**VIETNAM CYBERSPACE SECURITY TECHNOLOGY**

**JSC**

**🙜🙞🕮🙜🙞**



**BÁO CÁO**

**CÀI ĐẶT SPLUNK THU THẬP LOG CẤU HÌNH CẢNH BÁO HỆ THỐNG WINDOW, LINUX VÀ THIẾT BỊ MẠNG**

NGƯỜI THỰC HIỆN : Mai Thành Thắng

Hà Nội - 10/2019

Mục Lục

[I. Thông tin chung 3](#_Toc24531759)

[II. Cấu hình nhận log cpu, ram, disk,… từ máy window 3](#_Toc24531760)

[1. App và add-on cần cấu hình 3](#_Toc24531761)

[2. Cấu hình trên splunk enterprise 3](#_Toc24531762)

[3. Cấu hình trên máy client window 8](#_Toc24531763)

[III. Cấu hình nhận log cpu, ram,process,… trên hệ thống Linux 8](#_Toc24531764)

[1. App và add-on cần cài đặt 8](#_Toc24531765)

[2. Cấu hình trên Splunk server 9](#_Toc24531766)

[a, App Nmon 9](#_Toc24531767)

[b, app và add-on linux: 10](#_Toc24531768)

[3. Cấu hình trên máy trạm 10](#_Toc24531769)

[IV. Cấu hình arlert, tạo report và dashboard 11](#_Toc24531770)

[1. Trên Windows 11](#_Toc24531771)

[2. Trên Linux 11](#_Toc24531772)

[2.1, Cấu hình alert, tạo report cho CPU trên Linux 11](#_Toc24531773)

[2.2. Dựng Dashboard: 16](#_Toc24531774)

[3. Trên thiết bị mạng 17](#_Toc24531775)

[a, Cấu hình trên thiết bị mạng 17](#_Toc24531776)

[b, Cấu hình trên Splunk server 19](#_Toc24531777)

[c, Tạo Cảnh báo , báo cáo và bảng điều khiển 23](#_Toc24531778)

[V. Cấu hình khác 24](#_Toc24531779)

# Thông tin chung

* Mô tả việc thu thập log trên hệ điều hành window và thiết bị mạng( Switch, fireware)
* Loại log thu thập:
  + Window: CPU, RAM, Disk
  + Thiết bi mạng: CPU, RAM, Bandwidth

# Cấu hình nhận log cpu, ram, disk,… từ máy window

## App và add-on cần cấu hình

* Tải gói cài đặt tại: <https://splunkbase.splunk.com/app/1680/#/overview> và <https://splunkbase.splunk.com/app/742/>
* Tiến hành cài đặt app và add-on:

+ Chọn 

+ Chọn **Install app from file.**

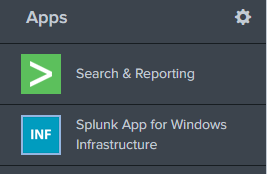
+ Chọn **Choose file** và chọn tập tin **splunk-app-for-windows-infrastructure\_152 .tgz**.

+ Bấm tích Upgrade app…..

+ Khởi động lại dịch vụ Splunk Enterprise .

Cài đặt tương tự với add-on: **splunk-add-on-for-microsoft-windows\_600.tgz**

Kết quả



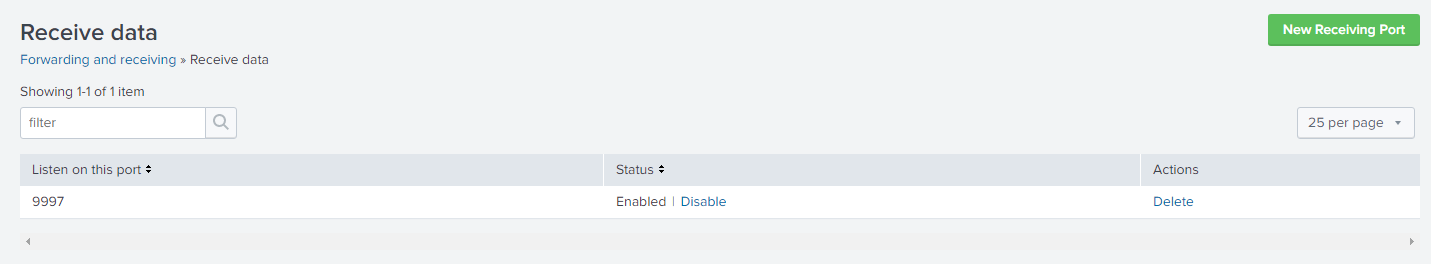


## Cấu hình trên splunk enterprise

Bước 1: Mở cổng nhận dữ liệu

* Trên giao diện GUI chọn **Settings > Forwarding and receiving**
* Ở mục **Receive data -> chọn Add new** -> nhập cổng **9997**

Kết quả



Bước 2: Copy thư mục **Splunk\_TA\_windows** vào **/opt/splunk/etc/deployment-apps**

* Tạo thư mục **local** trong Splunk\_TA\_windows và copy file **input.conf** từ thư mục **default** ở trong Splunk\_TA\_windows
* Chỉnh sửa nội dung:

[perfmon://CPU]

counters = % Processor Time; % User Time; % Privileged Time; Interrupts/sec; % DPC Time; % Interrupt Time; DPCs Queued/sec; DPC Rate; % Idle Time; % C1 Time; % C2 Time; % C3 Time; C1 Transitions/sec; C2 Transitions/sec; C3 Transitions/sec

disabled = 0

instances = \*

interval = 10

mode = single

object = Processor

useEnglishOnly=true

## Logical Disk

[perfmon://LogicalDisk]

counters = % Free Space; Free Megabytes; Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec

disabled = 0

instances = \*

interval = 10

mode = single

object = LogicalDisk

useEnglishOnly=true

## Physical Disk

[perfmon://PhysicalDisk]

counters = Current Disk Queue Length; % Disk Time; Avg. Disk Queue Length; % Disk Read Time; Avg. Disk Read Queue Length; % Disk Write Time; Avg. Disk Write Queue Length; Avg. Disk sec/Transfer; Avg. Disk sec/Read; Avg. Disk sec/Write; Disk Transfers/sec; Disk Reads/sec; Disk Writes/sec; Disk Bytes/sec; Disk Read Bytes/sec; Disk Write Bytes/sec; Avg. Disk Bytes/Transfer; Avg. Disk Bytes/Read; Avg. Disk Bytes/Write; % Idle Time; Split IO/Sec

disabled = 0

instances = \*

interval = 10

mode = single

object = PhysicalDisk

useEnglishOnly=true

index = perfmon

## Memory

[perfmon://Memory]

counters = Page Faults/sec; Available Bytes; Committed Bytes; Commit Limit; Write Copies/sec; Transition Faults/sec; Cache Faults/sec; Demand Zero Faults/sec; Pages/sec; Pages Input/sec; Page Reads/sec; Pages Output/sec; Pool Paged Bytes; Pool Nonpaged Bytes; Page Writes/sec; Pool Paged Allocs; Pool Nonpaged Allocs; Free System Page Table Entries; Cache Bytes; Cache Bytes Peak; Pool Paged Resident Bytes; System Code Total Bytes; System Code Resident Bytes; System Driver Total Bytes; System Driver Resident Bytes; System Cache Resident Bytes; % Committed Bytes In Use; Available KBytes; Available MBytes; Transition Pages RePurposed/sec; Free & Zero Page List Bytes; Modified Page List Bytes; Standby Cache Reserve Bytes; Standby Cache Normal Priority Bytes; Standby Cache Core Bytes; Long-Term Average Standby Cache Lifetime (s)

disabled = 0

interval = 10

mode = single

object = Memory

useEnglishOnly=true

index = perfmon

## Network

[perfmon://Network]

counters = Bytes Total/sec; Packets/sec; Packets Received/sec; Packets Sent/sec; Current Bandwidth; Bytes Received/sec; Packets Received Unicast/sec; Packets Received Non-Unicast/sec; Packets Received Discarded; Packets Received Errors; Packets Received Unknown; Bytes Sent/sec; Packets Sent Unicast/sec; Packets Sent Non-Unicast/sec; Packets Outbound Discarded; Packets Outbound Errors; Output Queue Length; Offloaded Connections; TCP Active RSC Connections; TCP RSC Coalesced Packets/sec; TCP RSC Exceptions/sec; TCP RSC Average Packet Size

disabled = 0

instances = \*

interval = 10

mode = single

object = Network Interface

useEnglishOnly=true

index = perfmon

## Process

[perfmon://Process]

