ClearPass Visibility POC Approach

Derin Mellor
Version 16th September 2019
Version 0.9971 DRAFT
Based on ClearPass 6.8.2

Contents
Objective ................................................................................................................................. 2
Configuration ............................................................................................................................ 3
Step1: Install ClearPass ............................................................................................................. 3
Step2 Basic Profiling into ClearPass ......................................................................................... 4
1 Configure Switch to send Broadcasts to ClearPass Data Port .................................................. 4
2 Configure Relay DHCP Requests to ClearPass ................................................................ ..... 5
3 Configure Cisco NetFlows ...................................................................................................... 6
4 Configure Aruba Controller IPFIX (Netflow next generation) ................................................. 6
5 Configure Aruba Switch “Device Fingerprint” ........................................................................ 6
6 Configure Aruba Switch “Port Mirroring” .............................................................................. 7
7 Configure SNMP MAC Notification Traps on HP/Aruba and Cisco switches .............................. 7
Step3: Tune ClearPass Server Configuration ............................................................................. 8
Step4: Configure Insight .......................................................................................................... 9
Step5: Import existing endpoint tables/audit ............................................................................. 10
Step6: Configure the Profiler details ......................................................................................... 10
Step7: Configure SMTP ............................................................................................................ 11
Step8: Define SNMP, SSH and WMI Profile Settings ................................................................ 11
Step9: Define Access Router .................................................................................................... 12
Step10: Define On-Demand Network Scan .............................................................................. 14
Step11: Update Network Scan to Scheduled ............................................................................ 15
Step12: Define an OnDemand Subnet Scan ............................................................................. 15
Step13: Update Subnet Scan to Scheduled ............................................................................. 16
Step14: Import Learnt NAS ...................................................................................................... 17
Step15: Update NAS SNMP Credentials ................................................................................. 18
Step16: Endpoint Audit Report ................................................................................................ 19
  ClearPass 6.8.2 Built-in Report ............................................................................................ 19
  ClearPass 6.7.x Import Custom Report ................................................................................... 19
  Endpoint Audit Report ......................................................................................................... 20
  Unseen Device Report ........................................................................................................... 23
Objective

This document attempts to explain how ClearPass could be deployed in a POC where the primary intention is for Visibility. This project may develop into Authentication – but not necessarily. NOTE the ClearPass Discovery capabilities has significantly improved with the 6.7 release.

This document explains how to interpret the results in order to identify and validate the endpoint’s location and classification.

Finally, we discuss how to generate an endpoint audit report that can be shared with the customer to understand what is a legitimate corporate device and how this information can then be imported back into ClearPass to create an effective network endpoint audit.
Configuration

Step 1: Install ClearPass
This comprises a ClearPass C1000 virtual appliance with 100 Access licenses. This should be installed in the normal manner. Details on this are available at https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Command/Core_Download/Default.aspx?EntryId=28206

Install using only an IP address on the Management interface.

The customer should have an HPE Passport account. This is required to get the Policy Manager license – required to get into the virtual appliance.

Make sure you update the Endpoint Profile Fingerprints updates:
Within the ClearPass’ Policy Manager→Software Updates specify the customer’s HPE Passport username and password:

On saving the ClearPass will attempt to interrogate the download site. This should pull down new Endpoint Profile Fingerprint and patches. Update the patches accordingly.

WARNING: If installing 6.7.0 you will not be able to active the licenses (due to the update site having a new certificate that is not trusted by this ClearPass). This is addressed by patching to 6.7.7.

NOTE Fingerprints are updated on the 1st and 15th of every month.

Step2 Basic Profiling into ClearPass
Select one or more of these options

1) Configure Switch to send Broadcasts to ClearPass Data Port
Traditionally, we would advise the customer to add another DHCP Relaying to their AccessRouter. Although this is very effective, customers may be antagonistic to making changes of AccessRouter for a POC. Secondly this does not work in simple flat-networks.

