TECHNICAL NOTE
CLEARPASS ACTIVE PROFILING
DEVICE DISCOVERY AND SUBNET SCANS

Revised By   Date   Changes
Dennis Boas  Oct 2016 Version 1a – updated for 6.6.2
# TABLE OF CONTENTS

- Clearpass Active Profiling .................................................................................................................. 1  
- Device Discovery and Subnet scans ..................................................................................................... 1  
- Introduction ......................................................................................................................................... 3  
- Device Discovery Techniques ............................................................................................................... 3  
- Device Discovery ................................................................................................................................. 3  
- Subnet Scans ....................................................................................................................................... 4  
- Configure Credentials .......................................................................................................................... 4  
  - SNMP Configuration .......................................................................................................................... 4  
  - SSH Configuration ............................................................................................................................ 5  
  - WMI Configuration ............................................................................................................................. 6  
- NMAP Scan .......................................................................................................................................... 6  
  - NMAP Scan Configuration ............................................................................................................... 7  
  - Using NMAP scan results for Authorization ................................................................................. 7  
- Configure Subnet Scan .......................................................................................................................... 9  
  - On Demand Subnet Scan .................................................................................................................... 10  
  - Trigger Endpoint Scans ...................................................................................................................... 11  
- Configure Device Discovery .................................................................................................................. 13  
  - Configure Network Device ............................................................................................................... 13  
  - Add Seed Device ............................................................................................................................... 14  
  - Discovered Devices ........................................................................................................................... 15  
  - Discovered Endpoints ....................................................................................................................... 17  
  - Importing Discovered Devices ......................................................................................................... 18  
- Troubleshooting .................................................................................................................................. 20  
  - Event Viewer ................................................................................................................................... 20  
  - Log Configuration .............................................................................................................................. 20  
  - Debug Web Page ............................................................................................................................... 21  
- Additional Resources ............................................................................................................................. 23
Introduction

This technical note is intended to help field engineers, customers, and partners understand, configure and deploy ClearPass Device Discovery and ClearPass subnet scanning. These features are used to discover and profile network access devices and endpoints. A critical element of network security is discovering what devices are connecting to the network and making sure that they are given the correct level of network access. Once a new device is discovered it can be profiled and authorized access based on attributes such as Host Name, Device Category, Device OS Family and Device Name. For example, network cameras and printers require access to different network resources and are often assigned to different VLANs. After the printer or camera is profiled, ClearPass will authorize and enforce the correct level of access and assign the correct VLAN. Discovering and profiling devices with statically assigned addresses requires different techniques than those that are used with dynamically addressed devices. ClearPass provides a set of tools to automate the discovery and profiling of both dynamically and statically addressed devices.

Device Discovery Techniques

Device discovery techniques can be broadly categorized as either active or passive. Active techniques involve a series of focused probes directed at network access devices or more generalized subnet scans. Active techniques are primarily used for discovering and profiling statically addressed devices. Passive techniques involve monitoring message exchanges such as DHCP requests, TCP exchanges or analyzing the user agent information from a HTTP connect packet. Passive techniques work best with dynamically addressed devices. Agents such as OnGuard can also provide endpoint profiling information. This Tech Note focuses on active discovery techniques.

Device Discovery

Device Discovery is a two-step process that identifies and profiles network access devices (switches and routers) and the endpoints (servers, computers, IoT devices, etc.) that are connected to them.

Step 1 uses SNMP to read information from the Bridge, ARP, LLDP and CDP MIBs on a network access seed device (switch or router). This information is used to discover neighboring network access devices. This process is repeated for each neighboring device until the scan depth limit is reached. Scan depth is configurable from one to five layers. The discovered network access devices can be imported into the ClearPass Network Device Table.

Scan depth = 2
Step 2 uses the IP to MAC mapping information from the ARP tables of the network access devices to generate a scan of each of the connected endpoints. This scan looks for specific open ports and then use SNMP, SSH and WMI to profile the endpoint.

- If port 22 is open use SSH to login and collect profiling information
- If port 135 is open use WMI to login and collect profiling information
- If port 161 is open use SNMP to collect profiling information
- If port 135 and port 3389 are both open assume the endpoint is Windows based

After the discovered endpoints are profiled, the Endpoints Table is updated with the new information.

