Hewlett Packard
Enterprise

HPE Security ArcSight DNS Malware Analytics

Software Version: 2.4

Getting Started Guide (Linux DCM)

February 8, 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only.

HPE Security ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

Follow this link to see a complete statement of copyrights and acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HPE Security ArcSight Technical Support Page: https://softwaresupport.hpe.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hpe.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

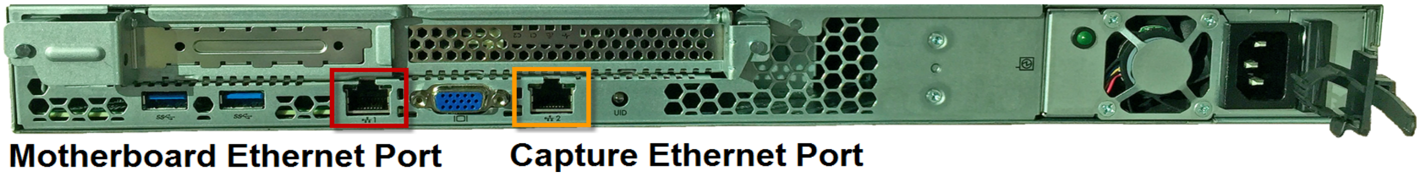
Install the DNS Capture Module

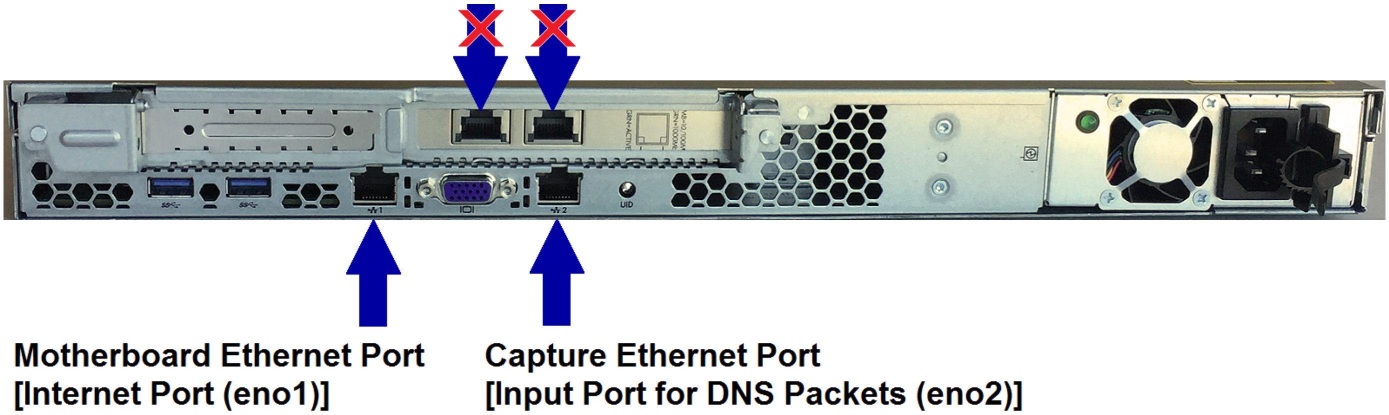
1. Mount the DNS Capture Module (DCM) in your server rack.

   See the rack-mounting instructions in the DCM packaging.

   If Issue: "TS01" on page 6

2. Configure your switch so that the TAP/SPAN port sends packets to the DCM.




Motherboard Ethernet Port
[Internet Port (eno1)]
Capture Ethernet Port
[Input Port for DNS Packets (eno2)]

3. Connect a CAT-6 RJ45 Ethernet cable from the TAP/SPAN/mirrored port of the switch to the DCM Capture Ethernet Port (port 2).

4. Connect a CAT-6 RJ45 Ethernet cable with Internet access to the DCM Motherboard Ethernet Port (port 1).

5. Plug the power cord into the DCM and power on the unit .

   Observe the following:

   - Red power button light – DCM is powered on and ready for service.

     If Issue: "TS02" on page 6

   - Green flashing light near Ethernet port #1 – Packet traffic is being received from the switch (Internet).

     If Issue: "TS03" on page 6

   - Green flashing light near motherboard Ethernet port – Suspicious packet traffic is being sent to the DNS Analytical Cloud.

