Содержание

Введение

Этот документ описывает, как включить Менеджеру доступа к сети (NAM) AnyConnect, регистрирующему, а также собрать и интерпретировать журналы. Примеры, включенные в документ, описывают другие опознавательные сценарии и журналы, которые отражают шаги, сделанные Менеджером Доступа к сети для аутентификации клиента.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Включите Регистрацию NAM

Если проблема определена, который может быть отнесен к модулю NAM, первый шаг должен включить Расширенную Характеристику входа в систему. В то время как модуль NAM работает, это должно быть сделано на клиентской оконечной точке.

Шаг 1. Открытое окно AnyConnect и удостоверяется, что находится в фокусе.

Шаг 2. Нажмите это сочетание клавиш, **Сдвиг влево + Левый Alt + L**. Нет никакого ответа.

Шаг 3. Щелкните правой кнопкой по значку AnyConnect в Лотке Системы Windows. Меню появляется.

Шаг 4. Выберите **Extended Logging**, таким образом, ему отобразили метку выбора. NAM теперь регистрирует подробные сообщения отладки.

Настройте захват пакета NAM

Когда Расширенная Регистрация включена, NAM также поддерживает буферное движение захвата пакета. Буфер по умолчанию ограничен приблизительно 1 МБ. Если захват пакета необходим, это может быть выгодно для увеличения размера буфера , таким образом, это перехватывает больше действий. Для расширения буфера файл значения XML должен вручную модифицироваться.

Шаг 1. На Компьютере с операционной системой Windows перейдите к:
C : \ProgramData\Cisco\Cisco AnyConnect безопасная мобильность доступ Client\Network Manager\system

Шаг 2. Открытый файл **internalConfiguration.xml**.

Шаг 3. Найдите XML-тэг <packetCaptureFileSize> 1 </packetCaptureFileSize> и отрегулируйте значение к 10 для размера буфера 10 МБ и так далее.

Шаг 4. Перезагрузите клиентский компьютер для изменения для вступления в силу.

Регистрационный набор

Набор журнала NAM сделан через Диагностику и средство создания отчетов (DART), которая является модулем комплекта AnyConnect. В установщике выберите модуль и используйте полную установку AnnyConnect ISO для установки. Интерфейс Cisco Media Services (MSI) установщик может также быть найден в ISO.

После того, как вы включаете Расширенную Регистрацию и выполняете тест, просто выполните DART и пройдите диалог, регистрационная связка (bundle) расположена по умолчанию на Настольном ПК со средой Windows.

В дополнение к связке (bundle) DART журнал сообщений NAM также полезен для определения местоположения существенных данных в журнале NAM. Для обнаружения журнала сообщений NAM перейдите к **окну настроек AnyConnect>, Менеджер Доступа к сети> передает Историю**. Журнал сообщений содержит метку времени каждого события сетевого подключения, которое может использоваться для обнаружения журналов относящимися к событию.

Чтение журналов NAM

Журналы NAM, особенно после включения Расширенной Регистрации содержат большое количество данных, большинство которых не важно и может быть проигнорировано. Этот

раздел перечисляет линии отладки, чтобы продемонстрировать , что каждый NAM шага берет для установления сетевого подключения. Когда вы работаете через журнал, эти ключевые фразы могут быть полезными для определения местоположения части журнала, относящегося к проблеме.

Регистрируйте сводку сетевого подключения без включенной аутентификации 802.1x

Пояснение: Это указывает, что пользователь выбрал сеть от модуля NAM, и NAM получил **userEvent ЗАПУСКА**.

Пояснение: Обе Машины Механизма состояний и Состояния сети Доступа были запущены.

Пояснение: экземпляр IPv4 был **отменен** для сброса состояний.

Пояснение: адаптер с **ID 484E4FEF-392C-436F-97F0-CD7206CD7D48** был выбран для соединения с сетью **test123**, который является названием сетевого подключения, настроенного в NAM.

Пояснение: NAM успешно затронул адаптер для этой сети. Теперь NAM пытается связаться (соединяются) с этой сетью (который, оказывается, радио):

Пояснение: **openNoEncryption** указывает, что сеть настроена как открытая. На Контроллере беспроводной локальной сети это использует Обход проверки подлинности MAC (MAB) для аутентификации.

Пояснение: **cs** может быть замечен много в журналах NAM. Они - несоответствующие журналы и должны быть проигнорированы.

Пояснение: Это сообщения Простого протокола доступа к объектам (SOAP), используемые, чтобы сказать GUI AnyConnect отображать сообщение статуса соединения, такое как **Соединение** в этом случае. Любые сообщения об ошибках, отображенные на окне NAM, могут быть найдены в одном из сообщений SOAP в журнале, который может использоваться для определения местоположения проблемы легко.

Пояснение: NAM получает событие **AUTH_SUCCESS**, которое вводит в заблуждение, потому что нет никакой аутентификации, которая в настоящее время происходила. Вы, получают это событие просто, потому что вы соединяетесь с открытой сетью, таким образом, проверкой подлинности по умолчанию успешно.

Пояснение: Ассоциация к идентификаторам наборов сервисов (SSID) успешна, время для обработки аутентификации.

Пояснение: Так как это - открытая сеть, она по умолчанию аутентифицируется. На этом этапе NAM связан с сетью и теперь запускает процесс DHCP:

Пояснение: NAM успешно получает IP-адрес.

Пояснение: Как только IP-адрес является полученным NAM, передаст ARP (протокол разрешения адресов) **(Получать-подключение)**. Как только ответ ARP получен, клиент связан.

Регистрируйте Сводку Сетевого подключения с помощью 802.1x и PEAP по Проводной сети

Пояснение: NAM начал соединяться с **сетью WiredPEAP**.

Пояснение: NAM совпал с адаптером к этой сети.

Пояснение: NAM начал соединяться с этой проводной сетью.

Пояснение: Клиент передает **EAPOL_START**.

Пояснение: Клиент получает Идентификационный Запрос от коммутатора, он теперь ищет учетные данные для передачи обратно.

Пояснение: По умолчанию Anyconnect передает **анонимный** как незащищенная идентичность (**внешняя идентичность**), таким образом, здесь это пробует **анонимный**, и посмотрите, соглашается ли сервер с ним. Факт, что идентичность является **анонимной** в противоположность **хосту / анонимная**, указывает, что это - проверка подлинности пользователя, а не аутентификация компьютера.

Пояснение: сервер RADIUS передает Transport Layer Security расширяемого протокола аутентификации (EAP-TLS) кадр без любого содержания. Его цель состоит в том, чтобы выполнить согласование о протоколе EAP-TLS с клиентом.

Пояснение: NAM распознает запрос сервера использовать EAP-TLS, но клиент настроен для использования Защищенного расширяемого протокола аутентификации (PEAP). Это - причина, что NAM передает встречное предложение обратно для PEAP.

Пояснение: сервер RADIUS принимает outter/unprotected идентичность.

Пояснение: **Защищенная** часть PEAP (для установления безопасного туннеля для обмена внутренними учетными данными) запускается, после того, как клиент получает подтверждение от сервера RADIUS для продолжения использования PEAP.

Пояснение: NAM передает сообщение приветствия клиента, инкапсулировавшее в сообщении EAP, и ждет приветствие сервера для прибытия. Сервер привет содержит сертификат ISE, таким образом, это занимает время, чтобы закончить передавать.

Пояснение: NAM извлек имя субъекта сервера ISE от серверного сертификата. Так как этому не установили серверный сертификат в базе доверенных сертификатов, вы не находите его там.

Пояснение: NAM ищет **внутреннюю/защищенную** идентичность, которая будет передаваться серверу RADIUS после того, как будет установлен туннель. В этом случае опция **"Automatically use my Windows logon name and password"** была включена на проводном адаптере, таким образом, NAM использует учетные данные начала сеанса окон вместо того, чтобы просить у пользователя его.

Пояснение: NAM передал клиентский ключ и спецификацию шифра к серверу и получил подтверждение. SSL negotation успешен, и туннель установлен.

Пояснение: Защищенная идентичность передается серверу, кто принимает идентичность.

Теперь пароль запросов к серверу.

Пояснение: NAM получает запрос пароля и передает пароль к серверу.

Пояснение: Сервер получает пароль, проверяет его и передает Успех EAP. Аутентификация успешна на этом этапе, и клиентские доходы, поскольку это получает IP-адрес от DHCP.