**Subnet Scans**

Instead of probing network access devices to discover connected endpoints, subnet scans probe all addresses in the selected subnets. When an endpoint is detected;

- If port 22 is open use SSH to login and collect profiling information
- If port 135 is open use WMI to login and collect profiling information
- If port 161 is open use SNMP to collect profiling information
- If port 135 and port 3389 are open assume the endpoint is Windows based

If the discovered endpoint has a statically assigned address it is profiled and the new information is added to the Endpoints Table.

**Configure Credentials**

The SNMP, SSH and WMI credentials used by both Device Discovery and subnet scans are configured in *Configuration >> Profile Settings*.

**Profile Settings**

The first step in configuring Device Discovery and subnet scans is to enter the access credentials in the configuration tabs

**SNMP Configuration**

Enter the subnets to be used for Device Discovery or subnet scans in a comma separated list. Do not end the list with a carriage return. Then add the SNMP credentials that should be used for the subnets.
You can add multiple sets of credentials. If Port 161 is open ClearPass will attempt to use each set of credentials to profile the device or endpoint.

SSH Configuration

Under the SSH Configuration tab enter the subnets to be used. Then add the CLI login credentials and the Enable password. If port 22 is open, ClearPass will use these credentials to login and gather profiling information.
WMI Configuration

Under the WMI tab enter the subnets to be used. Then add the Active Directory domain credentials. Multiple domains can be configured. If port 135 is open, ClearPass will attempt to use the WMI protocol to gather profiling information.

NMAP Scan

ClearPass release 6.6.2 added the option of using NMAP scans and signatures for device profiling. NMAP scans return host open ports and host services for scanned endpoints. This information is used for device profiling and is posted to the Endpoint (Fingerprints tab).
Configuration >> Identity >> Endpoints

NMAP Scan Configuration

NMAP scans are enabled in the Profiler Tab under Administration >> Server Manager >> Server Configuration >> Cluster-Wide Parameters.

Using NMAP scan results for Authorization

The NMAP information shown in the Fingerprint tab can be used for endpoint authorization. In this example we will use a MAC Auth service and create a simple role to determine the format of the NMAP information.
This role will match any existing fingerprint. After forcing a MAC authentication, we can examine the Authorization attributes in Access Tracker. This will show the format of the returned attributes.

Using this information, we can create a role (LAB SSL 5.8) to authorize access if the endpoint is using SSH version 5.8
To test our new role mapping, re-authenticate the endpoint. Access Tracker now shows the correct role being applied.

Note: NMAP scans are triggered by Device Discovery, periodic subnet scans and on-demand subnet scans.

**Configure Subnet Scan**

If the Subnet Scan tab is configured, ClearPass will automatically scan the configured subnets once a day. To configure subnet scans, go to **Configuration > Profile Settings** and select a Policy Manager Zone for the scan.
After selecting the correct, add the subnets in a comma separated list. ClearPass will automatically scan the configured subnets once every 24 hours.

You can change the scan interval under Administration >> Server Manager >> Server Configuration >> Cluster Wide Parameters.

On Demand Subnet Scan

On Demand Subnet Scans can be run as needed and are recommended after adding new devices to the network.
Select **On-Demand Subnet Scan**, then enter the subnets to scan and click **Submit**. For both On Demand and automatic scans the endpoint table will only be updated if Static IP is True.

A subnet scan added the above endpoint entry. Notice that Static IP is True and the Fingerprint shows that both SNMP and SSH were used to profile the device.

**Trigger Endpoint Scans**

An SNMP or NMAP scan can be manually triggered from the endpoint table. This can be useful if ClearPass was not able to classify the endpoint. In the following example; Device Category, OS Family and Device Name are all unknown.

By selecting the table entry and clicking Trigger Server Action an NMAP or SNMP scan can be manually initiated
The NMAP scan below shows open ports, Network Applications and Device category. In this case NMAP's confidence is 100%. If this is correct, selecting Update will update the endpoint table.

The endpoint entry now shows the correct Device Category, Device OS Family and Device Name. The fingerprint shows that NMAP profiled the endpoint.
The other type of scan that can be triggered is SNMP. Subnet scans only profile statically addressed endpoints. With triggered scans, SNMP can be used to gather additional profile information for dynamically addressed endpoints.

Typically SNMP scans are most effective for network devices since they generally support SNMP.

You can only trigger one NMAP or SNMP scan at a time. If the scans do not show up in the pull down menu, make sure you don’t have more than one endpoint entry selected.