counters = % Processor Time; % User Time; % Privileged Time; Virtual Bytes Peak; Virtual Bytes; Page Faults/sec; Working Set Peak; Working Set; Page File Bytes Peak; Page File Bytes; Private Bytes; Thread Count; Priority Base; Elapsed Time; ID Process; Creating Process ID; Pool Paged Bytes; Pool Nonpaged Bytes; Handle Count; IO Read Operations/sec; IO Write Operations/sec; IO Data Operations/sec; IO Other Operations/sec; IO Read Bytes/sec; IO Write Bytes/sec; IO Data Bytes/sec; IO Other Bytes/sec; Working Set - Private

disabled = 0

instances = \*

interval = 10

mode = single

object = Process

useEnglishOnly=true

index = perfmon

## ProcessInformation

[perfmon://ProcessorInformation]

counters = % Processor Time; Processor Frequency

disabled = 0

instances = \*

interval = 10

mode = single

object = Processor Information

useEnglishOnly=true

index = perfmon

## System

[perfmon://System]

counters = File Read Operations/sec; File Write Operations/sec; File Control Operations/sec; File Read Bytes/sec; File Write Bytes/sec; File Control Bytes/sec; Context Switches/sec; System Calls/sec; File Data Operations/sec; System Up Time; Processor Queue Length; Processes; Threads; Alignment Fixups/sec; Exception Dispatches/sec; Floating Emulations/sec; % Registry Quota In Use

disabled = 0

instances = \*

interval = 10

mode = single

object = System

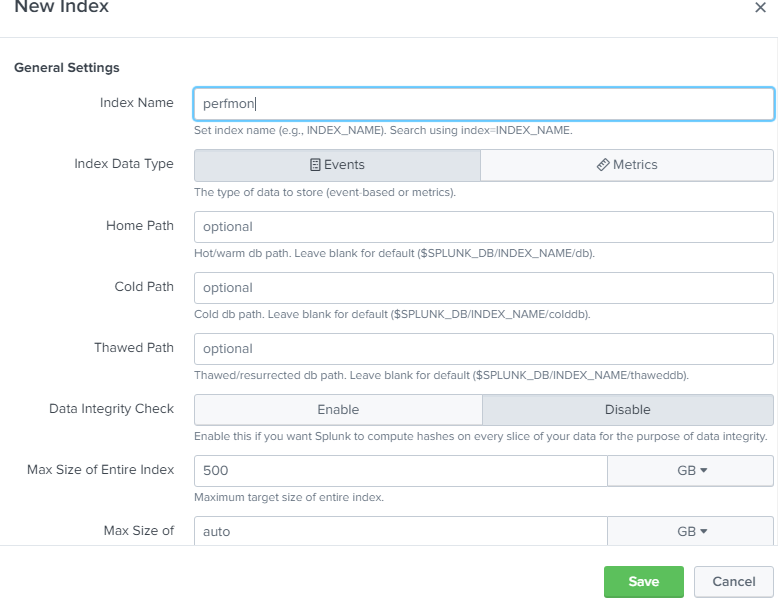
useEnglishOnly=true

index = perfmon

**Lưu ý:** Nếu có thay đổi khác index mặc định nên chỉnh sửa theo hướng dẫn link sau: [https://docs.splunk.com/Documentation/MSApp/1.5.2/MSInfra/DownloadandconfiguretheSplunkAdd-onforWindows#How\_to\_change\_the\_configuration\_files\_to\_handle\_custom\_indexes](https://docs.splunk.com/Documentation/MSApp/1.5.2/MSInfra/DownloadandconfiguretheSplunkAdd-onforWindows%23How_to_change_the_configuration_files_to_handle_custom_indexes)

Bước 3: Tạo Indexes nhận dữ liệu

* Trên giao diện GUI của Splunk chọn **Setting -> Indexes**, chọn **New Index**





Bước 4: Cấu hình **Forwarder Management**.

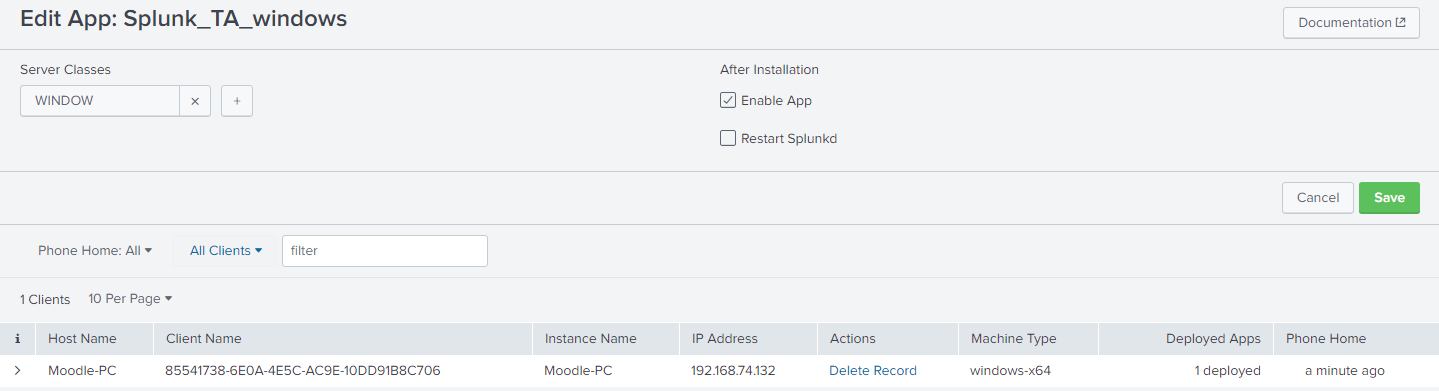
* Copy **Splunk\_TA\_windows** trong **/opt/splunk/etc/apps** sang thư mục **/opt/splunk/etc/deployment-apps**



* Cấp quyền thực thi cho thư mục **/opt/splunk/etc/deployment-apps/ Splunk\_TA\_windows/bin:**

chmod –R +x bin

* Vào giao diện GUI của Splunk chọn **Setting-**> **Forwarder Management** và chọn tab **Apps**.
* Chọn **Splunk\_TA\_windows** bấm **Edit**
* Bấm “+” chọn “Server Classes” bạn muốn triển khai
* Tích **Enable app** và bấm **Save**



* Restart lại Splunk

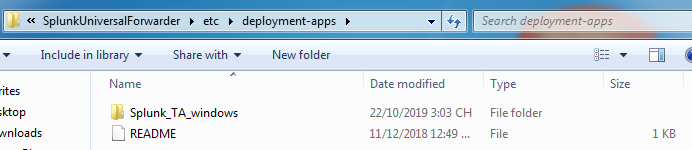
## Cấu hình trên máy client window

Bước 1: Cài Splunk forwarder

<https://docs.splunk.com/Documentation/Forwarder/7.3.2/Forwarder/InstallaWindowsuniversalforwarderfromaninstaller>

Bước 2: copy Splunk\_TA\_windows

* Dùng ứng dụng Bitvise để kết nối FTP với server chạy Splunk( lưu ý phải là quyền root – xem các cài đặt mục VI)
* Vào mục **/opt/splunk/etc/deployment-apps/** khéo thả thư mục Splunk\_TA\_windows ra máy trạm windows bạn muốn sử dụng để lấy log
* Copy Splunk\_TA\_windows vào đường dẫn **C:\ProgramFiles\Splunk\etc\deployment-apps\**



Bước 3: Khởi động lại Splunk

cd \Program Files\Splunk\bin

splunk.exe restart

# Cấu hình nhận log cpu, ram,process,… trên hệ thống Linux

## App và add-on cần cài đặt

* Truy cập trên web brower tải gói phần mềm sau:

App: <https://splunkbase.splunk.com/app/1753/>

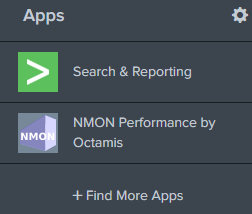
Add-on: <https://splunkbase.splunk.com/app/3248/>

* Hoặc bạn có thể cài đặt app và add-on:

App: <https://splunkbase.splunk.com/app/273/>

Add-on: <https://splunkbase.splunk.com/app/833/>

* Cài đặt app và add-on: (giống mục II phần 1)
* Kết quả





## Cấu hình trên Splunk server

### a, App Nmon

Bước 1: Mở cổng nhận dữ liệu từ máy trạm ( Giống mục II phần 2)

Bước 2: Tạo indexer mới :

