# 目次



# 概要

この資料に AnyConnect ネットワーク アクセス マネージャ（NAM）ロギングを有効に し、またログを集め解読する方法を記述されています。 資料に含まれている例はクライアントを認証するためにネットワーク アクセス マネージャが踏むステップを反映するログおよび異なる認証シナリオを記述します。

# 前提条件

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

# NAM ロギングを有効に して下さい

NAM モジュールと関連しているかもしれない問題が識別されれば第一歩は拡張ログ記録機能を有効に することです。 これはクライアント エンドポイントで NAM モジュールが動作している間する必要があります。

ステップ 1. AnyConnect ウィンドウを開き、確かめて下さいフォーカスにあることを。

ステップ 2.このキーコンビネーションを、**左シフト + 去りました Alt + L.**押して下さい。 無応答

があります。

ステップ 3. Windows システムトレイの AnyConnect アイコンの右クリック。 メニューはポップアップします。

ステップ 4.**拡張記録を**選択して下さいそうすればチェックマークを表示するもらいます。 NAM は今詳しいデバッグ メッセージを記録 します。

# NAM パケットキャプチャを設定して下さい

拡張ロギングが有効に なるとき、NAM はまたパケットキャプチャ バッファ行を保存します。 バッファは 1MB にデフォルトで約制限されます。 パケットキャプチャが必要である場合、バッファサイズを増加することは有利であるより多くのアクティビティをキャプチャ します。 バッファを伸ばすために、XML 設定ファイルは手動で修正する必要があります。

ステップ 1： Windows PC で、に参照して下さい:
**C:\ProgramData\Cisco\Cisco AnyConnect セキュアな機動性 クライアント\ネットワーク アクセス マネージャ\システム**

ステップ 2.ファイルを開く **internalConfiguration.xml。**

ステップ 3. XML タグ <packetCaptureFileSize>1</packetCaptureFileSize> を見つけ、10 に 10MB バッファサイズのために値を、等合わせて下さい。

ステップ 4.実施されるために変更のためのクライアントPC をリブートして下さい。

# 収集を記録 して下さい

NAM ログ 収集は AnyConnect スイートのモジュールである診断およびレポーティング ツール（投げ矢）でされます。 インストーラで、モジュールを選択し、インストールするのに AnnyConnect 完全なインストール ISO を使用して下さい。 Ciscoメディア サービス インターフェイス（MSI）インストーラはまた ISO の中で見つけることができます。

拡張ロギングを単に有効に した、テストを行い、投げ矢を実行し、ダイアログを通過する後、ログ バンドルはウィンドウズ の デスクトップにデフォルトであります。

投げ矢バンドルに加えて、NAM メッセージ ログは NAM ログで関連データを見つけてまた有用です。 NAM メッセージ ログを、ナビゲート **AnyConnect Settings ウィンドウ > ネットワーク アクセス マネージャ > メッセージ ヒストリ**に見つけるため。 メッセージ ログはログをイベントに関連した見つけるのに使用することができる各ネットワーク接続 イベントのタイムスタンプが含まれています。

# NAM ログを読むこと

NAM は特に拡張ロギングを有効に した後、含まれていますほとんどが関係がなく、無視することができる多量のデータが記録 します。 このセクションは各ステップ NAM を示すためにデバッグ行を奪取 します ネットワーク接続を確立するためにリストします。 ログによってはたらくとき、これらのキー句は問題に関連したログの一部を見つけて有用かもしれません。

## 802.1X によって有効に される 認証なしでネットワーク接続の概略を記録 して下さい

説明： これはユーザが NAM モジュールからネットワークを選択した、NAM は**開始する**の userEvent 受け取りましたことを示し。

説明： アクセス両方状態マシンおよびネットワーク状態 マシンは始動されました。

説明： 得られた IPv4 例は状態をリセットするために**取り消しました**。

説明： ID **484E4FEF-392C-436F-97F0-CD7206CD7D48** のアダプタは NAM で設定されるネットワーク接続の名前であるネットワーク **test123** に接続するために選択されました。

説明： NAM は正常にこのネットワークのためのアダプタを実行しました。 この場合 NAM は関連付けることをワイヤレスであることを起こる）に（接続する）このネットワーク（試みます:

説明： **openNoEncryption は**ネットワークが開いたで設定されることを示します。 ワイヤレス LAN コントローラでそれは MAC 認証 バイパス（MAB）を認証するのに使用します。

説明： **CS は** NAM ログでたくさん見られる場合があります。 これらは関係がない口グで、無視する必要があります。

説明： これらは AnyConnect GUI をこの場合**関連付け**のような接続ステータス メッセージを表示するように言うのに使用されるシンプル オブジェクト アクセスプロトコル（石鹸）メッセージです。 NAM ウィンドウで表示するどのエラーメッセージでも問題を容易に見つけるのに使用することができる口グの石鹸メッセージの 1 つで見つけることができます。

説明： NAM は現在起こった認証がないので誤解する **AUTH_SUCCESS** イベントを受け取ります。 オープンネットワークに接続するので単に得ますこのイベントを、そうデフォルトで認証成功していますあります。

説明： Service Set Identifier （SSID）へのアソシエーションは成功しています、時間を計ります認証を処理するために。

説明： これはオープンネットワークであるので、デフォルトで認証されます。 この時点で、NAM はネットワークに接続され、今 DHCPプロセスを開始します:

説明： NAM は IP アドレスの取得に成功します。

説明： IP アドレスが受け取られれば NAM はゲートウェイ（得**接続**）に ARP （アドレス解決プロトコル

## 802.1X を使用してネットワーク接続および有線ネットワーク上の PEAP の概略を記録 して下さい

説明： NAM はネットワーク **WiredPEAP** に接続し始めました。

説明： NAM はこのネットワークにアダプタを一致させました。

説明： この有線ネットワークに NAM によって開始される接続。

説明： クライアントは **EAPOL_START を**送信 します。

説明： クライアントはスイッチから送信するために Identity 要求を、それ今探します 資格情報を受け取ります。

説明： デフォルトで、Anyconnect は無防備識別（**outter 識別**）として**匿名を**、そうここにそれ試み、**匿名を**サーバがそれと良いかどうか見ます送信 します。 識別が**ホスト**に対して**匿名/匿名**であるというファクトはマシン 認証よりもむしろそれがユーザ認証であることを、示します。

説明： RADIUSサーバはコンテンツなしで拡張可能認証プロトコル転送する 層 セキュリティ（EAP-TLS）フレームを送信 します。 その目的はクライアントと EAP-TLS プロトコルをネゴシエートすることです。

説明： NAM は EAP-TLS を使用するためにサーバの要求を認識しますが、クライアントは Protected Extensible Authentication Protocol （PEAP）を使用するために設定されます。 これは NAM が PEAP のためのカウンターオファーを送返すという原因です。

説明： RADIUSサーバは outter/無防備識別を受け入れます。

説明： PEAP の**保護された**部分は（セキュアトンネルを内部資格情報を交換するために確立するため）PEAP の使用を続けるためにクライアントが RADIUSサーバから確認を受け取った後、開始します。

説明： NAM は EAP メッセージでカプセル化されるクライアント HELLO を送信 し、来るためにサーバHello を待っています。 サーバの HELLO は ISE 認証が含まれています、従って転送することを終わる時間かかります。

説明： NAM はサーバ証明から ISE サーバのサブジェクト名を得ました。 それに信頼ストアにインストールされるサーバ証明がないのでそれをそこに見つけません。

説明： NAM はトンネルが確立された後 RADIUSサーバに送信 されるべき**内部の/保護された**識別を探します。 この場合、「**自動的に Windows ログオン名前を使用すればパスワード**」オプションは配線されたアダプタで有効に なりました、従って NAM はそれをユーザに頼むかわりにウィンドウ ログオン クレデ ンシャルを使用します。

説明： NAM はサーバに Client 鍵暗号 spec を送り、確認を受け取りました。 SSL ネゴシエーションは正常であり、トンネルは確立されます。

説明： 識別を受け入れる保護された識別はサーバに送信 されます。 この場合 Server 要求 パスワード。

説明： NAM は Password 要求を受け取り、サーバにパスワードを送ります。

説明： サーバはパスワードを受け取り、確認し、EAP 成功を送信 します。 認証はこの時点で正常であり、クライアントは DHCP からそれとして得ます IP アドレスを続行します。