Installation

Step 1: App installation

Install the Cisco Networks (cisco_ios) App on your search head
Install the Cisco Networks Add-on (TA-cisco_ios) on your search head AND indexers/heavy forwarders
Syslog input: Enable a UDP input with a custom port number on your Splunk forwarder or Splunk indexer. Set the sourcetype to **cisco:ios** or **syslog**

Step 2: Configure your Cisco devices

Cisco IOS

This includes all IOS variants. Not all commands are supported on all models

Basic logging and timestamping

```
service timestamps debug datetime msec localtime show-timezone yearservice timestamps log datetime msec localtime show-timezone yearservice sequence-numberslogging trap informationallogging host [YOUR SYSLOG/SPLUNK SERVER IP] transport udp port [YOUR UDP PORT]
```

Enable change auditing

```
archive log config logging enable logging size 200 notify syslog contenttype plaintext hidekeys!login on-failure loglogin on-success loglogging userinfo!ip ssh logging events
```

Monitor interface changes

General

```
logging event trunk-status globallogging event link-status global
```

Interface level

```
logging event trunk-statuslogging event spanning-treelogging event status
```

MAC move notifications, STP logging, IP SLA logging etc.

```
mac address-table notification mac-movespanning-tree loggingip sla logging trapsip dhcp limit lease logip dhcp conflict loggingip nat log translations syslogxconnect logging pseudowire statusntp loggingepm logging
```

For DHCP utilization logging on your devices, do this for each pool

```
utilization mark high 80 log
```

For ARP threshold logging, do this on your SVIs and IP interfaces

```
arp log threshold entries 2048
```

TrustSec

If you are using Cisco TrustSec, add the following cts sxp log binding-changescts logging verbose

ACL logging

General

Remember to add the **log** or **log-input** keyword to your access list entries if you want to enable access list logging

Access list correlation tags

```
ip access-list logging hash-generation
```

CPU and Memory Utilization logging

This generates CPU and memory notifications. CPU notifications if the CPU has been over 80% for more than 5 seconds. Memory if there is less than 20000KB. process cpu threshold type total rising 80 interval 5memory free low-watermark processor 20000memory free low-watermark io 20000

NX-OS

This includes all NX-OS variants. Not all commands are supported on all models

Basic logging and timestamping

```
logging logfile messages 6logging server [YOUR SYSLOG/SPLUNK SERVER IP] 6 use-vrf [YOUR MGMT VRF]logging timestamp millisecondslogging monitor 6no logging rate-limit
```

Enable change auditing

This feature is not supported on the NX-OS platform

Monitor interface changes

General

```
logging message interface type ethernet descriptionlogging event link-status defaultlogging event trunk-status default
```

Interface level

```
logging event port link-statuslogging event port trunk-status
```

MAC move notifications, STP logging, IP SLA logging etc.

```
mac address-table notification mac-moventp logging
```

ACL logging

General

Remember to add the **log** or **log-input** keyword to your access list entries if you want to enable access list logging

NX-OS ACL logging

```
logging level acllog 6acllog match-log-level 6logging logfile messages 6
```

Step 3: Configure Device to Role mappings (OPTIONAL)

If you'd like to be able to select devices in the dashboards using their roles, i.e. Core, Edge, PE etc, install the app Splunk App for Lookup File Editing and open up the **cisco_networks_host_to_role.csv** lookup file to add your own device to role mappings.

This process could also be automated from your CMDB by replacing the content of the aforementioned lookup file. Make sure you keep the original headers.

Troubleshooting

Not seeing authentication results?

Results from wired 802.1x (DOT1X) authentications are sent with severity "level 7 - debugging". To correct this configure logging trap debugging on your device. Take extra precautions in actual debugging situations as "debug all" will result in a huge increase in events forwarded to your Splunk servers.

Not seeing Route Monitoring results?

In order to monitor Route Changes via Syslog, the following EEM applet must be configured on your routers: event manager applet route-table-monitor event routing network 0.0.0.0/0 ge 1 action 0.5 set msg "Route changed: Type: $_routing_type, Network: $_routing_network, Mask/Prefix: $_routing_mask, Protocol: $_routing_protocol, GW: $_routing_lastgateway, Intf: $_routing_lastinterface" action 1.0 syslog msg "$msg"

About this App

This App and the Cisco Networks Add-on was created by Mikael Bjerkeland (mikael@bjerkeland.com).
Commercial support is available by contacting the author.
Community support is available at Splunkbase.