As we are primarily interested in seeing the DHCP broadcasts we can use the following simple approach:

1) Flat network with single VLAN: Connect a switch port to the Data port – this will receive the DHCP broadcasts.
2) Network with multiple VLANS, and the customer does not want to add DHCP Relaying to the AccessRouter: Configure a trunk port with all the necessary VLANS – this will receive the DHCP broadcasts for each VLAN.

WARNING: This has only had rudimentary testing... **
* Because ClearPass ignores broadcast DHCP requests and only considers unicast DHCP Requests.

** The span port on the network side is exactly that (just a trunk port with all VLANs present), and as such it will never see the (unicast) DHCP response... Unclear whether ClearPass will look at DHCP Responses...

The beauty of the above approach is it keeps the traffic load to a minimum.

Alternatively, we can add Span ports but traffic should be filtered to only pass the broadcast.

On ClearPass:

To check that this is working us the ClearPass “Collect Logs” can capture the network traffic.

2 Configure Relay DHCP Requests to ClearPass

This is our oldest and most reliable profiling. Clearly, it doesn’t help with devices with static IP addresses. If possible try and persuade customer to move to DHCP even if this is with reserved IP addresses.

```
vlan 1
  name "Management"
  untagged 1-10
  ip address 192.168.137.90 255.255.255.0
  ip helper-address 192.168.137.10
  ip helper-address 192.168.137.20
  exit

vlan 10
  name "Corp"
  tagged 6-8
  ip address 10.137.10.90 255.255.255.0
  ip helper-address 192.168.137.10
  ip helper-address 192.168.137.20
  exit

vlan 20
  name "Voice"
  tagged 6-8
  ip address 10.137.20.90 255.255.255.0
  ip helper-address 192.168.137.10
  ip helper-address 192.168.137.20
  voice
  exit

vlan 30
  name "Guest"
  tagged 6-8
  ip address 10.137.30.90 255.255.255.0
  ip helper-address 192.168.137.10
  ip helper-address 192.168.137.20
  exit
```

Where 192.168.137.10 is my DHCP server

Where 192.168.137.20 is my ClearPass
3 Configure Cisco NetFlows

Enable Netflows on Cisco switches — configuration defined here

ClearPass’ default configuration is to reprofile every 24 hours.

There are concerns that having too many switches configured with netflows may overwhelm ClearPass.

4 Configure Aruba Controller IPFIX (Netflow next generation)

IPFIX feature on Aruba Controllers injects device classification into ClearPass.

```
ifmap cppm
  enable
  server host "192.168.137.20" port 443 username "apiadmin" passwd <password>
```

Where 192.168.137.20 is the IP address of my ClearPass.
Clearly the apiadmin account’s password has to be configured (or whatever the account you use as long as it has an AccessType of API Access Admin).

5 Configure Aruba Switch “Device Fingerprint”

If the Aruba switch is running 16.06 or above you can configure the Device Fingerprint capability. This injects device classification into ClearPass.

```
radius-server host <CPPM-IP address>
radius-server cppm identity <IDENTITY> key <KEY>
device-fingerprinting timer 60
device-fingerprinting policy "profile1"
  http
  lldp
  dhcp
  cdp
  exit
device-fingerprinting apply policy "profile1" 1-6
device-fingerprinting 1-6 client-limit 4
```

This uses HTTPS to inject information into ClearPass. More details of the wired configuration available at

NOTE: You need to have the Intermediate CA for ClearPass HTTPS installed on the switch. I’m pretty confident that the IP is taken from the RADIUS server that is responding.
NOTE: The <IDENTITY> is a ClearPass API Administrator (Does this work??? Admin certainly does) within the Policy Manager → Administrator → User and Privileges → Admin Users.

NOTE: At this stage DHCP Profiling is superior on the ClearPass.

6 Configure Aruba Switch “Port Mirroring”
You could configure the switch to mirror all the uplink traffic on to another physical port on the switch that is connected in to ClearPass’ data port

```bash
mirror 1 port 5
interface 8 monitor all both mirror 1
```

This will mirror all the traffic on port 8 on to port 5.

