DHCP Integration

Contents

DHCP Integration 1
About DHCP 1
Requirements 1
Configure the DHCP Server 2
Install and Configure NXLog 3
Configure the Sensor 4

DHCP Integration

The ability to correlate the origin of an event detected by the Sensor with the IP address a host was using at the same time is the primary reason to collect DHCP logs. This document describes the process for forwarding DHCP logs to the VMware NSX Network Detection and Response for ingestion and processing.

About DHCP

The Dynamic Host Configuration Protocol (DHCP) is a UDP protocol that dynamically allocates IP addresses from a pool and reclaims them when they are no longer in use. Systems running Windows Server provide DHCP services in many environments.

Typically, you can forward system logs using *Windows Event Forwarding* (https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx) (WEF), however WEF does not support DHCP logs. Therefore you must deploy a third-party solution to collect and forward DHCP logs from Windows Servers. There are a number of solutions available: this document describes using *NXLog* (https://nxlog.co/).

Requirements

The following are required for integration:

- At least one Sensor deployed in either a Hosted or On-Premises environment.
- Configure the Windows Server 2016, 2012, or 2008 providing DHCP services to save DHCP logs.
- Download, install, and configure the *NXLog Community Edition* (https://nxlog.co/products/nxlog-community-edition/download).

  Note: There are other third-party solutions available to collect and forward DHCP logs from Windows Servers. You do not have to use *NXLog* (https://nxlog.co/).

- Configure the User Portal to ingest the DHCP data.

Configure the DHCP Server

Configuration Steps

Enable DHCP logging on the Windows Server 2016, 2012, or 2008.

Procedure

Step 1: Login to the server

Use an account with full administrator rights to login to the Windows Server.

Step 2: Access the DHCP MMC

From the Start button, select Programs → Administrative Tools → DHCP.

Note: The method of accessing the MMC may vary depending on the version of Windows Server you are using.

Step 3: Select DHCP properties

Expand the tree in the left pane of the DHCP window. If the DHCP servers are correctly configured, they will be listed here. Both IPv4 and IPv6 will be listed if you have enabled DHCP for multiple protocols.

Select the protocol you want logged, then right-click and select Properties.

Step 4: Enable logging

Ensure the Enable DHCP Audit Logging option is selected on the General tab of the Properties pop-up.

Click the OK button to dismiss the pop-up.

Step 5: Define the logging path

In the left pane of the DHCP window, select the DHCP server, then right-click and select Properties. In the Properties pop-up, check the Database Path option. Windows will save the DHCP logs in the defined directory. The default location is `C:\Windows\Sysnative\dhcp\` (`C:\Windows\System32\dhcp\` on 32-bit systems). You can change this location if desired.

The format of log filenames is `DhcpSrv-Log-`*`Xxx`*`.log` for IPv4 and `DhcpV6SrvLog-`*`Xxx`*`.log` for IPv6. The *`Xxx`* is the day of the week: `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, `Sat`, `Sun`.

Note: There are several limitations to the logs:

- The default weekly file size limit is 70 MB. Once the sum of all the log files exceeds 70 MB, the server stops logging until the next day.
- If the free disk space on the server disk falls below 20 MB, audit logging is halted. Logging resumes when the free space is greater than 20 MB.

  Modify the `HKLM\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\DhcpLogFilesMaxSize` key to increase the weekly file size limit.

Click the OK button to dismiss the pop-up. Close all the other windows by applying changes if prompted.

Install and Configure NXLog

Configuration Steps

Windows Event Forwarding (https://social.technet.microsoft.com/wiki/contents/articles/33895.windows-event-forwarding-survival-guide.aspx) does not support DHCP logs. To collect and forward DHCP logs from Windows Servers you must install a third-party solution. This document provides an overview of configuring *NXLog* (https://nxlog.co/).

Refer to the *NXLog documentation* (https://nxlog.co/docs/nxlog-ce/nxlog-reference-manual.html) for complete details.

Procedure

Step 1: Download and install NXLog

Download the *NXLog Community Edition* (https://nxlog.co/products/nxlog-community-edition/download). Install the application at `C:\Program Files (x86)\NXlog`.

Step 2: Configure NXLog

Edit the configuration file. Its default location is `C:\Program Files (x86)\NXlog\conf\nxlog.conf`.

```
define ROOT C:\Program Files (x86)\NXlog

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<Input DHCP_IN>
    Module      im_file
    # Located at this path (note escaped backslash, use glob)
```

```
    # Use System32 for 32-bit systems
    File        "C:\\Windows\Sysnative\\dhcp\\DhcpSrvLog-*.log"
    # Remember the last place in the log
    SavePos     TRUE
    # Each log is written to a single line
    InputType   LineBased
</Input>

<Output TCP_Out>
    # Send log by TCP
    Module      om_tcp
    # Output log as individual lines seperated by CRLF
    OutputType  LineBased
    # Send the log to this host
    Host        IP_ADDRESS
    # Send the log to this port
    Port        8080
</Output>

# associate input to output, skipping any processors
<Route DHCP_TO_TCP>
    Path        DHCP_IN => TCP_OUT
</Route>
```

IP_ADDRESS should be the address of the Sensor.

Step 3: Start the NXLog service

Refer to the *NXLog documentation* (https://nxlog.co/docs/nxlog-ce/nxlog-reference-manual.html) for instructions on starting the service. Configuration errors will be written to the `%LogFile%`.

The PORT NUMBER configured for the User Portal must match this PORT value.

Configure the Sensor

Configuration Steps

Once the Windows Server has been set up properly, the Sensor can be configured to ingest the DHCP logs.

Procedure

Step 1: Login to the Web UI

Using your Web browser, login to the User Portal at *https://user.lastline.com/* (https://user.lastline.com/) (for EMEA customers *https://user.emea.lastline.com/* (https://user.emea.lastline.com/)) for a hosted deployment or the Manager Web UI for an On-Premises installation.

Step 2: Navigate to the DHCP collection tab

From the Main navigation menu, click **[Admin]**. On the Admin page, select **[Data sources]** from left sidebar menu. Then on the Data sources page, click **[DHCP collection]**.

Step 3: Select an appliance

Click the **[Appliance:]** button and select the appropriate Sensor from the Select Appliance pop-up.

Step 4: Add a DHCP Collector

Click the **[+]** button to configure a collector in the DHCP COLLECTORS list. Fill in the following:

- Enter a NAME. This name uniquely identifies the data generator. This field is required. A string of lowercase characters is expected.
- The GENERATOR IP(S) field is optional. This is the IP address of the generator as seen by the collector (to enable firewall filtering). If set, the collector will only accept records from sources at the specified IP address(es). Any records from other IP addresses are discarded. If left unset, the collector will accept records sent from any IP address.
- Set the PORT NUMBER. This is the port on the sensor where the DHCP log data will be received. This field is required. It accepts values from 1024 to 65535.

When you are done, click SAVE.

Configuration Result

Saving the collector triggers a reconfiguration on the sensor, after which a DHCP ingestion process is ready to receive DHCP logs on the specified port number. The progress of the reconfiguration action can be followed on the Admin→Appliances→Monitoring logs tab.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com