Change Log

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>August 2019</td>
<td>Anish Pansare</td>
<td>First Published Version – Phase 1</td>
</tr>
</tbody>
</table>

Copyright

© Copyright 2019 Hewlett Packard Enterprise Development LP.

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. A complete machine-readable copy of the source code corresponding to such code is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett-Packard Company. To obtain such source code, send a check or money order in the amount of US $10.00 to:

Hewlett-Packard Company
Attn: General Counsel
3000 Hanover Street
Palo Alto, CA 94304
USA

Please specify the product and version for which you are requesting source code. You may also request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com.
Contents

Introduction .................................................................................................................................................. 5
Software Requirements .............................................................................................................................. 5
Installation and Deployment Guide ........................................................................................................... 5
Pictorial view of the Integration .................................................................................................................. 6
Configuration ............................................................................................................................................... 7
  Configuration of ClearPass ......................................................................................................................... 7
  Create a ClearPass API User ..................................................................................................................... 7
  Create a ClearPass Operator Profile ......................................................................................................... 8
  Create a ClearPass OAuth API Client ....................................................................................................... 10
  Configuration of Nozomi ......................................................................................................................... 12
Monitoring/Reviewing ClearPass and Nozomi communications ................................................................. 16
Figures

Figure 1: Pictorial view of ClearPass Policy Manager integration with Nozomi Networks ........................................... 6
Figure 2: Create an API level account in ClearPass ........................................................................................................ 7
Figure 3: Creating a restricted access Operator Profile – Part1 ......................................................................................... 8
Figure 4: Creating a restricted access Operator Profile – Part2 ......................................................................................... 9
Figure 5: Create an API Client ............................................................................................................................................ 10
Figure 6: Generate Access Token ...................................................................................................................................... 11
Figure 7: Nozomi Main Dashboard ................................................................................................................................ 12
Figure 8: Configuring communication with ClearPass-1 .................................................................................................. 12
Figure 9: Configuring communication with ClearPass-2 .................................................................................................. 13
Figure 10: Configuring communication with ClearPass-3 .................................................................................................. 14
Figure 11: Endpoint Dictionary Attributes created by Nozomi ......................................................................................... 14
Figure 12: Example of Endpoints created by Nozomi ........................................................................................................ 15
Figure 13: Normalized Endpoint data created by Nozomi ................................................................................................. 15
Figure 14: Custom Endpoint data created by Nozomi ......................................................................................................... 15
Figure 15: Logs from Nozomi Smart Polling screen-1 ....................................................................................................... 17
Figure 16: Logs from Nozomi Smart Polling screen-2 ....................................................................................................... 16
Figure 17: Example of API logs between Nozomi and ClearPass ....................................................................................... 17
Introduction

This Integration Guide covers the configuration and use of the integration between Nozomi Networks and ClearPass Policy Manager. The Nozomi platform delivers continuous ICS threat monitoring and asset discovery, combining a deep embedded understanding of industrial protocols, devices, and applications with ICS-specific behavioral anomaly detection, threat intelligence, risk analytics, and automated threat modeling. This initial integration between Nozomi and ClearPass focuses on the ability for Nozomi to detect, discover and classify OT/ICS endpoints and share this classification directly with ClearPass via the ClearPass Security Exchange framework and the open API we expose. Nozomi will automatically update the ClearPass Policy Manager Endpoint Database with endpoint classification data and a number of custom security attributes.

This is Phase1 of our planned integration with Nozomi Networks, centralized visibility of network assets and endpoints across IT and OT infrastructure. From here a centralized endpoint and edge security policy can be defined and administered. Check back for updates to our Nozomi Networks integration framework.

Software Requirements

The minimum software version required for ClearPass is 6.7.2. ClearPass runs on hardware appliances with pre-installed software or as a Virtual Machine under the hypervisors. Hypervisors that run on a client computer such as VMware Player are not supported. Supported Hypervisors are listed under release notes:


Interoperability validation is done with ClearPass version 6.8.1 and Nozomi Networks version 18.5.8.

Installation and Deployment Guide

The generic ClearPass installation and deployment guide is located here:

Pictorial view of the Integration

The diagram below shows a pictorial overview of the components and how they interact with each other.