7 Configure SNMP MAC Notification Traps on HP/Aruba and Cisco switches
The switch will inform ClearPass when a device connects/disconnects, it also indicates the port the device connected on.

Here is the typical Aruba switch configuration:
```
snmp-server host <CPPM-IP> community <string> trap-level all
snmp-server enable traps mac-notify
snmp-server trap-source <ip source of trap>
snmp-server enable traps link-change <port-list>
```

On each of the ports
```
interface <port> mac-notify traps learned
interface <port> mac-notify traps removed
```

On ClearPass configure the necessary community string (this must match above):
Step 3: Tune ClearPass Server Configuration

Configure the Log Accounting Interim-Update Packets:

**NOTE** On the span port only enable if using either option 1 or 6 in the above list.

- Use the FQDN name here rather than FQDN
- Do not enable as it finds too many Internet devices
- Do not use the Data port
Reduce the SNMP polling time of Access Router ARP tables

Step 4: Configure Insight
By default, Insight is configured to report information for up to 30 days. If you want to identify known devices that haven’t been seen for more than 30 days then this log needs to be extended. For example, increase this to 90 days:

This will allow you to generate an Insight report for devices that haven’t been seen for within the last month.
Step 5: Import existing endpoint tables/audit
Integrate any available MDM.

Import from IDS or Management systems.

Import from any existing audits: CSV can be converted to necessary XML using the ASE ClearPass Endpoint Batch Import solution (https://ase.arubanetworks.com/solutions/id/91).

Step 6: Configure the Profiler details

NOTE Enabling NMAP it will scan TCP ports 1-65534.

If this is viewed as too intense might be better to populate the “Profile Scan Ports” section and add a csv list of interested TCP ports to be scanned. In which case disable the “Enable Endpoint Port Scans using Nmap”.

It might be worth initially running in full scan to get a list of all the ports they have. Use this to craft a CSV list of port scans. Keep in might this list should still include the well known ports. Once this is complete the full scan can be disabled.

Here’s a common list of useful ports
4,546,547,554,631,636,749,750,751,752,753,754,760,1029,1080,1270,1293,1433,1434,1503,1521,1
812,1813,1863,2083,2375,2376,2377,2483,2484,3128,3306,3389,3479,3480,4243,5000,5004,5005,5
357,5358,5432,5500,5631,5632,5722,5985,5986,6600,7680,9001
Step 7: Configure SMTP

Although the CPG’s “Test” is better than the PolicyManager’s (CPG → Configuration → Receipts → Email Receipts has more error reporting) it relies on having at least 1 Access or Onboard license (without this you can’t login to the CPG).

Use the PolicyManager’s Test

If you don’t receive the email use ClearPass “Collect Logs” to take a network trace...

Step 8: Define SNMP, SSH and WMI Profile Settings
Step 9: Define Access Router

- **Edit External Account**
  - Name: SNMP
  - Type: SNMP
  - Description: SNMP v2 with community string
  - Community String: ***************

- **Edit External Account**
  - Name: SSH
  - Type: SSH
  - Description: User access
  - Username: admin
  - Password: ***************
  - Verify Password: ***************

- **Edit External Account**
  - Name: WMI
  - Type: WMI
  - Description: WMI connection
  - Domain: \mydomain\mydomain
  - Username: administrator
  - Password: ***************
  - Verify Password: ***************

**ClearPass Policy Manager**

Network Devices

- Device 1: Aruba 2530
  - IP: 192.168.37.00
  - Description: Added by Network Discovery
- Device 2: Wi-Fi
  - IP: 192.168.37.100
- Device 3: MacOut
  - IP: 192.168.37.204
- Device 4: VAP
  - IP: 192.168.37.99
These need to be defined so that ClearPass can read the ARP table and get the MAC address to IP address mappings.

Don’t use a range of IP addresses (i.e., 192.168.137.99–192.168.137.100) – it has issues. Subnets are OK but I prefer defining each NAD explicitly.