* Tạo indexes mới tên: **nmon**

Bước 3: Cấu hình apps nmon

* Vào thư mục **nmon**  theo đường dẫn **$SplunkHome/ect/apps**
* Copy thư mục TA-nmon từ đường **$SplunkHome/ect/apps** vào thư mục **nmon/resourse/**
* Sửa phần **Application-level permissions** dung file **default.meta** trong thư mục **metadata** thành:

**# Application-level permissions**

**[]**

**#owner = admin**

**access = read : [ \* ], write : [ admin ]**

* Khởi động lại dịch vụ splunk

Bước 4: Cấu hình deployments-apps

* Copy thư mục **TA-nmon** từ thư mục **$SplunkHome/ect/apps** sang **$SplunkHome/ect/deployment-apps**
* Sửa nội dung file **default.meta**  trong thư mục **metadata** thành:

**# Application-level permissions**

**[]**

**access = read : [ \* ], write : [ admin ]**

**export = system**

* Khởi động lại deployments-apps: /bin/splunk reload deploy-server

Bước 5: Cấp quyền cho thư mục **dispatch/**

* Vào thư mục **$SplunkHome/var/run/splunk**

**chmod -R 777 dispatch/**

### b, app và add-on linux:

Bước 1: Tạo thư mục **local** trong **Splunk\_TA\_nix**

Bước 2:

* Copy file **input.conf** trong Splunk\_TA\_nix/default sang thư mục **local** vừa tạo
* Sửa nội dung file input:

Sửa “**disabled = 1 -> disable = 0” và “disabled = true -> disable = false”**

Dùng lệnh  **sed -i ‘**s/**disabled = 1 / disable = 0’ input.conf**

**sed -i ‘**s/**disabled = true / disable = false’ input.conf**

## Cấu hình trên máy trạm

* Cấu hình systat:

sudo apt-get update

sudo apt-get install sysstat

**Nếu dùng apps for linux**

* Thực hiện add monitor thư mục **/opt/splunkforwarder/var/log/splunk/audit.log** trong splunkforwarder:

**cd /opt/splunkforwarder/bin**

**./splunk add monintor /opt/splunkforwarder**

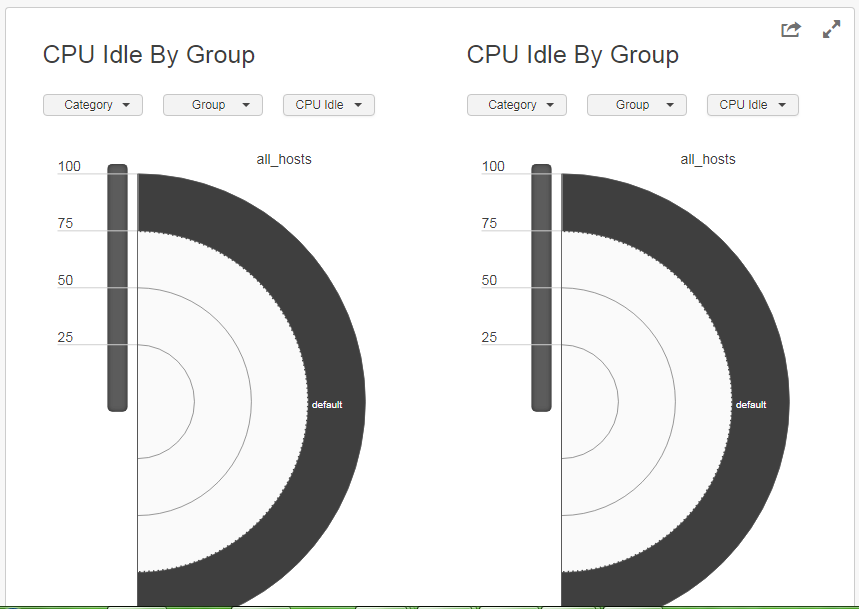
* Cấu hình indexs nhận dữ liệu

Vào thư mục **/opt/splunkforwarder/etc/apps/search/local** sửa tệp tin **input.conf**

**[monitor:///var/log/auth.log]**

**disabled = false**

**index = os**



# Cấu hình nhận log CPU, mem,log .… thiết bị mạng

## 1, Cấu hình trên thiết bị mạng:

service timestamps debug datetime msec localtime show-timezone year

service timestamps log datetime msec localtime show-timezone year

service sequence-numbers

logging trap informational

logging host <ip\_splunk\_sv> transport

**Bước 1: Bật lưu trữ và đăng nhập**

archive

log config

logging enable

logging size 200

notify syslog contenttype plaintext

hidekeys

login on-failure log

login on-success log

logging userinfo

**Bước 2: Cài đặt ghi log chung** :

logging event trunk-status global

logging event link-status global

**Bước 3: Cấu hình Log trên interface và SVI (Switch virtual interface)**

interface X

logging event trunk-status

logging event spanning-tree

logging event status

**Bước 4: Theo dõi MAC, STP logging, IP SLA, NTP, …:**

mac address-table notification mac-move

spanning-tree logging

ip sla logging traps

ip dhcp limit lease log

ip dhcp conflict logging

ip nat log translations syslog

xconnect logging pseudowire status

ntp logging

epm logging

**Bước 5: Logs ngưỡng ARP trên SVIs và interfaces:**

interface X

arp log threshold entries 2048

**Bước 6: Logging Trustsec ( dịch dụ bảo mật cisco):**

cts sxp log binding-changes

cts logging verbose

**Bước 7:**  **ACL Logging:**

ip access-list logging hash-generation

**Bước 8: CPU và memory log**:

process cpu threshold type total rising 80 interval 5

memory free low-watermark processor 20000

memory free low-watermark io 20000

**Bước 9:** **Cấu hình SNMP trên thiết bị:**

snmp-server enable trap

snmp-server community public ro  
snmp-server community private rw

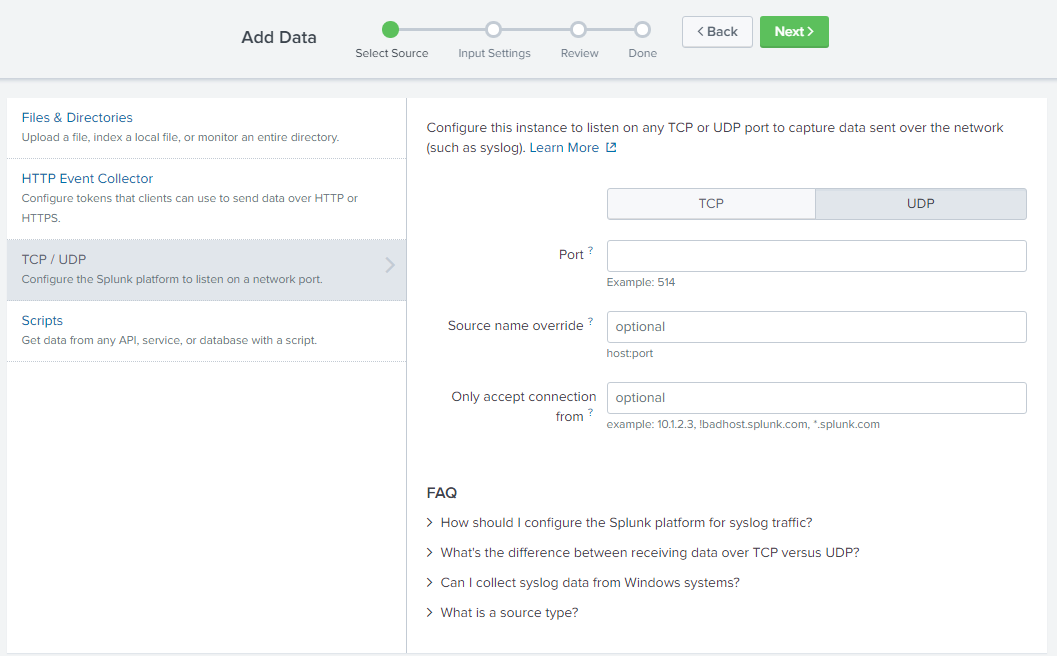
snmp-server host 192.168.74.131 traps public

## 2, Cấu hình trên Splunk server

* **Cấu hình SNMP server.**

**Bước 1:** Trên giao diện splunk-server chọn **setting->data input** ở mục **Local Input** chọn **UDP**

- Chọn **New local UDP**



Bước 2: cấu hình thông tin như bên dưới

Port: 514

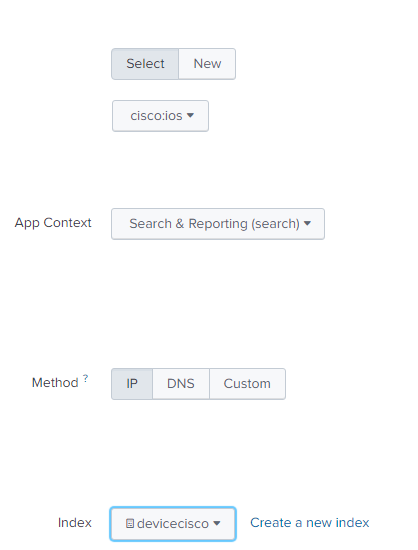
Only access connection from: hostname hoặc IP thiết bị mạng

Bấm next

Source type: cisco:ios

Host: IP

Index: Mặc định hoặc chọn theo index tự thiết lập



Bấm review -> submit để kiểm tra kết quả.