*Figure 1: Pictorial view of ClearPass Policy Manager integration with Nozomi Networks*

Nozomi synchronizes its asset inventory list into ClearPass endpoint database. The device context can be used for Dynamic Segmentation leveraging policies.

Discovered devices are pushed into ClearPass Policy Manager endpoint database leveraging the endpoints REST APIs. Periodic sync occurs to push data into ClearPass.
Configuration

Configuration of ClearPass

Prior to creating and enabling the integration in Nozomi a number of configuration elements need to be pre-created in ClearPass. Follow the below configuration steps carefully, collecting data as highlighted as you will need this in the following section when configuring Nozomi to communicate with ClearPass.

Create a ClearPass API User

As part of the communications channel between the two products, Nozomi will use a number of APIs (both TIPS and REST), access to the TIPS API’s is validated via Username/Password combination credentials. This UserID needs to have minimum levels of access, do not use a Super Administrator profile, use API Administrator as shown below.

Create a user from Administration -> Users and Privileges -> +ADD -> {Create a user, ensure that you set a privilege level of API Administrator}

Make a note of the UserID and the password that was configured, ensure Privilege level is API Administrator

Figure 2: Create an API level account in ClearPass
Create a ClearPass Operator Profile

Nozomi also uses the REST APIs as part of the integration, REST APIs are authenticated under an OAuth framework. Create as shown below an API Client. To secure access to only the REST API for the API Client create a restricted access Operator Profile as shown below. In summary all options are set as ‘No Access’ except for API Services and Policy Manager, which is custom and then specific as shown below.

Under API Services

- **Allow API Access = Allow Access**

Under Policy Manager

- **Dictionaries – Attributes = Read, Write, Delete**
- **Dictionaries – Fingerprints = Read, Write, Delete**
- **Identity – Endpoints = Read, Write, Delete**

*Figure 3: Creating a restricted access Operator Profile – Part 1*
Figure 4: Creating a restricted access Operator Profile – Part 2

Policy Manager

Select operator permissions for Policy Manager

- Application Licenses
  - Operators with this privilege can manage Application Licenses
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Authentication - Methods
  - Operators with this privilege can manage authentication methods
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Certificate - Revocation List
  - Operators with this privilege can manage Revocation Lists
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Certificate - Trust List
  - Operators with this privilege can manage certificate trust lists
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Certificates
  - Operators with this privilege can manage certificates
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Clearpass Portal
  - Operators with this privilege can manage Clearpass Portal
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Configuration - Network Scan
  - Operators with this privilege can manage Network Scan under Configuration
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Configuration - Services
  - Operators with this privilege can manage Services under Configuration
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Dictionaries - Attributes
  - Operators with this privilege can manage attributes
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Dictionaries - Context Server Actions
  - Operators with this privilege can manage context server actions
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Dictionaries - Fingerprints
  - Operators with this privilege can manage fingerprints
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Events - Login Audit
  - Operators with this privilege can manage login audits
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Events - System Events
  - Operators with this privilege can manage system events
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- External Servers - Endpoint Context Servers
  - Operators with this privilege can manage endpoint context servers
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- External Servers - File Backup Server
  - Operators with this privilege can manage file backup servers
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- External Servers - SNMP trap receivers
  - Operators with this privilege can manage SNMP trap receivers
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- External Servers - Syslog Export Filters
  - Operators with this privilege can manage syslog export filters
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- External Servers - Syslog Targets
  - Operators with this privilege can manage syslog targets
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete

- Identity - Endpoints
  - Operators with this privilege can manage endpoints
    - No Access ○ Read ○ Read, Write ○ Read, Write, Delete
Create a ClearPass OAuth API Client

Next create an API Client **Guest -> Administration -> API Services -> API Clients -> {Create API Client}**

Ensure you use the Operator Profile previously created to restrict the capabilities of the API Client.

Notice the highlighted configuration options needed, and set as appropriate

- **Operating Mode = ClearPass REST API** – Client will be used for API calls to ClearPass
- **Operator Profile = Use the Profile you created previously**
- **Grant Type = Client credentials (grant_type = client_credentials)**

Ensure you record the Bearer Token and the Client ID i.e. nozomi-rest as below

**Figure 5: Create an API Client**

After creating an API client, select the client and click on **Generate Access Token**. This bearer token is needed in Nozomi’s configuration. Nozomi is yet to implement lifecycle management for tokens, so set the **Access Token Lifetime** to a greater value. For example, we can set the token lifetime to 52 weeks.
At this time all of the necessary config has been created in Policy Manager, ensure you collected the below list of information before proceeding to the next section.

- CPPM API Administrator Username
- CPPM API Administrator Password
- CPPM OAuth2 API Bearer Token
Configuration of Nozomi Networks

For this initial integration between the two products, there is limited configuration required on Nozomi. After the configuration is complete the Nozomi platform will continue to update the ClearPass Policy Manager EndpointDb as it discovers new endpoints. Follow the below to configure and enable the integration.

From the Nozomi dashboard follow the **Administration -> Smart Polling**

**Figure 7: Nozomi Networks Main Dashboard**

Click the “+” icon on the top right.

**Figure 8: Configuring communication with ClearPass-1**
Select the Aruba ClearPass integration from the drop down.

*Figure 9: Configuring communication with ClearPass-2*

![Image of ClearPass integration setup]

Fill in the requested data. You’ll need to enter the ClearPass node details and enter the bearer token created above.

*Figure 10: Configuring communication with ClearPass-3*

![Image of ClearPass integration configuration]

Please note the **Query** should be set to “nodes”. **Run interval** is in seconds and Aruba recommends to keep at 60 seconds interval. **Username** should be ClearPass API administrator created earlier. **Password** is API administrator’s password. **Bearer Token** is previously generated on Page 11.
As part of enabling the above integration, Nozomi will create a number of custom Endpoint Dictionary attributes using the ClearPass REST API, /attribute. This is a record of the Dictionary Attributes created by Nozomi, these custom attributes can then be used for role-mapping/enforcement actions in a Service Policy.

**Figure 11: Endpoint Dictionary Attributes created by Nozomi**

![Dictionary Attributes Table]

The Endpoint data is sent by Nozomi, it creates the Endpoints, sets the endpoint classification and also configures custom endpoint attributes. An example of the data sent is below.

**Figure 12: Example of Endpoints created by Nozomi**

![Endpoints Table]
Looking closer at the endpoint data we can see several important things, the mac-address, mac-vendor, and some endpoint classification as determined by Nozomi, other valuable data such as the date the endpoint was added and profiled, said another way the time Nozomi updated ClearPass with the endpoint attributes.

**Figure 13: Normalized Endpoint data created by Nozomi**

<table>
<thead>
<tr>
<th>Endpoint</th>
<th>Attributes</th>
<th>Fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MAC Address</strong></td>
<td>000c29425f52</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>device info from Scada Guardian Nozomi Networks</td>
<td></td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Known client</td>
<td></td>
</tr>
<tr>
<td><strong>MAC Vendor</strong></td>
<td>VMware, Inc.</td>
<td></td>
</tr>
<tr>
<td><strong>Added by</strong></td>
<td>oauth2:nozomi-rest</td>
<td></td>
</tr>
<tr>
<td><strong>Online Status</strong></td>
<td>Not Available</td>
<td></td>
</tr>
<tr>
<td><strong>Connection Type</strong></td>
<td>Unknown</td>
<td></td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>192.168.1.32</td>
<td></td>
</tr>
<tr>
<td><strong>Static IP</strong></td>
<td>TRUE</td>
<td></td>
</tr>
<tr>
<td><strong>Hostname</strong></td>
<td>-</td>
<td></td>
</tr>
<tr>
<td><strong>Device Category</strong></td>
<td>PLC</td>
<td></td>
</tr>
<tr>
<td><strong>Device OS Family</strong></td>
<td>Rockwell_Automation/AI</td>
<td></td>
</tr>
<tr>
<td><strong>Device Name</strong></td>
<td>ControlLogix_1756-ENB</td>
<td></td>
</tr>
<tr>
<td><strong>Added At</strong></td>
<td>Aug 08, 2019 14:17:30 PDT</td>
<td></td>
</tr>
<tr>
<td><strong>Last Profiled At</strong></td>
<td>Aug 08, 2019 14:17:30 PDT</td>
<td></td>
</tr>
</tbody>
</table>

In addition to the standard data, Nozomi supplies other custom attributes, clicking on the **Attributes** tab provides the below attributes, any of this data could be used in Policy.