NOTE: If ClearPass fails to read the NAD using SNMP you will get an error in the Event Viewer:
Step 10: Define On-Demand Network Scan

ClearPass will scan the network looking for devices. It connects to the seed router(s) and hierarchically search for other router, switches, controllers and find associated connected devices. From this it collates these device details including any location information.

Make sure ClearPass is whitelisted in any IDS or NextGen firewalls.

As this generates a lot of traffic run this at a quiet period to get an initial baseline.

Specify “seed” router(s), time of scan and number of hops to search:

![ClearPass Policy Manager](image)

**WARNING:** Performing network scans can be resource intensive and time consuming. For large networks, scans could take more than an hour and ideally should be done on a ClearPass node that is not servicing core authentications, or should be done outside of normal business hours.

This service will start running within 30s and collect the information.

[Image of ClearPass Policy Manager]

Populate with as many NAS, AccessRouter, hosts, etc. Don’t assume it will automatically find these: The Seed NAS (and associated “discovered” NASs) won’t necessarily be in their ARP table.

This is a coma separated list of IP addresses.
Step 11: Update Network Scan to Scheduled

Update the Network Scan to be a scheduled at a quiet time.

Step 12: Define an OnDemand Subnet Scan

Be explicit of the VLANs you want to scan. This is effective at profiling quiet devices particularly with static IP addresses. This is intensive, similar in nature to the Network scan – suitable whitelisting should be added. Run this at a quiet period to get an initial baseline.
This service will start running within 30s and collect the information.

And once the scan is complete...

Step 13: Update Subnet Scan to Scheduled
Step 14: Import Learnt NAS

Once the Network Discover and Subnet Scan are complete ClearPass should have learnt the NAS (switches, controllers, VPN, routers, fat-AP, etc) on the network. This provides a simple mechanism to import these devices:

This allows you to import these devices. Devices that don’t present a Name can’t be imported.

Select the device – choose the interface that will be used as the source IP for the RADIUS Request:

On importing it will prompt for the RADIUS and TACACS secret:

Although these may not be used at this stage it makes sense to configure so that if you want to move to a control environment the ClearPass is already configured.
Step15: Update NAS SNMP Credentials

By configuring the NAS’ SNMP credentials will aid ClearPass extracting the latest ARP entries.

ClearPass will poll all these based on the poll timer set in Step3. If there is a problem polling the NAS it will be reported in the Event Viewer with incorrect SNMP credentials:
Step 16: Endpoint Audit Report

ClearPass 6.8.2 Built-in Report

6.8.2 integrates the Active Endpoint Security that reports the Endpoints that have connected within the scan/polled period. And the Idle Endpoints Security the Endpoints that have not connected within this scanned/polled period.

Refer to the next section for the configuration.

ClearPass 6.7.x Import Custom Report

If using 6.7.x you can get this from this [Arubapedia](https://example.com) URL or [AfP](https://example.com) URL.

This has not been tested on prior to 6.7.
WARNING: If you have resilience Insight setup you will have to import this template into each Insight server – this can only be done when it is operating as the Master.

Once imported you should see:

**Endpoint Audit Report**
Create a scheduled report of all the Endpoints seen in the last month:
This will generate a report every Sunday morning at 6am covering the devices that have updated over the last week.
When the report is completed an email will be sent to this email address (in this case derin.mellor@hpe.com).

To force the report to run click the “run button”:

This will also attempt to email it...

If you didn’t receive the email – you can manually download the report when it has completed. When the report has completed the status button will report red (because this is a scheduled report):
Manually download the report using the Folder ICON:

Open the zipped file – see Review Discovered Endpoints below.

**Unseen Device Report**

Repeat the same process for the “Unseen Device Report”
This will create a CSV. This reports devices that haven’t been seen is a specified timeframe (eg day, week, month). In the example the schedule is set for a week this will report Known endpoints not seen in 7 days:

These deserve investigating.
Review Discovered Endpoints

If all is working you should have an email with an attached endpoint audit:

This contains a PDF Stakeholder report and a CSV Technician’s report.