* Kiểm tra xem thông tin hệ thống đã nhận được thông tin từ phía thiết bị đẩy về chưa:  
  snmpwalk -v 2c -c public 192.168.74.150
* Kiểm tra OID của CPU, memory sửa dụng trên trang: <https://iphostmonitor.com/mib/oids/CISCO-PROCESS-MIB/>
* Lấy đúng thông tin CPU hay trạng thái mới nhất của hệ thống bằng app SNMP input:

+ Tải app SNMP input: <https://splunkbase.splunk.com/app/1537/>

+ Cài đặt app như bình thường.

* Cấu hình SNMP input trên giao diện của splunk:
* Vào đường dẫn : **Setting -> data input -> SNMP -> new** 

Phần more setting có thể cấu hình hoặc không cần cấu hình.

* Chỉnh sửa cấu hình trên bằng dòng lệnh:  
  + Vào mục **/opt/splunk/etc/apps/snmp\_ta** tạo một thư mục **local** trong thư mục đó tạo một file **input.conf** và chỉnh sửa nội dung ví dụ như sau:

#######

###CPU memory

#####

[snmp://CPU\_memory]

communitystring = public

destination = 192.168.74.150

do\_bulk\_get = 0

do\_get\_subtree = 0

host = router\_audit

index = devicecisco

ipv6 = 0

object\_names = .1.3.6.1.4.1.9.9.109.1.1.1.1.12.2,.1.3.6.1.4.1.9.9.109.1.1.1.1.13.2

port = 161

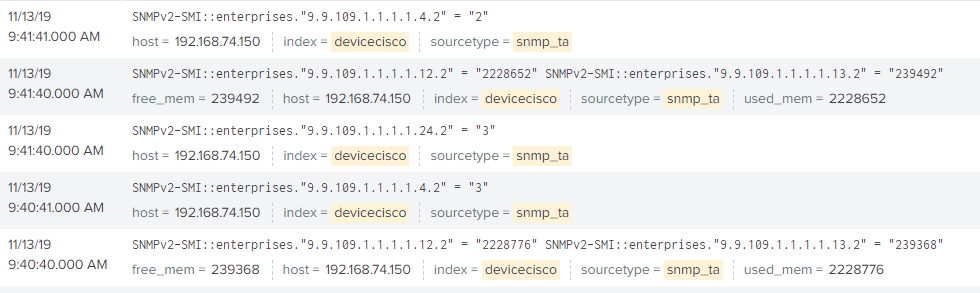
snmp\_mode = attributes

snmp\_version = 2C

sourcetype = snmp\_ta

split\_bulk\_output = 0

* Kết quả: khi thực hiện searh: index="devicecisco" sourcetype=snmp\_ta



# Cấu hình cảnh báo, tạo báo cáo và bảng điều kiển

## Trên Linux

### 1.1, Cấu hình alert, tạo report cho CPU trên Linux

Yêu cầu:

CPU usage: 50% total CPU usage 80% total usage

**Check one process/total cores usage**: 100% total cores 150% total CPU core

Load Average: Load of 0.75 of one core x total cores Load of 1.00 of one core x total cores

Memory usage: 50% total usage 80% total usage

**Filesystem usage:** 80% total usage 90% total usage(df.sh)

Swap usage: 80% total usage 90% total usage

**Zombie process:** 5 dead processed 10 dead processes

**Ping:** Not OK Not OK( ping.sh)

**Number of user concurrent login**: 10 users 15 users (sshd.sh)

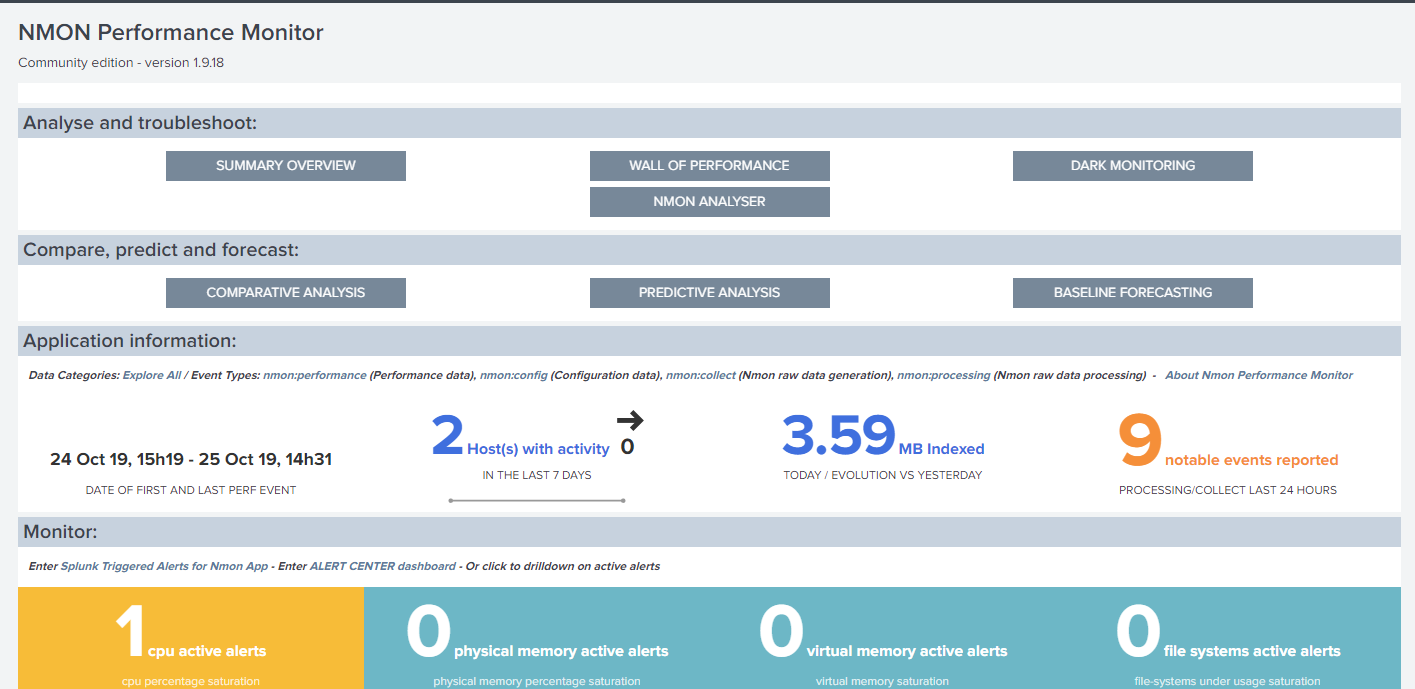
**Total processes**: > 200 processes > 300 processes(ps aux | wc -l)

