / 8 = 1310720

40M = 40 *1024* 1024 / 8 = 5242880

備註: 官方文件只***1000**而非**1024**



網路流量告警範本

設備名稱: {{ $alert->sysName }}

位置: {{ $alert->location }}

嚴重性: {{ $alert->severity }}

@if ($alert->state == 0) 已用時間: {{ $alert->elapsed }} @endif

時間戳: {{ $alert->timestamp }}

@foreach ($alert->faults as $key => $value)

網路埠位: {{ $value['ifName'] }}

描述: {{ $value['ifDescr'] }}

In 速率: {{ $value['ifInOctets_rate']*8/1048576 }} Mbit/s

Out 速率: {{ $value['ifOutOctets_rate']*8/1048576 }} Mbit/s

In 速率: {{ round(($value['ifInOctets_rate']*8/1048576),2,PHP_ROUND_HALF_DOWN) }} Mbit/s

```
Out 速率: {{ round(($value['ifOutOctets_rate']*8/1048576),2,PHP_ROUND_HALF_DOWN) }} Mbit/s
In 原始數值: {{ $value['ifInOctets_rate'] }}
Out 原始數值: {{ $value['ifOutOctets_rate'] }}


@endforeach
```

外掛程式

WeatherMap安裝

安裝php

```
suod apt insatll php-pear
```

安裝WeatherMap套件

```
cd /opt/librenms/html/plugins
git clone https://github.com/librenms-plugins/Weathermap.git
```

刷新權限

```
chown -R librenms:librenms Weathermap/
chmod 775 /opt/librenms/html/plugins/Weathermap/configs
```

備註:如果有使用SELinux需要再輸入下面指令

```
chcon -R -t httpd_cache_t Weathermap/
```

設定排程

```
vim /etc/cron.d/librenms
```

```
*/1 * * * * librenms /opt/librenms/html/plugins/Weathermap/map-poller.php >> /dev/null 2>&1
```

安裝Check_MK

```
cd /opt/
git clone https://github.com/librenms/librenms-agent.git
```

```
cd librenms-agent
```

linux	freebsd
`cp check_mk_agent /usr/bin/check_mk_agent`	`cp check_mk_agent_freebsd /usr/bin/check_mk_agent`

```
chmod +x /usr/bin/check_mk_agent
```

xinetd	systemd
`cp check_mk_xinetd /etc/xinetd.d/check_mk`	`cp check_mk@.service check_mk.socket /etc/systemd/system`

```
mkdir -p /usr/lib/check_mk_agent/plugins /usr/lib/check_mk_agent/local
```

```
cp /opt/librenms-agent/agent-local/* /usr/lib/check_mk_agent_local
```

```
chmod +x /usr/lib/check_mk_agent/local/$script
```

xinetd	systemd
`/etc/init.d/xinetd restart`	`systemctl enable check_mk.socket && systemctl start check_mk.socket`

最後開啟module的unix-agent就可以看到你設備更多資訊

參考文件

https://yushiryu.com/librenms-告警模板/#7_網路流量異常告警
https://hanelin.medium.com/監控軟體-librenms-服務應用-weathermap-d92073d64236

Libremns官方文件

pfsense□□□

□□qemu-guest

2. Manual installation

(a) Create the following 2 files

vim /etc/rc.conf.local

qemu_guest_agent_enable="YES"

qemu_guest_agent_flags="-d -v -l /var/log/qemu-ga.log"

#virtio_console_load="YES"

vim /usr/local/etc/rc.d/qemu-agent.sh

#!/bin/sh

sleep 3

service qemu-guest-agent start

(b) install qemu-guest-agent

i. pkg install -y qemu-guest-agent

ii. chmod +x /usr/local/etc/rc.d/qemu-agent.sh

(c) Change Proxmox settins

i. Shutdown pfsense

ii. Proxmox VM → Options → QEMU Guest Agent → Enable

iii. Restart VM