Contenu

Introduction

Ce document décrit comment activer le gestionnaire d'accès au réseau d'AnyConnect (NAM) se connectant aussi bien que collecter et interpréter les logs. Les exemples inclus dans le document décrivent les différents scénarios d'authentification et les logs qui reflètent les étapes prises par le gestionnaire d'accès au réseau pour authentifier le client.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Se connecter de l'enable NAM

Si on identifie une question qui peut être liée au module NAM, la première étape est d'activer la fonctionnalité de journalisation étendue. Ceci doit être fait sur le point final de client tandis que le module NAM s'exécute.

Étape 1. Ouvrez la fenêtre d'AnyConnect et assurez-vous qu'elle est au foyer.

Étape 2. Appuyez sur cette combinaison de touches, **déplacement gauche + a laissé l'Alt + le L.** Il n'y a aucune réponse.

Étape 3. Clic droit sur l'icône d'AnyConnect dans la barre d'état de système Windows. Un menu s'affiche.

Étape 4. Sélectionnez **se connecter étendu** ainsi il fait afficher un coche. NAM se connecte maintenant les messages de débogage détaillés.

Configurez la capture de paquet NAM

Quand se connecter étendu est activé, NAM garde également aller de mémoire tampon de capture de paquet. La mémoire tampon est par défaut limité environ à 1MB. Si la capture de paquet est nécessaire, il peut être salutaire d'augmenter la taille de mémoire tampon ainsi elle capture plus d'activités. Pour étendre la mémoire tampon, un fichier de configuration XML doit être manuellement modifié.

Étape 1. Sur le PC Windows, parcourez à :
**Client de mobilité de C:\ProgramData\Cisco\Cisco AnyConnect \ gestionnaire \ système sécurisés d'accès au réseau **

Étape 2. Fichier ouvert **internalConfiguration.xml.**

Étape 3. Localisez la balise <packetCaptureFileSize>1</packetCaptureFileSize> XML et ajustez la valeur à 10 pour une taille de mémoire tampon 10MB, et ainsi de suite.

Étape 4. Redémarrez le PC client pour la modification pour le prendre effet.

Collecte de log

La collecte de log NAM est faite par l'intermédiaire du diagnostic et de l'outil de génération de rapports (DART), qui est un module de suite d'AnyConnect. Dans l'installateur, sélectionnez un module et employez la pleine OIN d'installation d'AnnyConnect pour installer. L'installateur de l'interface de services de médias de Cisco (MSI) peut également être trouvé à l'intérieur de l'OIN.

Après que vous activiez se connecter étendu et réalisiez un essai, exécutiez simplement le DART et passiez par le dialogue, le paquet de log se trouve par défaut sur le bureau Windows.

En plus du paquet de DART, le journal des messages NAM est également utile de localiser les données appropriées dans le log NAM. Afin de trouver le journal des messages NAM, naviguez vers l'**historique de fenêtre de configurations d'AnyConnect > de gestionnaire > de message d'accès au réseau**. Le journal des messages contient l'horodateur de chaque événement de connexion réseau, qui peut être utilisé pour trouver les logs concernant l'événement.

Lecture des logs NAM

NAM se connecte, particulièrement après que vous activez se connecter étendu, contient un grand nombre de données, plus dont soyez inutile et pouvez être ignoré. Cette section répertorie les lignes de débogage pour expliquer chaque étape NAM prend pour établir une connexion réseau. Quand vous travaillez par un log, ces phrases clés peuvent être utiles de placer une partie du log concernant la question.

Connectez-vous le résumé d'une connexion réseau sans authentification activée par 802.1x

Explication : Ceci indique que l'utilisateur a sélectionné un réseau de module NAM, et NAM a reçu un **userEvent du DÉBUT**.

Explication : L'ordinateur de condition d'accès Et l'ordinateur d'état de réseau ont été démarrés.

Explication : L'exemple d'ipv4 obtenu **s'est annulé** afin de remettre à l'état initial les états.

Explication : L'adaptateur avec l'ID **484E4FEF-392C-436F-97F0-CD7206CD7D48** a été sélectionné pour se connecter au réseau **test123**, qui est le nom de la connexion réseau configurée dans NAM.

Explication : NAM a avec succès engagé l'adaptateur pour ce réseau. Maintenant essais NAM à s'associer (se connecter) à ce réseau (qui s'avère justement être Sans fil) :

Explication : **l'openNoEncryption** indique que le réseau est configuré comme ouvert. Sur le contrôleur Sans fil de réseau local il utilise la dérivation d'authentification MAC (MAB) pour authentifier.

Explication : **le Cs** peut être vu beaucoup dans des logs NAM. Ce sont les logs inutiles et devraient être ignorés.

Explication : Ce sont des messages de protocole simple d'Access d'objet (SAVON) utilisés pour dire le GUI d'AnyConnect d'afficher le message d'état de la connexion tel qu'**associer** dans ce cas. Tous les messages d'erreur affichés sur la fenêtre NAM peuvent être trouvés dans un des messages de SAVON dans le log qui peut être utilisé pour localiser la question facilement.

Explication : NAM reçoit un événement **AUTH_SUCCESS**, qui trompe parce qu'il n'y a aucune authentification qui s'est actuellement produite. Vous êtes obtenez cet événement simplement parce que vous vous connectez à un réseau ouvert, ainsi par l'authentification par défaut êtes réussi.

Explication : L'association à l'Identifiant SSID (Service Set Identifier) est réussie, chronomètrent pour manipuler l'authentification.

Explication : Puisque c'est un réseau ouvert, il est par défaut authentifié. En ce moment, NAM est connecté au réseau et commence maintenant le processus DHCP :

Explication : NAM saisit avec succès une adresse IP.

Explication : Une fois qu'une adresse IP est reçue NAM enverra la demande d'ARP (Address Resolution Protocol passerelle (Obtenir-**Connectivité**). Une fois que la réponse d'ARP est reçue le client est connecté.

Connectez-vous le résumé d'une connexion réseau utilisant le 802.1x et le PEAP au-dessus du réseau câblé

Explication : NAM commencé pour se connecter au réseau **WiredPEAP**.

Explication : NAM a apparié un adaptateur à ce réseau.

Explication : Se connecter commencé par NAM à ce réseau câblé.

Explication : Le client envoie **EAPOL_START**.

Explication : Le client reçoit la demande d'identité du commutateur, il recherche maintenant un laisser-passer pour renvoyer.

Explication : Par défaut, Anyconnect envoie **anonyme** en tant qu'identité non protégée (**identité externe**), tellement ici il essaye **anonyme** et voit si le serveur est BIEN avec lui. Le fait que l'identité est **anonyme** par opposition à l'**hôte/anonyme** indique que c'est une authentification de l'utilisateur, plutôt que l'authentification de machine.

Explication : Le serveur de RAYON envoie une trame de Layer Security de Protocol-transport d'authentification extensible (EAP-TLS) sans n'importe quel contenu. Son but est d'être en pourparlers le protocole d'EAP-TLS avec le client.

Explication : NAM identifie la demande du serveur d'utiliser l'EAP-TLS mais le client est configuré pour utiliser le Protected Extensible Authentication Protocol (PEAP). C'est la raison pour laquelle NAM renvoie un contre-offre pour le PEAP.

Explication : Le serveur de RAYON reçoit identité externe/non protégée.

Explication : La partie **protégée de** débuts PEAP (pour établir un tunnel sécurisé pour permuter les qualifications intérieures), après que le client reçoive une confirmation du serveur de RAYON pour continuer l'utilisation du PEAP.

Explication : NAM envoie un client bonjour encapsulé dans le message d'EAP et attend le serveur bonjour pour être livré. Le serveur bonjour contient le certificat ISE, ainsi cela prend un certain temps de terminer transférer.

Explication : NAM a extrait le nom du sujet du serveur ISE du certificat de serveur. Puisqu'il n'a pas le certificat de serveur installé dans la mémoire de confiance, vous ne la trouvez pas là.

Explication : NAM recherche identité **intérieure/protégée** à envoyer au serveur de RAYON après que le tunnel soit établi. Dans ce cas, « **utilisez automatiquement mon nom de connexion de Windows et l'**option de **mot de passe** » a été activée sur l'adaptateur de câble, ainsi les fenêtres d'utilisations NAM ouvrent une session des qualifications au lieu de demander à l'utilisateur lui.

Explication : Clé de client et spécification de chiffrement envoyées par NAM au serveur et à la confirmation reçue. La négociation SSL est réussie et un tunnel est établi.

Explication : L'identité protégée est envoyée au serveur, qui reçoit l'identité. Maintenant le serveur demande le mot de passe.

Explication : NAM reçoit la demande de mot de passe et envoie le mot de passe au serveur.

Explication : Le serveur reçoit le mot de passe, le vérifie et envoie l'Eap-succès. L'authentification est réussie en ce moment, et le client poursuit pendant qu'elle obtient l'adresse IP du DHCP.