**Check FC adtapter status**: 1 port offline 2 port offline (lspci | grep -i emulex)

#### 2.1.1,Dùng app TA-Nmon

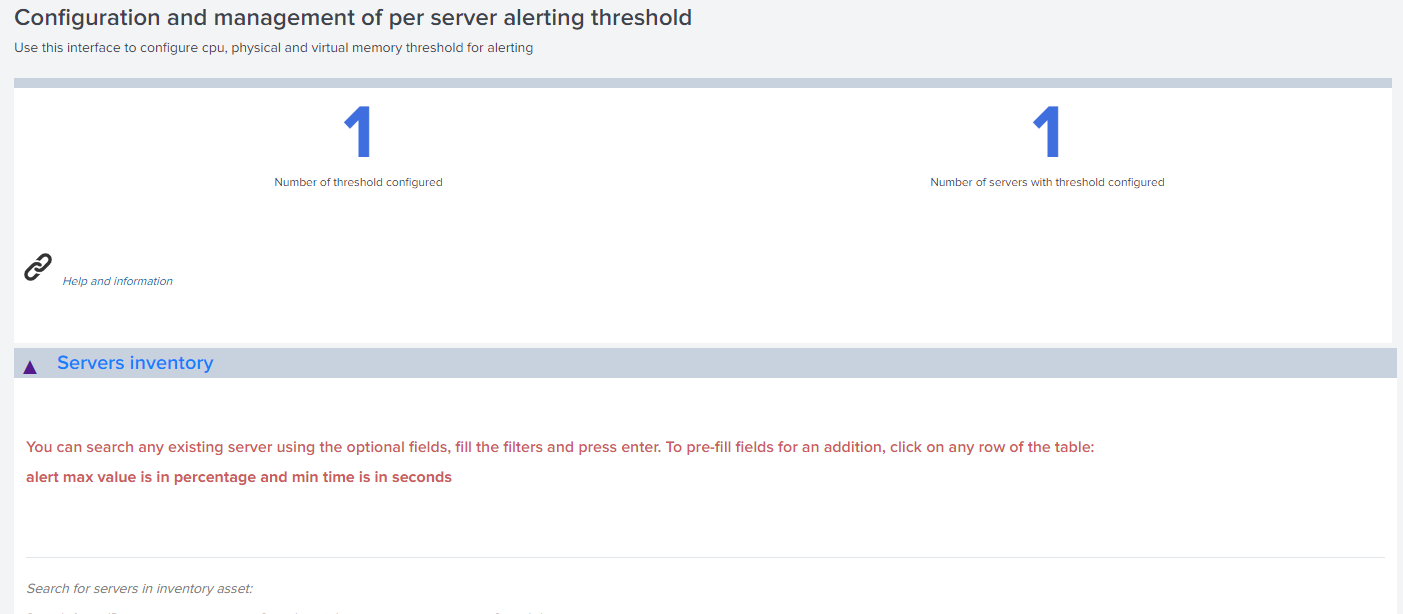
Cách 1:

* Trên giao diện web của Splunk vào ứng dụng **NMOM Performen**

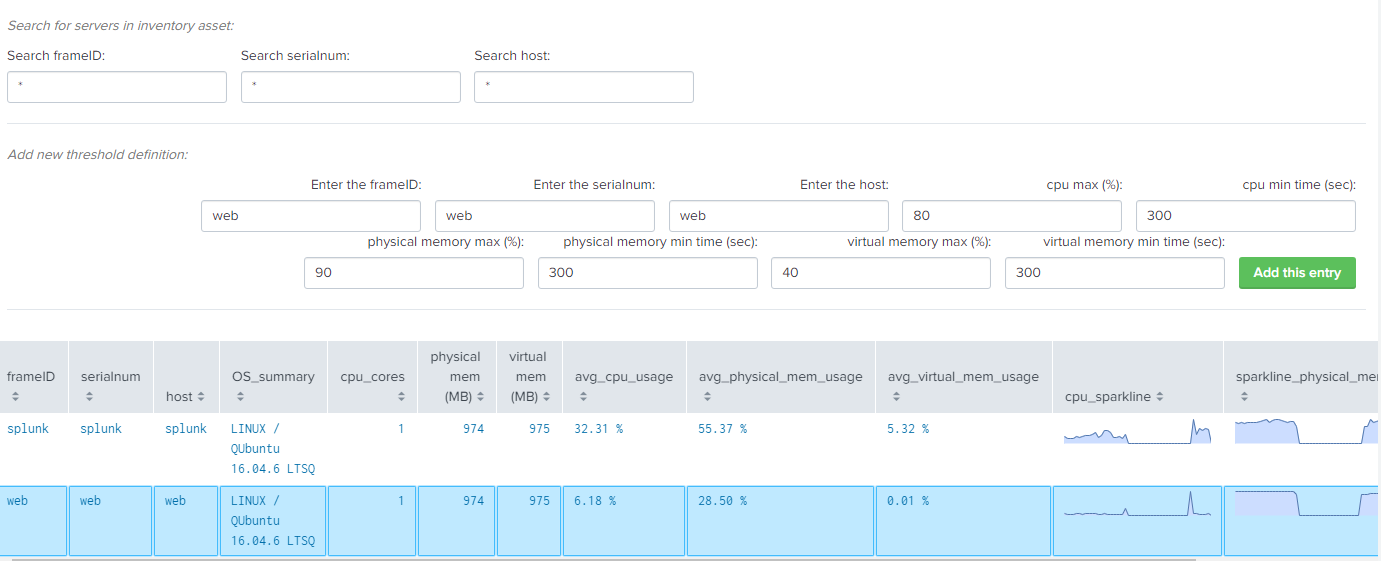


* Thiết lập ngưỡng cảnh bảo trên giao diện đối với CPU

Chọn **Setting (thanh menu app góc bên trái) -> Alert threshold configure -> Server alerting threshold for cpu & memory**



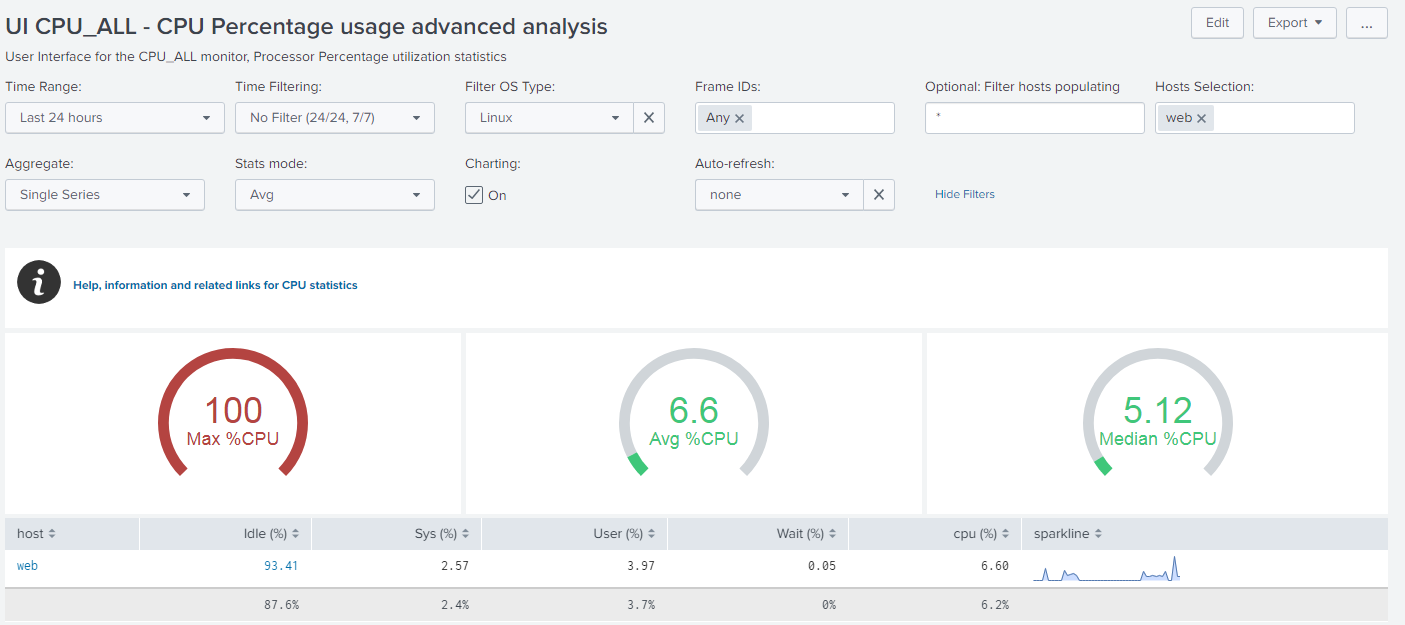
* Chọn **Server Inventory** sẽ hiện thị ra server hệ thống bạn muốn đặt cảnh báo
* Chọn server để đặt cảnh báo cấu hình ngưỡng cảnh bảo khi Cpu hay memory vượt quá max. Sau đó bấm **Add this entry**



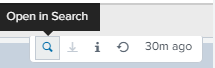
* Có thể thay đổi thông số cấu hình ở trên tại **Threshold table - currently configured alerting thresholds per server**

Cách 2:

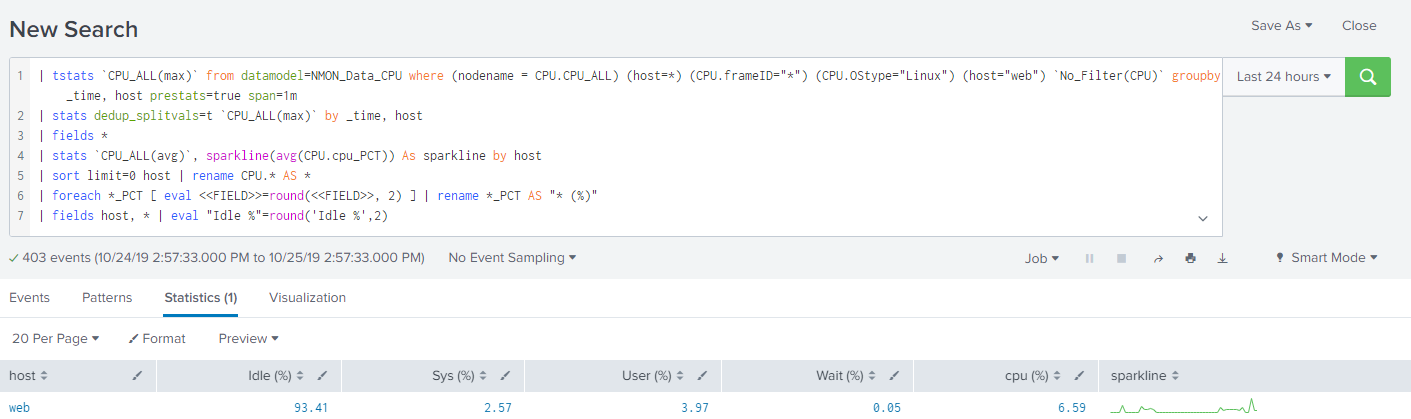
* Trên giao diện ứng dụng **NMON Performan** chọn **LINUX -> CPU -> CPU\_ALL >>…**



* Trên đó là thông tin tổng quan về trạng thái CPU của hệ thống linux
* Trên bảng hiển thị thông tin các server đang kết nối tới app NMON bạn chọn server để xem bằng cách như dưới hình.

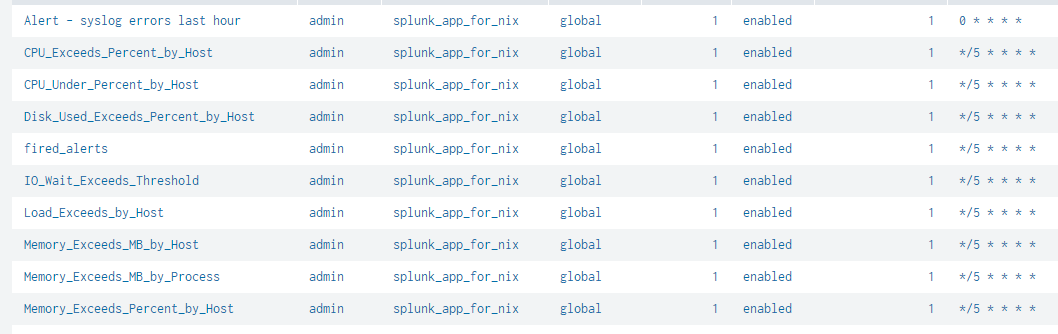
****

* Kết quả



* Tạo alret cảnh báo ngưỡng CPU ở trang trên bạn chọn **Save as -> Alert**

**Kết quả**



#### Nếu dùng app for Linux

Trên app **search and report** thực hiện search để thiết lập cảnh báo:

**CPU:** host=web sourcetype = cpu

| table \_time cpu\_user\_percent

| chart latest(cpu\_user\_percent)

**Memory**: host=web sourcetype="vmstat" memFreePct="\*" memUsedPct="\*"

| table \_time memFreePct,memUsedPct

| chart latest(memUsedPct)

**LoadAvg**: source="vmstat" host =web loadAvg1mi="\*"

| table \_time loadAvg1mi

| rename loadAvg1mi as "Load average CPU"

| chart latest("Load average CPU") **Swap**: source="vmstat" swapUsedPct > "1"

**Check one process/total cores usage**: host = web source = top pctCPU="\*"

| table \_time pctCPU

| chart latest(pctCPU)

**Filesystem usage**: source="df" host =web

| table \_time storage\_used\_percent storage\_free\_percent

| rename storage\_used\_percent as "FileSystem\_use\_pct" , storage\_free\_percent as "FileSystem\_free\_pct"

| timechart latest("FileSystem\_use\_pct") latest("FileSystem\_free\_pct") **Number of user concurrent login**: source=who host = web | stats distinct\_count(USERNAME)

**Total processes**: source=ps host = web

| table process

| stats distinct\_count

**Ping: (** Tạo extract file gán trường )  
index=os sourcetype="pingstatus"

| stats count by status  
**Zoombie**: source = ps host = web | stats count by S

**Lưu ý:**

**latest(** value) lấy giá trị mới nhất.

Phần kiểm tra gói tin ping . Ta phải viết một đoạn shell kiểm tra ping và gửi thông báo

Ví dụ: ping.sh

#!/bin/bash

ip=<ip máy trạm>

while [ 1 ]; do

ping -c 1 $ip 1> /dev/null

result=$?

if [ $result == "1" ]; then

echo FAIL on `date`. Doing tracert!

fi

if [ $result == "0" ]; then

echo SUCCEED on `date`

fi

sleep .4

done

* Sau khi có file này xong cấu hình thêm trong phần input.conf

[script://./bin/ping.sh]

interval = 600

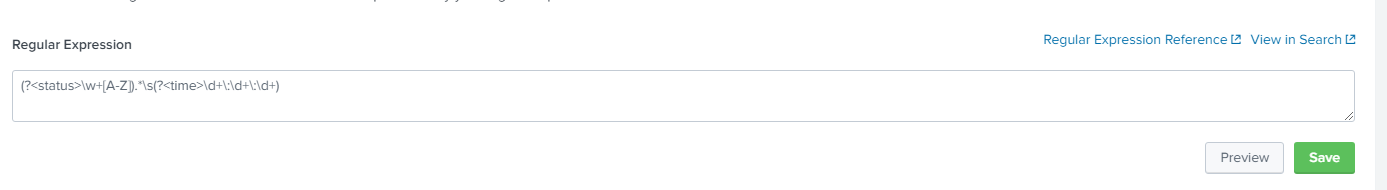
sourcetype = pingstatus

source = pingstatus

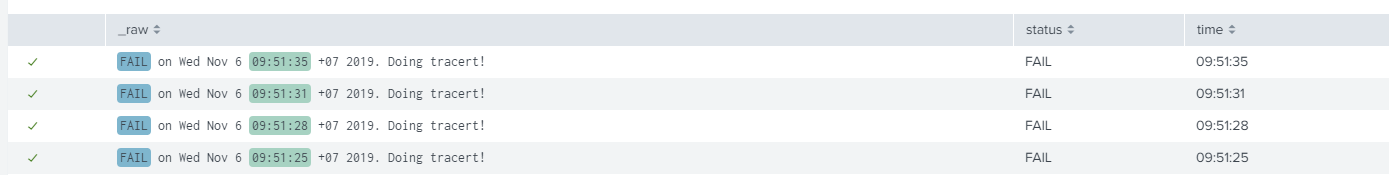
disabled = 0

index = os

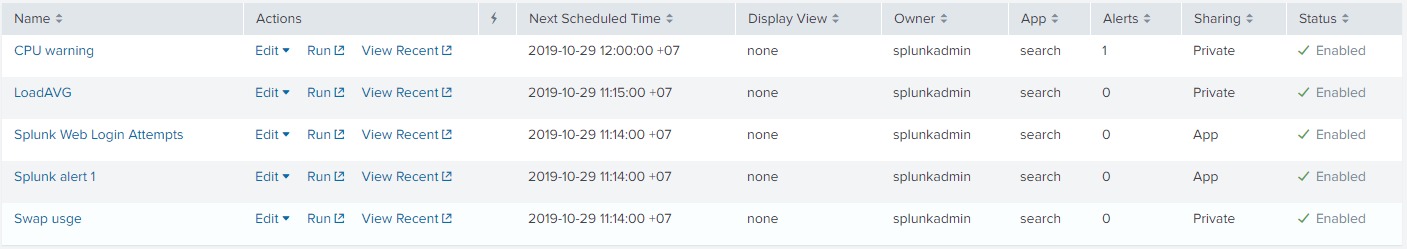
* Ở trên app **search and report** khi ta lấy thông tin của nguồn pingstatus, cần chuẩn hóa dữ liệu. Dữ liệu trạng thái trả về là FAIL hoặc SUCCEED.
* Chọn “Extract new Fields” . Chọn **I prefer to write the regular expression myself** tức là sẽ thiết lập biểu tức chính quy tốt nhất để tạo ra trường theo ý của mình, ở đây