**Figure 14: Custom Endpoint data created by Nozomi**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Nozomi_firmware_version</td>
<td>= 18.002</td>
</tr>
<tr>
<td>2. Nozomi_ip</td>
<td>= 192.168.1.32</td>
</tr>
<tr>
<td>3. Nozomi_mac_vendor</td>
<td>= VMware, Inc.</td>
</tr>
<tr>
<td>4. Nozomi_product_name</td>
<td>= ControlLogix 1756-ENBT/A</td>
</tr>
<tr>
<td>5. Nozomi_protocols</td>
<td>= ethertip</td>
</tr>
<tr>
<td>6. Nozomi_roles</td>
<td>= slave</td>
</tr>
<tr>
<td>7. Nozomi_serial_number</td>
<td>= 00112235</td>
</tr>
<tr>
<td>8. Nozomi_type</td>
<td>= PLC</td>
</tr>
<tr>
<td>9. Nozomi_vendor</td>
<td>= Rockwell Automation/Allen-Bradley</td>
</tr>
<tr>
<td>10. Click to add...</td>
<td></td>
</tr>
</tbody>
</table>
Monitoring/Reviewing ClearPass and Nozomi Networks communications

Once the sync has started endpoint data will be populated directly into the Policy Manager EndpointDb, you can view the logs from the Smart Polling screen.

*Figure 15: Logs from Nozomi Smart Polling screen-1*

![Logs from Nozomi Smart Polling screen-1](image)

Sample logs shown below.

*Figure 16: Logs from Nozomi Smart Polling screen-2*

```
[2019-08-09T21:00:37+00:00 #1314] INFO -- : Started polling 10.2.100.86
[2019-08-09T21:00:37+00:00 #1314] INFO -- : Send asset information to clear pass - started
[2019-08-09T21:00:37+00:00 #1314] INFO -- : Update ClearPass assets - started
[2019-08-09T21:00:37+00:00 #1314] INFO -- : Connect to ClearPass host 10.2.51.153
[2019-08-09T21:00:38+00:00 #1314] INFO -- : Send modified asset having mac 00:50:56:99:04:b3
[2019-08-09T21:00:38+00:00 #1314] INFO -- : Send asset information to clear pass - success
```
If the Sync is not working or shows an error then it’s likely you’ve missed capturing some of the information, recheck the data recorded, additionally you can view the API calls between Nozomi and ClearPass from **Guest->** **Administration->** **Support->** **Application Log** below an example of API’s from Nozomi to ClearPass.

**Figure 17: Example of API logs between Nozomi and ClearPass**

---

**Home -> Administration -> Support -> Application Log**

**Application Log**

The events and messages generated by this application are logged here. For in-depth information about an event, click on it.

<table>
<thead>
<tr>
<th>Time</th>
<th>IP</th>
<th>User</th>
<th>Severity</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API Trace: GET /api/endpt -&gt; 200 OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API call &quot;GET /api/endpt?filter= (&quot;mac_address&quot;:&quot;005056992b74&quot;)&quot; succeeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API Trace: GET /api/endpt -&gt; 200 OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API call &quot;GET /api/endpt?filter= (&quot;mac_address&quot;:&quot;00bb662266ff&quot;)&quot; succeeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API Trace: PUT /api/endpt/6773 -&gt; 200 OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API Trace: GET /api/endpt -&gt; 200 OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API call &quot;GET /api/endpt?filter= (&quot;mac_address&quot;:&quot;001a1e007c20&quot;)&quot; succeeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API Trace: GET /api/endpt -&gt; 200 OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API call &quot;GET /api/endpt?filter= (&quot;mac_address&quot;:&quot;00bb662266ff&quot;)&quot; succeeded</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019-08-19</td>
<td>10.2.100.88</td>
<td>oauth2:Nozomi</td>
<td>info</td>
<td>API Trace: GET /api/endpt -&gt; 200 OK</td>
</tr>
</tbody>
</table>