

Deploying Managed Detection and Response windows Syslog forwarder (Beta)



Contents

Overview.....	3
Requirements	3
Download and install forwarder	4
Check service is running and ports are Open and Listening..	4

Overview

N-able has developed a Syslog forwarder to send logs in an encrypted format to the N-able MDR console. This is intended for customers who don't have or want to use virtualization to spin up a VM to forward logs to the console.

Requirements

The Syslog forwarder will preferably be installed on a windows server with a minimum of 4Gb and 4 cores. This will also be given a static IP.

Download and install the N-able MDR forwarded

Download the syslog forwarded usin the following link:
<https://eu-engineers.com/AdluminForwarderInstaller.msi>

Once downloaded open command prompt as administrator and run the following from the download location of the above MSI installer

```
msiexec /i AdluminForwarderInstaller.msi tenant=TENANT_ID_CODE_HERE
```

the TENANT ID you will get from the N-able MDR console see below:

Obtain the MDR tenant ID

- The *MDR tenant ID* is a unique code that will associate the devices with a particular tenant in MDR within N-able MDR partner level, choose the customer you want the Tenant ID for, go to the downloads sections.

Tenant Data	
Name	N-able Demo (2023-11-03)
Tenant ID	194369df-598a-412f-bdcc-c101a467678b-02e2e8dd-643c-4747-9bce-4a25022f014e

Once succesfully run this will create a Windows service. However, The service is not a typical windows service; it is unable to let Windows know when it has successfully started like most services do, so it will never show as “running” within the Services app. The purpose of running it as a service is its auto-start feature, allowing the forwarder to start after rebooting.

When installed, it will spawn multiple processes for the respective ports it is listening on as seen below


Background processes (167)

- > ☐ Acrobat Update Service
- ☒ Adlumin Forwarder
- ☒ Adlumin Forwarder
- ☒ Adlumin Forwarder
- ☒ Admin By Request

0%	0.3 MB	0 MB/s	0 Mbps	0%
0%	30.6 MB	0 MB/s	0 Mbps	0%
0%	0.5 MB	0 MB/s	0 Mbps	0%
0%	1.1 MB	0 MB/s	0 Mbps	0%
0%	19.6 MB	0 MB/s	0 Mbps	0%

Very low	Very low
Very low	Very low
Very low	Very low
Very low	Very low
Very low	Very low

Once installed, ensure it works by navigating to a log file called adlumin forwarder found in c:\windows\system32 as seen below. It will show the ports it is listening on.


adlumin_forwarder
 C:\Windows\System32

Type: Text Document
 Date modified: 2/1/2024 11:20 PM
 Size: 207 bytes

adlumin_forwarder - Notepad

File Edit Format View Help

```

2024-02-01 23:20:22,766 Adlumin syslog forwarder version 2.1.3W starting up...
2024-02-01 23:20:22,766 Authenticating tenant ID 3da078c5-b62f-4f59-bb1a-d75713cbbf21-d32b6e05-9a0e-4ce3-b540-0180c4d39320...
2024-02-01 23:20:23,459 Authentication successful!
2024-02-01 23:20:23,607 Excluding Adlumin IP addresses: ['35.155.54.98', '44.232.42.82']
2024-02-01 23:20:23,607 Excluding own IP address: 10.255.252.111
2024-02-01 23:20:23,608 Loaded data from configuration file.
2024-02-01 23:20:23,608 Tenant ID: 3da078c5-b62f-4f59-bb1a-d75713cbbf21-d32b6e05-9a0e-4ce3-b540-0180c4d39320
2024-02-01 23:20:23,608 Forwarding endpoints: ['https://master-ingest-1.securityeco.com']
2024-02-01 23:20:23,619 Kinesis dependencies successfully loaded; inserting events directly into stream...
2024-02-01 23:20:23,699 (vpn) Listening for UDP connections on 0.0.0.0:20001
2024-02-01 23:20:23,699 (firewall) Listening for UDP connections on 0.0.0.0:20000
2024-02-01 23:20:23,699 (misc1) Listening for UDP connections on 0.0.0.0:20002
2024-02-01 23:20:23,699 (misc2) Listening for UDP connections on 0.0.0.0:20003
2024-02-01 23:20:23,700 (misc4) Listening for UDP connections on 0.0.0.0:30003
2024-02-01 23:20:23,700 (misc3) Listening for UDP connections on 0.0.0.0:30002
2024-02-01 23:20:23,700 (misc5) Listening for UDP connections on 0.0.0.0:30005
2024-02-01 23:20:23,700 (misc7) Listening for UDP connections on 0.0.0.0:30007
2024-02-01 23:20:23,700 (misc6) Listening for UDP connections on 0.0.0.0:30006
2024-02-01 23:20:23,701 (misc9) Listening for UDP connections on 0.0.0.0:30009
2024-02-01 23:20:23,700 (misc8) Listening for UDP connections on 0.0.0.0:30008
2024-02-01 23:20:23,701 (misc10) Listening for UDP connections on 0.0.0.0:30010
2024-02-01 23:20:23,701 (carbonblack) Listening for UDP connections on 0.0.0.0:20005
2024-02-01 23:20:23,701 (carbonblack_defense) Listening for UDP connections on 0.0.0.0:20006
2024-02-01 23:20:23,701 (network_security_device) Listening for UDP connections on 0.0.0.0:514
2024-02-01 23:20:23,701 (darktrace) Listening for UDP connections on 0.0.0.0:20007
2024-02-01 23:20:23,702 (network_security_device) Listening for UDP connections on 0.0.0.0:30000
2024-02-01 23:20:23,702 (endpoint_security) Listening for UDP connections on 0.0.0.0:30001
2024-02-01 23:20:23,702 (sophos) Listening for UDP connections on 0.0.0.0:31000
2024-02-01 23:20:23,702 (crowdstrike) Listening for UDP connections on 0.0.0.0:32000
2024-02-01 23:20:23,702 (hpux) Listening for UDP connections on 0.0.0.0:40001
2024-02-01 23:20:23,703 (office365) Listening for UDP connections on 0.0.0.0:45000
2024-02-01 23:20:23,703 (aix) Listening for UDP connections on 0.0.0.0:40002

```

With ports not active and listening you can configure your syslogs to be sent to these ports, where we will encrypt the logs and ensure they are sent to your partner tenant within the N-able MDR console.