* Chọn Save để lưu lại trường này và thực hiện kiểm tra theo cấu trúc tìm kiếm pingstatus ở trên

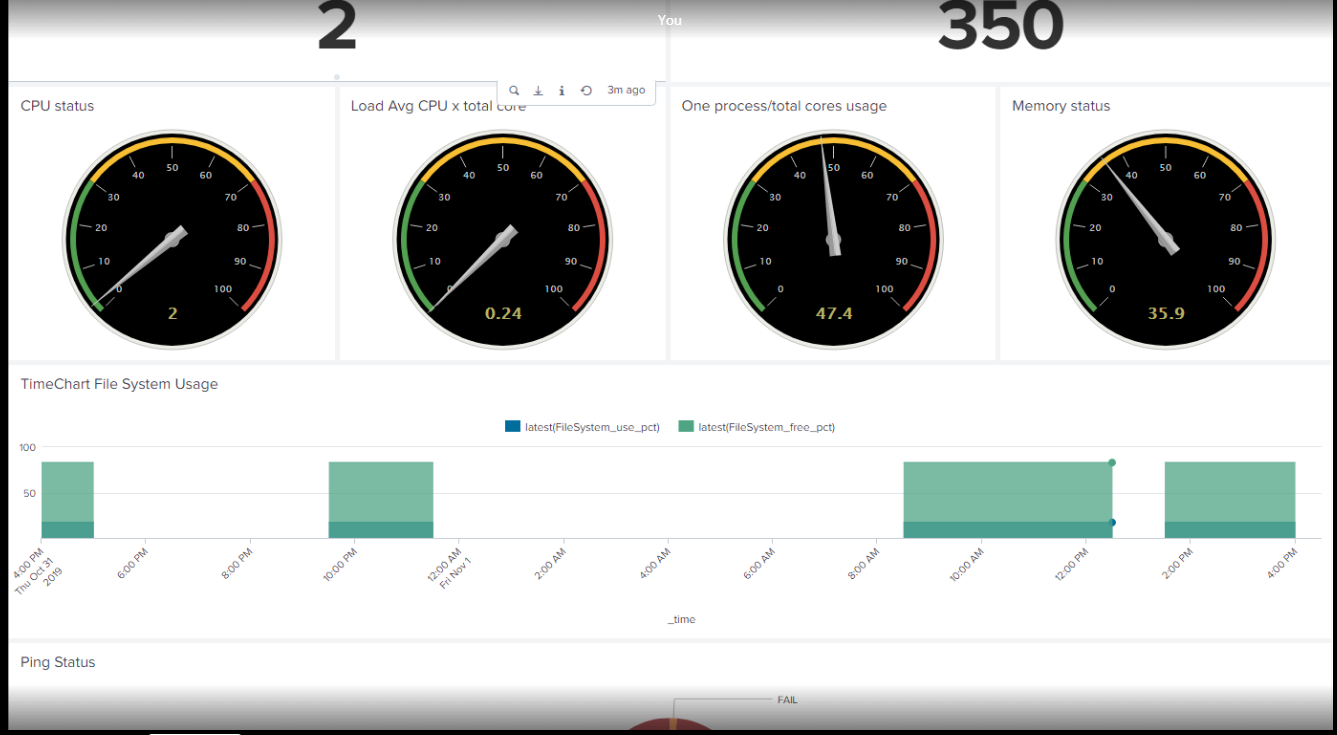


**Kết quả ví dụ:**



### Xây dựng bảng điều khiển theo dõi:

* Từ việc tạo cảnh báo và báo cáo ở trên add nó vào một dashboard



## Trên thiết bị mạng

### Tạo cảnh báo:

**Cảnh báo mức nguy hiểm đối với thiết bị:**

index="audit\_device\_cisco" sourcetype=snmp\_ta mem\_used=\*

| eval Total = mem\_used + mem\_free

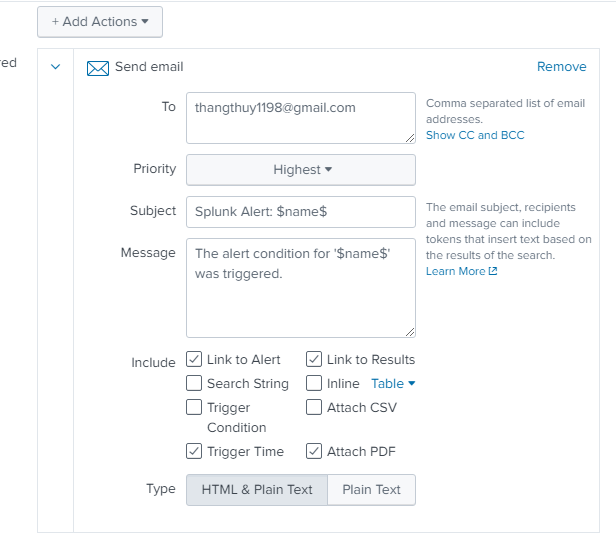
| eval Pct\_used = (mem\_used/Total)\*100

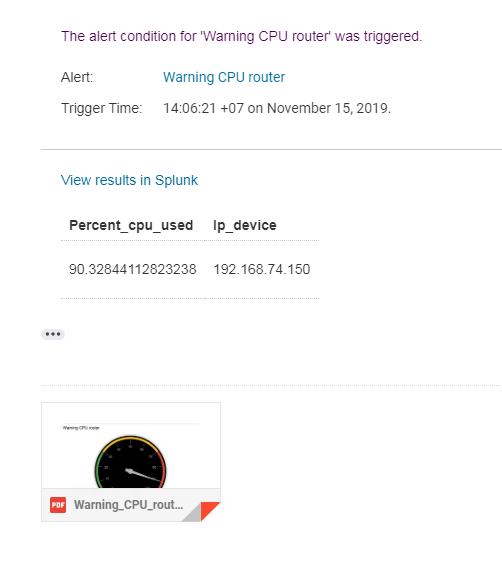
| where Pct\_used > 90

| chart latest(Pct\_used) as "Percent\_cpu\_used" latest(host) as Ip\_device

**Tạo alert gửi mail**

* Cấu hình email. Setting -> Server setting -> email setting





### **Tạo bảng báo cáo và điều khiển**:

**Memory\_cpu\_use:**  
index="devicecisco" sourcetype=snmp\_ta used\_mem=\*

| table used\_mem free\_mem

| eval total = used\_mem + free\_mem

| eval Pct\_used= (used\_mem/total)\*100

| chart latest(Pct\_used)

**CPUTotal\_used\_1min**

index="devicecisco" OID="enterprises.\"9.9.109.1.1.1.1.24.2\""

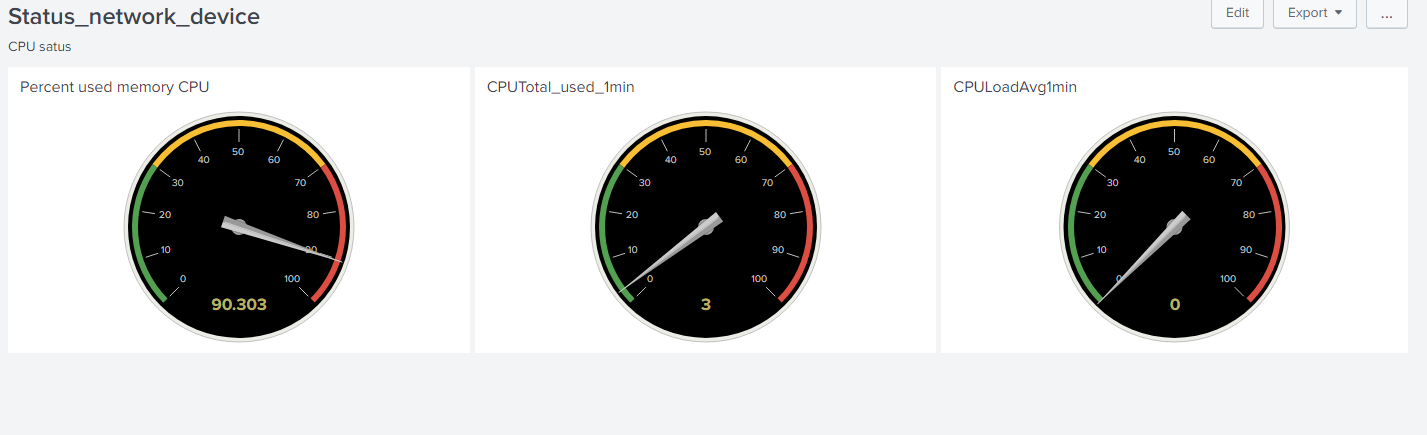
| chart latest(value)

**CPULoadAvg1min**

index="devicecisco" OID="enterprises.\"9.9.109.1.1.1.1.4.2\""

| chart latest(value)

Kết quả:



# Cấu hình khác

* **Cấu hình dịch vụ SSH trên server Splunk**

sudo apt update

sudo apt install openssh-server

Vào chỉnh sửa file theo đường dẫn **/etc/ssh/**

nano sshd\_config

* **Cấu hình login với quyền root**

Tìm đoạn và sửa thành nội dung sau:

# Authentication:

LoginGraceTime 120

PermitRootLogin yes

StrictModes yes

Khởi động lại dịch vụ SSH:

sudo service ssh

Đổi mật khẩu user root

sudo passwd root

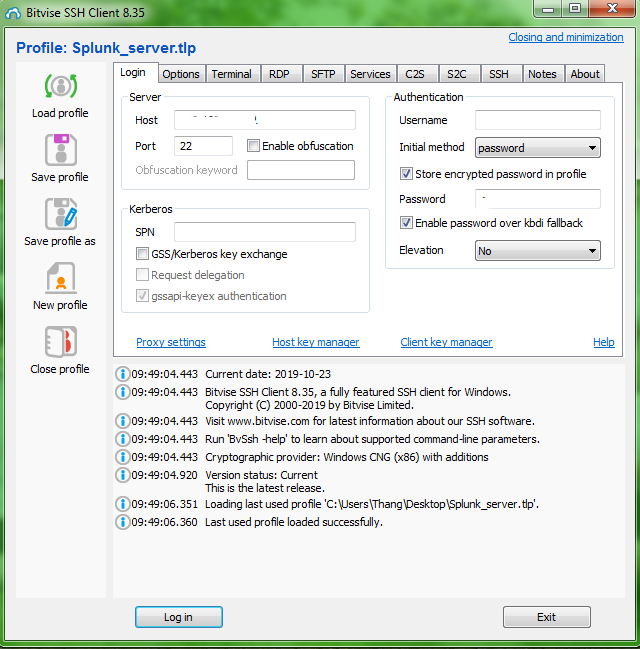
* **Cài đặt phần mềm bitvise-SSH client:**

Truy cập vào link để tài gói cài đặt: <https://www.bitvise.com/ssh-client-download>

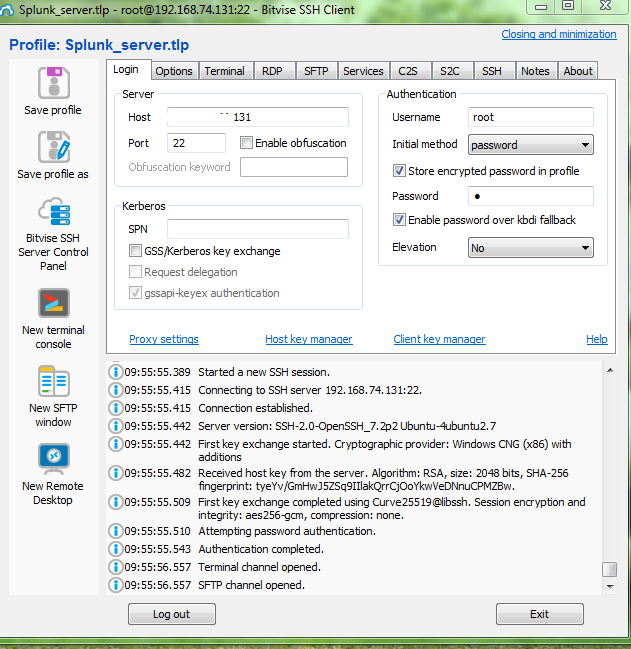
Sau khi tải về tiến hành kích đúp và gói BvSshClient-Inst



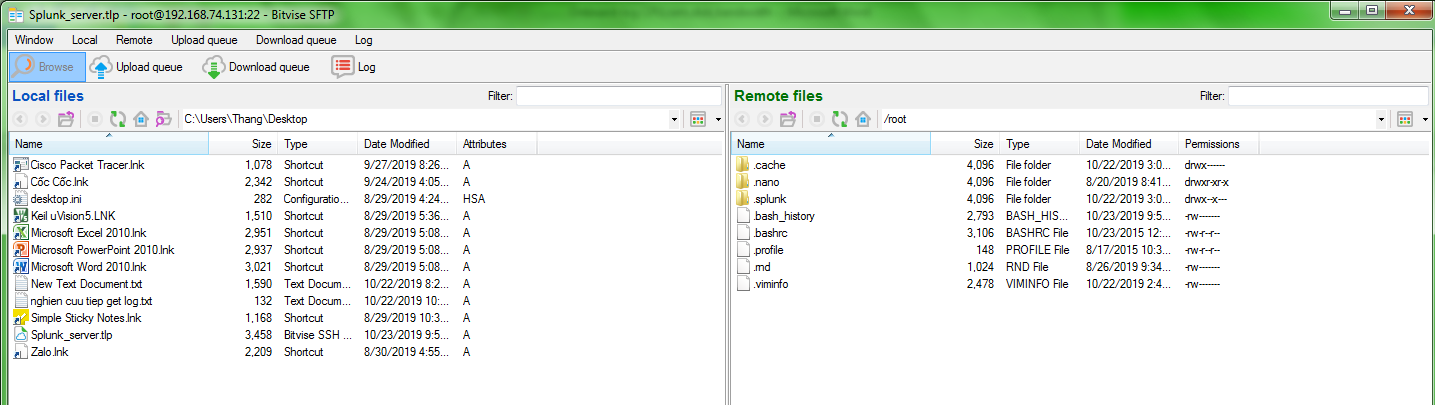
Đây là giao diện của phần mềm Bitvise ssh.

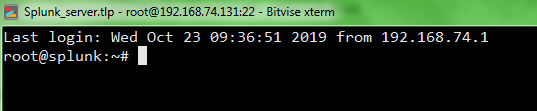


* Điền thông tin đăng nhập của root và vào bấm loggin hiển thị như hình



* Lúc này dịch vị FTP và remote desktop sẽ khởi chạy và có thể lấy file từ sever splunk ra bên ngoài và có thể quản trị bằng giao diện dòng lệnh



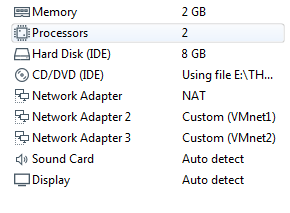


**Cài đặt một môi trường Router ciso trên VMW\_15**

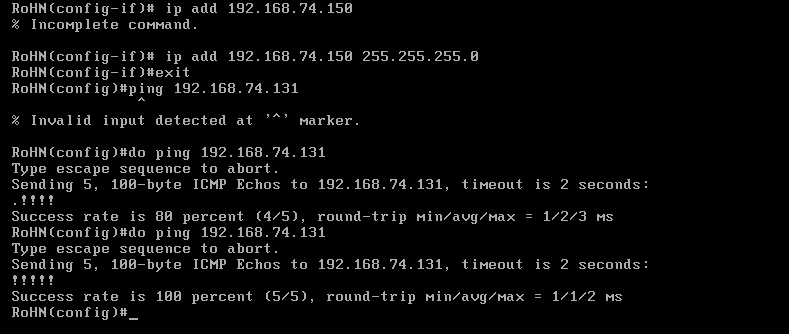
* Tải đĩa hoặc file Ova link: <https://www.rogerperkin.co.uk/ccie/ccie-virtual-rack-csr-1000v-routers/>

**Nếu là đĩa :**

* Thực hiện các bước tạo máy ảo như bình thường đến mục chọn loại máy chọn “ Other”
* Add thêm 2 card mạng cho máy ảo này.



* Chọn đĩa vừa tải về nạp vào và chạy
* Trong cấu hình nhớ bấm 1 phím bất kỳ để chạy đến bước cuối cùng nó có cảnh báo thì bấm OK
* Kế quả



**Nếu là file ova thì cứ bấm vào và import vào thư mục nào đó đợi nó khởi tạo thành công ta được kết quả như trên.**

Cấu hình SSH-router  
- Cấu hình ip cho cổng NAT- mặc định G0

* Cấu hình domain: ip domain-name
* Cấu hình user và pass đăng nhập:
* Cấu hình sshv2: ip ssh version 2
* Cấu hình key-SSH:

crypto key generate rsa ( để giá trị 1024)

* Cấu hình đăng nhập từ xa:

line vty 0 4

login local

transport ssh