     If Issue: "TS04" on page 6

Setup DNS Malware Analytics

1. Launch HPE - ArcSight DNS Malware Analytics from the Chrome web browser.

   Use the URL that was sent to you in the "Welcome" email.

2. Complete the **Company Information** and **User Information** fields and then click **Create Account**.

   If Issue: "TS05" on page 7

3. Accept the EULA.
4. See the regular documentation for operating in the DNS Malware Analytics Portal.
5. If there are any additional issues, see "TS06" on page 7.

Troubleshooting the installation and setup

TS01	The DCM may be damaged. Contact Technical Support for an assessment and a possible RMA.
TS02	The power cord may not be securely plugged into the DCM or into the power receptacle. If the power cord is correctly plugged into the DCM and power receptacle, the DCM power supply could be bad. Contact Technical Support for an assessment and a possible RMA.
TS03	Ensure that the cable is completely plugged into Ethernet Capture Port on the DCM. Next, ensure that the network switch is functioning and that the cable is completely plugged into the TAP port on this device. Finally, ensure that the cable and its connectors are not damaged.
TS04	Ensure that the cable is completely plugged into a motherboard Ethernet port on the DCM. Next, ensure that the cable and its connectors are not damaged. Finally, ensure that the cable is completely plugged into the switch handling live Internet traffic.

TS05	If you cannot access the Portal screens, then the 24-hour registration period may have expired. Contact Technical Support and request another invite email or a default login.
TS06	Further troubleshooting.

- If the DCM cannot access the Internet, contact your company's network IT engineer and do the following:
  - Verify that your DCM has been provided an IP address through DHCP.
  - When the DCM is turned on and connected, verify that its IP address can be seen on the Internet side of the firewall and, or on the router.
- If your company requires a fixed IP address, contact your company's network IT engineer and do the following:
  - Obtain the DCM administrative login and password from Technical Support.
  - Ensure that you met the conditions in TS01 – TS04.
  - Attach a Keyboard Video Mouse (KVM) to the DCM.
  - Log in to the Linux server system using the administration password that you obtained earlier.
  - Open a console window on the DCM and execute the ping command:

    ```
    $ ping 8.8.8.8
    ```

    If the DCM responds to a ping, then the module can access the Internet. If the DCM does not response to the ping, there may be a proxy issue. In this case, go to the next trouble shooting item.
- If you cannot access the Internet, there may be proxy issues that need to be addressed.

  ```
  http://YOUR PROXY URL HERE:Proxy Port Number
  ```

  Example: `http://mylittleproxypony.com:5020`
  - Obtain the DCM administrative login and password from Technical Support.
  - Obtain your company proxy URL and port number from your IT administrator.
  - Ensure that you met all the conditions in TS01 – TS04.
  - Attach a Keyboard Video Mouse (KVM) to the DCM.
  - Log in to the Linux server system using the administration password that you obtained earlier.
  - Edit the `/etc/profile.d/dmaenv.sh` file in order to add a proxy:
    i. Go to `/etc/profile.d`

       ```
       cd /etc/profile.d
       ```

    ii. Open `dmaenv.sh` with `vi` editor to add a proxy.

       ```
       vi dmaenv.sh
       ```

    iii. Start edit mode by pressing `i` on your keyboard.

    iv. Add your proxy in the file.

       Examples:

       ```
       export http_proxy=http://YOUR_PROXY:PORT_NUMBER
       export https_proxy=http://YOUR_PROXY:PORT_NUMBER
       ```

    v. Press **Escape** to enter command mode.

    vi. Write and quit from the file by typing `:wq` and pressing **Enter**.

    This permanently sets the proxy parameters.
  - Restart the DCM and verify that the DCM can access the Internet.
  - To test for Internet connectivity, open a console window on the DCM and execute the ping command:

    ```
    $ ping 8.8.8.8
    ```

    If the DCM responds to the ping, then the module can access the Internet. If the DCM does not respond to the ping, then contact Technical Support.

	• If any of the above troubleshooting items did not help the DCM gain access to the Internet, then log out of Linux and restart the DCM. If this does not correct matters, then contact Technical Support.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on Getting Started Guide (Linux DCM) (DNS Malware Analytics 2.4)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!