This should contain a PDF and CSV. Within these will be the endpoints that have been updated (UpdatedAt field) within the report period or 1 day (24 hours), 1 week (7 days) or 1 month (30 days).
Stakeholder Report
The PDF is effectively a stakeholder report that summaries the state of the network and identifies things that need further investigation.

- **Known vs Unknown vs Disabled endpoints**: Ultimately you want to minimise the Unknown.

- **Number of devices that we have observed a spoofed MAC address**: ClearPass is not finding all the information about these devices.

- **Breakdown of numbers of device types**: Devices that have suspicious fingerprints.
**Technician’s Report**

The CSV contains technical details.

This enables a technician to locate the device can validate it. This can then be imported back into ClearPass – more on this later.

Open this in Excel:

![Excel Spreadsheet](image)

**Validate Endpoints**

Using the Endpoints spreadsheet investigate the following:

1) **Unknown devices: status = Unknown**
   These devices need to be validated
   (Endpoints Filter on status column for Unknown)

2) **Disabled devices: status = Disabled**
   Why are these devices still connected to the network?
   (Endpoints Filter on status column for Disabled)

3) **IP only**
   These are all the devices that have been found, typically by an active subnet scan but the matching MAC address has not been found in the polled ARP tables.
   (Endpoints Filter on macaddress column using text filter begins with 'x')

4) **Static IP**
   Is this a legitimate device with a static IP? If not why is ClearPass not seeing the DHCP Request from these devices?
   (Endpoints Filter on is__static__ip column for “TRUE”)

5) **No IP**
   Possibly an indication that ClearPass is not polling the correct ARP table
6) Generic category
Identify the device types and create custom fingerprint for these devices
Feed this information (device type, category and fingerprint) back to Aruba TAC
(Endpoints Filter on device_category column for generic)

7) Unprofiled
Either an indication of
   a. DHCP Requests are not being relayed to ClearPass
   b. Device has a static IP – ie no DHCP
   c. Active scanning is not scanning that network
   d. Firewall is blocking the active scans
   e. Device is transient and was not connected during active scan
(Endpoints Filter on fingerprint column for {})
Updating and Importing Endpoint Information

The customer should validate all the endpoints updating the Endpoints sheet Status column (eg Known) and possibly add other columns that provide extra information (eg Owner).

WARNING: If you intend using the import tool then the updates must be done in the Endpoints tab.


Go into the CSV file can copy the contents:
Go to the ASE ClearPass Endpoint Batch Import:

Download the resultant file:
Within ClearPass Endpoints import this file:

This import will warn of any issues.
When you look at the updated Endpoint:

The other fields appear in the Attributes tab:

Manually Update Learnt Endpoints
This has already been covered from the CSV perspective. But often it is easier to do this direct from the ClearPass PolicyManager GUI:

Look at any interesting Endpoints

Note that this reports the associated NAD (switch 192.168.137.90) and port.

It has also learnt the IP address, hostname. Looking at the fingerprint:
This information has been learnt via NMAP and WMI scan.

<table>
<thead>
<tr>
<th>Endpoint Fingerprint Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WMI OS Name:</strong> Microsoft Windows Server 2012 R2 Standard</td>
</tr>
<tr>
<td><strong>Host Services:</strong> 135 -- mRPC  139 -- netbios-ssn  443 -- https</td>
</tr>
<tr>
<td><strong>Host Open Ports:</strong> 135, 139, 443</td>
</tr>
</tbody>
</table>

Set Status

Correct categorization
APPENDIX A: Reporting ClearPass Profile Fingerprints

When reporting a new or incorrect fingerprint

- Collect the device make, model, version
- What do you think it should be classified as?
- What is the fingerprint ClearPass received?
  - Use the information from the ClearPass Endpoint Audit report
  - Or export the Endpoint from ClearPass – this includes the fingerprint

For

- Aruba SE – Use https://jira.arubanetworks.com submit details
- Partner/Customer – Raise a TAC case with these details