Версия 4.0 AnyConnect и агент положения NAC не появляются на руководстве устранения неполадок ISE

Содержание

Введение

Платформа Identity Services Engine (ISE) предоставляет возможности положения, которые требуют использования агента Network Admission Control (NAC) (для Microsoft Windows, Macintosh, или через webagent) или Версия 4.0 AnyConnect. Модуль положения ISE Версии 4.0 AnyConnect работает точно как агент NAC и поэтому упоминается как агент NAC в этом документе. Наиболее распространенный признак сбоя положения для клиента - то, что агент NAC не появляется, так как рабочий сценарий всегда заставляет окно агента NAC появляться и анализировать ваш ПК. Этот документ помогает вам сужать много причин, которые могут вести положение отказывать, что означает, что не появляется агент NAC. Это не предназначено, чтобы быть исчерпывающим, потому что журналы агента NAC могут только декодироваться Центром технической поддержки Cisco (TAC), и возможные основные причины являются многочисленными; однако, это стремится разъяснять, что ситуация и точно определять проблему далее, чем просто "агент не появляется с анализом положения" и вероятно поможет вам решать наиболее распространенные причины.

Предварительные условия

Требования

Сценарии, признаки и шаги, перечисленные в этом документе, записаны для вас для решения проблем после того, как будет уже завершена начальная настройка. Для начальной конфигурации обратитесь к Posture Services на Руководстве по конфигурации Cisco ISE на Cisco.com.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ISE Version1.2. x
- Агент NAC для версии 4.9 ISE. x
- Версия 4.0 AnyConnect

Примечание: Информация должна также быть применима к другим версиям ISE, пока Комментарии к выпуску не указывают на главные изменения в поведении.

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.

Методика устранения проблем

Что заставляет агента появиться?

Агент появляется, когда это обнаруживает узел ISE. Если агент снимает показания это, это не имеет полного доступа к сети и находится в сценарии перенаправления положения, это постоянно ищет узел ISE.

Там нас документ Cisco.com, который объясняет подробные данные процесса обнаружения агента: Процесс обнаружения Агента Network Admission Control (NAC) для платформы Identity Services Engine. Во избежание дублирования содержания этот документ только обсуждает ключевой момент.

Когда клиент соединяется, это подвергается Проверке подлинности RADIUS (фильтрация по MAC-адресам или 802.1x), в конце которого, ISE возвращает Список контроля доступа (ACL) перенаправления и URL перенаправления к сетевому устройству (коммутатор,

Устройство адаптивной защиты (ASA) или Контроллер беспроводной локальной сети) для ограничения трафика клиента, чтобы только позволить ему получать разрешения IP-адреса и Сервера доменных имен (DNS). Весь HTTP (S) трафик, который прибывает от клиента, перенаправлен к уникальному URL на ISE, который заканчивается **CPP** (Клиентское Положение и Настраивающий), кроме трафика, предназначенного к самому порталу ISE. Агент NAC передает обычный пакет GET HTTP к шлюзу по умолчанию. Если агент не получает ответа или какого-либо другого ответа, чем перенаправление CPP, он считает, что имеет полное подключение, и не продолжает положение. Если это получает Ответ HTTP, который является перенаправлением к URL CPP в конце определенного узла ISE, то это продолжает процесс положения и контакты тот узел ISE. Это только появляется и запускает анализ, когда это успешно получает подробные данные положения от того узла ISE.

Агент NAC также обращается к настроенному адресу IP - адреса хоста обнаружения (он не ожидает, что несколько будут настроены). Это ожидает быть перенаправленным там также для получения URL перенаправления с идентификатором сеанса. Если IP-адрес обнаружения является узлом ISE, то он не преследует, потому что он ждет, чтобы быть перенаправленным для получения правильного идентификатора сеанса. Таким образом, хост обнаружения не обычно необходим, но может быть полезен, когда установлено как любой IP-адрес в диапазоне ACL перенаправления для инициирования перенаправления (как в сценариях VPN, например).

Возможные причины

Перенаправление не происходит

Это - наиболее распространенная причина безусловно. Чтобы проверить или лишить законной силы, открывает браузер на ПК, где агент не появляется и видит, перенаправлены ли вы к странице разгрузки агента положения при вводе любого URL. Можно также ввести случайный IP-адрес, такой как **http://1.2.3.4** во избежание возможной проблемы DNS (если IP-адрес перенаправляет, но название веб-сайта не делает, можно посмотреть на DNS).

Если вы перенаправлены, необходимо собрать журналы агента и связку (bundle) поддержки ISE (с положением и швейцарским модулем к режиму отладки) и связаться с Центром технической поддержки Cisco. Это указывает, что агент обнаруживает узел ISE, но что-то не в состоянии во время процесса получать данные положения.

Если никакое перенаправление не происходит, у вас есть своя первая причина, которая все еще требует дополнительного исследования основной причины. Хорошее начало должно проверить конфигурацию на устройстве доступа к сети (Контроллер беспроводной локальной сети (WLC) или коммутатор) и переместиться в следующий элемент в этом документе.

Атрибуты не установлены на сетевом устройстве

Эта проблема является подслучаем **Перенаправления, Не Происходит** сценарий. Если перенаправление не происходит, первая вещь состоит в том, чтобы проверить (поскольку

проблема происходит на данном клиенте), что клиент правильно размещен в правильный статус уровнем беспроводного доступа или коммутатором.

Вот пример выходных данных **международной** команды **<interface number> сеанса show authentication** (вам, возможно, придется добавить **подробность** в конце на некоторых платформах), взятый коммутатор, где связан клиент. Необходимо проверить, что статус является "успехом Authz", что ACL перенаправления URL правильно указывает к намеченному ACL перенаправления, и что перенаправление URL указывает к ожидаемому узлу ISE с **CPP** в конце URL. Поле ACS ACL не является обязательным, потому что оно только показывает, настроили ли вы загружаемый список доступа на профиле авторизации на ISE. Однако, важно посмотреть на него и проверить, что нет никакого конфликта с ACL перенаправления (см. документы о конфигурации положения в случае сомнения).

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address: 000f.b049.5c4b
          IP Address: 192.168.33.201
           User-Name: 00-0F-B0-49-5C-4B
              Status: Authz Success
              Domain: DATA
     Security Policy: Should Secure
     Security Status: Unsecure
      Oper host mode: single-host
    Oper control dir: both
       Authorized By: Authentication Server
         Vlan Policy: N/A
             ACS ACL: xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL: redirect
        URL Redirect: https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
     Session timeout: N/A
        Idle timeout: N/A
   Common Session ID: C0A82102000002D8489E0E84
     Acct Session ID: 0x000002FA
              Handle: 0xF60002D9

Runnable methods list:

      Method  State
      mab     Authc Success
```

Для устранения проблем WLC, который выполняет AireOS, войдите**, показывают подробность беспроводного клиента <мак адрес>** и входят**, показывают mac-address беспроводного клиента <мак адрес> подробность** для устранения проблем WLC, который выполняет Cisco IOS XE. Подобные отображения данных и вы должны проверить URL перенаправления и ACL и если клиент находится в состоянии "POSTURE_REQD" или подобен (это варьируется в зависимости от версии программного обеспечения).

Если атрибуты не присутствуют, необходимо открыть опознавательные подробные данные в ISE клиента, которого вы устраняли неполадки (перейдите к **Операциям> Аутентификации**), и проверьте в разделе Результата, что передавались атрибуты перенаправления. Если бы они не передавались, то необходимо рассмотреть политику авторизации для понимания, почему атрибуты не были возвращены для этого конкретного клиента. Вероятно, одно из условий не совпадало, таким образом, это - хорошая идея устранить неполадки их один за другим.

Помните, что, относительно ACL перенаправления, перенаправлений Cisco IOS® в операторах permit (таким образом, ISE и IP-адреса DNS должны быть запрещены), в то

время как AireOS на WLC перенаправляет на инструкциях deny (таким образом, это разрешено для ISE и DNS).

Атрибуты существуют, но сетевое устройство не перенаправляет

Главной причиной в этом случае является проблема конфигурации. Необходимо рассмотреть конфигурацию сетевого устройства против руководства по конфигурации и примеров конфигурации на Cisco.com. Если это верно, проблема, как правило, существует всюду по всем портам или точкам доступа (AP) сетевого устройства. В противном случае проблема могла бы только произойти на некотором switchports или некоторых AP. Если это верно, необходимо сравнить конфигурацию тех, где проблема происходит по сравнению с портами или AP, где хорошо работает положение.

AP FlexConnect чувствительны, потому что у них может каждый быть уникальная конфигурация, и легко сделать ошибку в ACL или VLAN в некоторых AP и не других.

Другая типичная проблема - то, что клиентская VLAN не имеет SVI. Это только применяется к коммутаторам и обсуждено подробно в Переадресации трафика ISE на коммутаторе серии Catalyst 3750. Все могло бы выглядеть хорошим с точки зрения атрибутов.

Вмешивающийся загружаемый Access-list (DACL)

Если, в то же время, что и перенаправление приписывает, вы выдвигаете DACL назад к коммутатору (или ACL Airespace для контроллера беспроводной локальной сети), то это могло заблокировать ваше перенаправление. DACL применен сначала и определяет то, что полностью отброшено и что продолжает обрабатываться. Затем ACL перенаправления применен и определяет то, что перенаправлено.

То, что это конкретно означает, - то, что большую часть времени, вы захотите разрешить весь трафик HTTP и Трафик HTTPS в вашем DACL. При блокировании его это не будет перенаправлено, так как это будет отброшено перед этим. Это не проблема безопасности, потому что тот трафик будет перенаправлен главным образом на ACL перенаправления после, таким образом, это не будет действительно позволено в сети; однако, необходимо разрешить тем двум типам трафика в DACL для них иметь возможность поразить ACL перенаправления прямо после.

Плохая версия агента NAC

Легко забыть, что определенные версии агента NAC проверены против определенных версий ISE. Много администраторов обновляют свой кластер ISE и забывают загружать связанную версию агента NAC в клиенте, настраивающем базу данных результатов.

При использовании устаревшую версию агента NAC для своего кода ISE, знают, что он мог бы работать, но он также не мог бы. Таким образом, не удивительно, что некоторые клиенты работают, и другие не делают. Один способ проверить состоит в том, чтобы перейти к разделу загрузки Cisco.com вашей версии ISE и проверки, которая версии агента NAC там. Как правило, существуют несколько поддерживаемые для каждой версии ISE. Эта

веб-страница собирает все матрицы: Информация о совместимости Cisco ISE.

Веб - прокси HTTP используется клиентами

Понятие веба - прокси HTTP - то, что клиенты не решают сами IP-адреса DNS веб-сайта, ни связываются с веб-сайтами непосредственно; скорее они просто отправляют свой запрос к прокси-серверу, который заботится о нем. Типичная проблема со стандартной конфигурацией - то, что клиент решает веб-сайт (такой как www. cisco . com) путем прямой передачи GET HTTP за ним к прокси, который перехвачен и законно перенаправил к порталу ISE. Однако вместо того, чтобы тогда передать следующий GET HTTP к IP-адресу портала ISE, клиент продолжает отправлять тот запрос к прокси.

В случае, если вы решаете не перенаправить трафик HTTP, предназначенный к прокси, у ваших пользователей есть прямой доступ ко всему Интернету (так как весь трафик проходит прокси), не аутентифицируясь или положение. Решение состоит в том, чтобы фактически модифицировать настройки обозревателя клиентов и добавить исключение для IP-адреса ISE в параметрах прокси. Таким образом, когда клиент должен достигнуть ISE, он отправляет запрос непосредственно к ISE а не к прокси. Это избегает бесконечного цикла, где клиент постоянно перенаправляется, но никогда не видит страницу входа.

Обратите внимание на то, что на агента NAC не влияют параметры прокси, введенные в систему, и она продолжает действовать обычно. Это означает, что при использовании веба - прокси у вас не может оба быть работы обнаружения агента NAC (потому что она использует порт 80), и сделайте, чтобы пользователи самоустановили агента, как только они перенаправлены к странице положения, когда они просматривают (так как это использует прокси - порт, и типичные коммутаторы не могут перенаправить на множественных портах).

Хосты обнаружения настроены в агенте NAC

Особенно после Версии 1.2 ISE, рекомендуется не настроить любой хост обнаружения на агенте NAC, пока у вас нет экспертных знаний в области того, что это делает и не делает. Агент NAC, как предполагается, обнаруживает узел ISE, который аутентифицировал устройство клиента через обнаружение HTTP. При доверии хостам обнаружения вы могли бы сделать, чтобы агент NAC связался с другим узлом ISE, чем тот, который аутентифицировал устройство, и это не работает. Версия 1.2 ISE отклоняет агента, который обнаруживает узел посредством хост-процесса обнаружения, потому что это хочет, чтобы агент NAC получил идентификатор сеанса от URL перенаправления, таким образом, обескураживают этому методу.

В некоторых случаях вы могли бы хотеть настроить хост обнаружения. Затем это должно быть настроено с любым IP-адресом (даже если несуществующий), который будет перенаправлен ACL перенаправления, и это не должно идеально быть в той же подсети как клиент (иначе, клиент будет ARP неопределенно для него и никогда не передавать пакет обнаружения HTTP).

Агент NAC иногда не появляется

Когда проблема более неустойчива, и действия, такие как отключение/перевключение подключения кабеля/Wi-Fi заставляют ее работать, это - более тонкая проблема. Это могла быть проблема с идентификаторами сеанса RADIUS, где идентификатор сеанса удален на ISE учетом RADIUS (отключите учет, чтобы видеть, изменяет ли это что-то).

При использовании ISE Version1.2 другая возможность состоит в том, что клиент передает много пакетов HTTP так, чтобы ни один не прибывал из браузера или агента NAC. Версия 1.2 ISE просматривает поле user-agent в пакетах HTTP, чтобы видеть, прибывает ли это от агента NAC или браузера, но много других приложений передают трафик HTTP с полем user-agent и не упоминают операционной системы или полезных сведений. Версия 1.2 ISE тогда передает Изменение Авторизации разъединить клиента. На Версию 1.3 ISE не влияет эта проблема beause, это работает другим способом. Решение состоит в том, чтобы или обновить к Версии 1.3 или позволять все обнаруженные приложения в ACL перенаправления так, чтобы они не были перенаправлены к ISE.

Обратная проблема: агент неоднократно появляется

Противоположная проблема может возникнуть, где агент появляется, делает анализ положения, проверяет клиента, и затем появляется снова вскоре после вместо того, чтобы позволить сетевое подключение и остаться тихим. Это происходит, потому что, даже после успешного положения, трафик HTTP все еще перенаправлен к порталу CPP на ISE. Это - хорошая идея тогда пройти политику авторизации ISE и проверить, что у вас есть правило, которое передает доступ разрешения (или подобное правило с возможными ACL и VLAN), когда это видит совместимого клиента и НЕ перенаправление CPP снова.

Дополнительные сведения

- Сервисы положения на руководстве по конфигурации Cisco ISE
- Процесс обнаружения агента NAC для ISE
- Переадресация трафика ISE на коммутаторе серии Catalyst 3750
- Cisco Systems – техническая поддержка и документация