Contents

Introduction

This document describes how to enable AnyConnect Network Access Manager (NAM) logging as well as to collect and interpret the logs. The examples included in the document describe different authentication scenarios and the logs that reflect the steps taken by Network Access Manager to authenticate the client.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Enable NAM Logging

If an issue is identified that may be related to NAM module, the first step is to enable Extended Logging feature. This must be done on the client endpoint while NAM module is running.

Step 1. Open AnyConnect window and make sure it's in focus.

Step 2. Press this key combination, **Left Shift + Left Alt + L**. There is no response.

Step 3. Right click on AnyConnect icon in Windows System Tray. A menu pops up.

Step 4. Select **Extended Logging** so it has a check mark displayed. NAM now logs detailed

debug messages.

Configure NAM Packet Capture

When Extended Logging is enabled, NAM also keeps a packet capture buffer going. The buffer is by default limited to about 1MB. If packet capture is needed, it may be beneficial to increase buffer size so it captures more activities. To extend the buffer, a XML setting file must be manually modified.

Step 1. On the Windows PC, browse to:
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system

Step 2. Open file **internalConfiguration.xml**.

Step 3. Locate XML tag <packetCaptureFileSize>1</packetCaptureFileSize> and adjust the value to 10 for a 10MB buffer size, and so on.

Step 4. Reboot the client PC for the change to take effect.

Log Collection

NAM log collection is done via Diagnostic And Reporting Tool (DART), which is a module of AnyConnect suite. In the installer, select a module and use AnnyConnect full installation ISO to install. The Cisco Media Services Interface (MSI) installer can also be found inside the ISO.

After you enable Extended Logging and perform a test, simply run DART and go through the dialogue, the log bundle is located by default on the Windows Desktop.

In addition to DART bundle, the NAM message log is also helpful to locate the relevant data in the NAM log. In order to find the NAM message log, navigate to **AnyConnect settings window > Network Access Manager > Message History**. The message log contains timestamp of each network connection event, which can be used to find the logs relevant to the event.

Reading NAM Logs

NAM logs, especially after you enable Extended Logging, contains a large amount of data, most of which are irrelevant and can be ignored. This section lists out the debug lines to demonstrate each step NAM takes to establish a network connection. When you work through a log, these key phrases may be helpful to locate part of the log relevant to the issue.

Log Summary of a Network Connection without 802.1x Enabled Authentication

Explanation: This indicates that the user has selected a network from NAM module, and NAM has received a **userEvent** of **START**.

Explanation: Both Access State Machine and Network State Machine have been started.

Explanation: The IPv4 instance got **cancelled** in order to reset the states.

Explanation: The adapter with ID **484E4FEF-392C-436F-97F0-CD7206CD7D48** was selected to connect to network **test123**, which is the name of the network connection configured in NAM.

Explanation: NAM has successfully engaged the adapter for this network. Now NAM tries to associate (connect) to this network (which happens to be wireless):

Explanation: **openNoEncryption** indicates that the network is configured as open. On the Wireless Lan Controller it uses MAC Authentication Bypass (MAB) to authenticate.

Explanation: **cs** can be seen a lot in NAM logs. These are irrelevant logs and should be ignored.

Explanation: These are Simple Object Access Protocol (SOAP) messages used to tell AnyConnect GUI to display the connection status message such as **Associating** in this case. Any error messages displayed on NAM window can be found in one of the SOAP messages in the log which can be used to locate the issue easily.

Explanation: NAM receives an **AUTH_SUCCESS** event, which misleads because there is no authentication which currently happened. You are get this event simply because you connect to an open network, so by default authentication is successful.

Explanation: Association to Service Set Identifier (SSID) is successful, time to handle authentication.

Explanation: Since this is an open network, it is by default authenticated. At this point, NAM is connected to the network and now starts DHCP process:

Explanation: NAM successfully acquires an IP address.

Explanation: Once an IP address is received NAM will send ARP (A**Get-Connectivity**). Once the ARP response is received the client is connected.

Log Summary of a Network Connection using 802.1x and PEAP over Wired Network

Explanation: NAM started to connect to network **WiredPEAP**.

Explanation: NAM matched an adapter to this network.

Explanation: NAM started connecting to this wired network.

Explanation: Client sends **EAPOL_START**.

Explanation: Client receives Identity Request from the switch, it now looks for a credential to send back.

Explanation: By default, Anyconnect sends **anonymous** as unprotected identity (**outter identity**), so here it tries **anonymous** and see if the server is OK with it. The fact that the identity is **anonymous** as opposed to **host/anonymous** indicates that it's a user authentication, rather than

machine authentication.

Explanation: RADIUS server sends an Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) frame without any content. Its purpose is to negotiate EAP-TLS protocol with the client.

Explanation: NAM recognizes server's request to use EAP-TLS but the client is configured to use Protected Extensible Authentication Protocol (PEAP). This is the reason that NAM sends back a counter-offer for PEAP.

Explanation: RADIUS server accepts the outter/unprotected identity.

Explanation: The **Protected** portion of PEAP (to establish a secure tunnel to exchange inner credentials) starts, after client receives a confirmation from RADIUS server to continue the use of PEAP.

Explanation: NAM sends a client hello encapsulated in EAP message and waits for server hello to come. The server's hello contains ISE certificate, so it takes some time to finish transferring.

Explanation: NAM extracted the subject name of the ISE server from server certificate. Since it doesn't have server certificate installed in the trust store, you do not find it there.

Explanation: NAM looks for the **inner/protected** identity to be sent to RADIUS server after tunnel is established. In this case, "**Automatically use my Windows logon name and password**" option has been enabled on the wired adapter, so NAM uses windows logon credentials instead of asking the user for it.

Explanation: NAM sent client key and cipher spec to server and received confirmation. SSL negotation is successful and a tunnel is established.

Explanation: Protected identity is sent to the server, who accepts the identity. Now server requests password.

Explanation: NAM receives password request and sends password to server.

Explanation: Server receives the password, verifies it and sends EAP-Success. Authentication is successful at this point, and client proceeds as it gets the IP address from DHCP.