Configure Device Discovery

After the Profile Credentials are configured, the next step is to configure the network seed device. Multiple seed devices can be configured. In a geographically dispersed deployment, configure at least one seed device for each location. A core or distribution layer switch is a good choice for a seed device.

Configure Network Device

Go to Configuration >> Network >> Devices and click on the SNMP Read Settings tab.
Enable ClearPass to use SNMP to access this device
Select SNMP version
Configure access credentials (community string)
Enable Force Read, causes all nodes in cluster to read information from this device
Enable Read ARP Table Info to extract MAC to IP mappings

Add Seed Device

In Monitoring >> Profiler and Discovery >> Network Discovery, click on Start Network Discovery Scan to add the seed devices.

- Set scan depth from 1 to 5 layers
- Add IP address of Seed Device
- Enable Probe ARP Entries
- Start Discovery

After Discovery has started the progress bar will show the status as “In Progress”.
In this example Discovery is complete and two devices and 13 endpoints have been discovered.

Devices are defined as Network Access Devices (switches and routers), Endpoints are servers, computers, Printers, IoT devices, etc.

**Discovered Devices**

The Discovered Devices page shows the results of the Device Discovery scan. In this example two switches were discovered. Clicking on the device opens the device details view.

The detail view reveals that port 5 of the HP-3800 is connected to the Aruba S2500 switch.
Examining the detailed view for the Aruba S2500 switch shows the connection back to the HP-3800 is via port 0 and that port 8 is connected to an address outside of the subnets configured in the SNMP Profile. For this reason, the profile information for 169.254.70.20 is incomplete and the device type is Unknown.

This unknown device is not listed as a discovered device since it’s not part of the profiled subnets shown below.
The network topology revealed by Device Discovery looks like this;

Discovered Endpoints

Discovered endpoints are shown on the Monitoring >> Profiler and Discovery >> Endpoint Profiler page. In this example one server was discovered and profiled, clicking on the server opens the detail view.

The fingerprint shows that the ClearPass VM server was profiled using SNMP.
Importing Discovered Devices

Device Discovery automates the process of adding new network devices to the ClearPass Network Device table. Go to Monitoring >> Profiler and Discovery >> Discovered Devices.

To add the HP3800 switch, select its device entry and click Import.

Configure the RADIUS and TACACS+ shared secrets and enable CoA. The network device will be added to the ClearPass network device table and the description will show that it was added by Network Discovery.

You can see the results of the import in Configuration >> Network >> Devices.
## TECHNICAL NOTE

### DEVICE DISCOVERY AND SUBNET SCANS

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>IP or Subnet Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HP-3800-48G-PoEP-4SP_</td>
<td>192.168.2.1</td>
<td>Added by Network Discovery</td>
</tr>
<tr>
<td>2</td>
<td>MAS</td>
<td>192.168.1.207</td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting

Event Viewer

To verify the discovery scan completed successfully check the event viewer. SNMP service shows the network scan completing successfully but also shows read device information errors.

SNMP was unable to get profiling information for 192.168.1.251. The most common reasons for this type of failure is either lack of SNMP support on the device or incorrect SNMP credentials.

Log Configuration

Go to Administration >> Server Manager >> Log Configuration and select ClearPass Network Services. Set SNMP request processing to DEBUG level.

This log entry shows that the SSH Login to 192.168.1.244 failed. The most common causes for this type of failure are invalid credentials or the target does not permit remote login.
"ip": "192.168.1.244",
"host_info": {
    "ip": "192.168.1.244",
    "mac": "000c292f6c23",
    "id": "scan-1471692033-27",
    "start": "2016-08-20T11:20:33.71779289Z",
    "end": "2016-08-20T11:20:57.451885387Z",
    "status": "ssh: scan-1471692033-27 connect/login to 192.168.1.244 failed. Endpoint profile failed."
}

**Debug Web Page**

To simplify troubleshooting, much of the information for the seed device and the discovered devices is collected in special web pages.

*Error! Hyperlink reference not valid.*

These pages show device information for configured (seed devices) such as Sys Name, Sys Description, Object ID, and NAD configuration.

Selecting **Discovered Devices** shows the basic device information for discovered devices.
Selecting **Switch Port Info** shows port level detail.
Additional Resources

Detailed information on ClearPass Profiling can be found in the ClearPass Profiling Tech Note and the ClearPass Profiling Quick Start Guide available on the support site.

Support Site: