NAC-устройство: Пример конфигурации положения AV Mac OSX на Cisco NAC выпуска 4.5

Содержание

Введение

Этот документ описывает, как настроить MAC OS X Чистая оценка положения Агента Доступа через Менеджера Network Admission Control (NAC) веб - консоль для выпуска 4.5.

Оценка положения Mac в этом выпуске ограничена поддержкой AV/AS только. См. Комментарии к выпуску устройства Cisco NAC (Clean Access) для списка AV/AS, которые поддерживаются на MAC OSX.

Предварительные условия

Требования

Выполните эти шаги перед попыткой этой конфигурации:

Этот документ предполагает выполнение Выпуска 4.5 устройства Cisco NAC и что вы завершили следующие шаги согласно рекомендациям в устройстве Cisco NAC – Чистят Руководство по установке и конфигурированию Access Manager, Выпуск 4.5:

1. Установите или обновите своего Менеджера NAC и Сервер NAC с выпуском 4.5 устройства Cisco NAC, как описано в Кратком руководстве по началу работы Установки оборудования устройства Cisco NAC, Выпуске 4.5.
2. Гарантируйте, что последний Агент MAC OS X (версия 4.5) и пакеты поддержки AV/AS доступен на вашем Менеджере NAC, как описано в, Настраивают и Обновления Загрузки.
3. Создайте страницу входа пользователя по умолчанию, как описано на Странице Регистрационной информации пользователя для входа.
4. Потребуйте использования MAC OS X, Чистый Агент Доступа 4.5, как описано в Требует Использования Агента.
5. Создайте одну или более ролей пользователя для пользователей Macintosh, как описано в, Создают Роли пользователя.

Примечание: См. MAC OS X ограничения Агента разделяют для версий OS X и продуктов AV/AS и Типов Требования, которые поддерживаются для оценки положения Mac.

Используемые компоненты

Сведения в этом документе основываются на Выпуске 4.5 NAC Cisco.

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.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Оценка положения Mac с моллюском AntiVirus (ClamAV)

Цель этой процедуры состоит в том, чтобы проверить, что ClamAV 1.1.0 установлен и обновлен со свежими описаниями вирусов на клиентском компьютере.

Если ClamAV 1.1.0 не установлен на клиентском компьютере, необходимо предоставить пользователю ссылку на веб-сайт ClamAV, чтобы загрузить и установить программное обеспечение. Затем, необходимо проверить, что ClamAV обновлен с последними определениями. В противном случае Чистый агент Доступа может связаться с AV Моллюска через вызов API (с типом требования *Обновления AV*) и запросить ClamAV обновить себя.

Примечание: С выпуска Cisco NAC 4.5 тип требования Обновления AV поддерживается только с ClamWin AV. Если их определения вируса не обновлены, для всего другого AV/AS *Распределение Ссылки* или *Локальный* тип *Проверки* требования могут быть настроены, чтобы повторно добиться пользователей.

Шаг 1. Настройте Правило Проверить, установлен ли ClamAV

1. Перейдите **к Управлению устройствами> Чистый Доступ> Чистый Агент Доступа> Правила> Новое Правило AV**.
2. Введите имя для правила. Данный пример использует *Is_Clamwin_Installed_OSX*.**Примечание:** Будьте описательными так, чтобы можно было легко определить цель правила. Можно использовать цифры и подчеркивания на название, но никакие пробелы.
3. Выберите **ClamWin** из Антивирусного выпадающего списка Поставщика.
4. Выберите **Installation** от Типа выпадают.
5. Выберите **Mac OSX** из выпадающего списка Операционной системы.Таблица внизу страницы заполнена с этими значениями.
6. Проверьте флажок **Installation** для 1. x.
7. Введите описание в текстовом поле Описания Правила и нажмите **Save Rule**.

Новое правило AV добавлено к нижней части Списка Правила.

Шаг 2. Настройте Требование, чтобы Повторно добиться Пользователей, если не Установлен ClamAV

Если Чистый Агент Доступа обнаруживает тот ClamAV 1.1.0, не установлен на клиентском компьютере, он изолирует пользователя. На этом этапе можно настроить тип требования *Распределения Ссылки* для предоставления пользователю ссылку для загрузки ClamAV 1.1.0.

1. Нажмите **Чистую вкладку Agent Доступа**, и затем нажмите **Requirements**.
2. Нажмите **New Requirement**.
3. Выберите **Link Distribution** из выпадающего списка Типа Требования.
4. Выберите **Mandatory** из Принуждать выпадающего списка Типа.В данном примере конечному пользователю сообщают об этом требовании и не может продолжиться или иметь доступ к сети, пока система клиента не удовлетворяет требование.См. Настройку Дополнительное / Требование аудита для получения информации о других типах осуществления.
5. Выберите уровень приоритета выполнения для этого требования на клиентском компьютере.Высокий приоритет (например, 1) означает, что это требование проверено в системе перед всеми другими требованиями (и появляется в Чистых диалоговых окнах Агента Доступа в том заказе). Данный пример предполагает, что проверка установки ClamWin является первым требованием положения и устанавливает приоритет в один (1).**Примечание:** Агент MAC OS X не поддерживает автоматическое исправление. Поэтому тип исправления установлен в руководство. Кроме того, функции, которые появляются на Новой странице конфигурации Требования (Тип исправления, Интервал и Число повторов) не служат никакой цели при создании типов требования для исправления Macintosh - клиента.
6. В текстовом поле URL Ссылки Файла введите URL, к которому конечные пользователи должны быть направлены для загрузки ClamAV 1.1.0.
7. В поданном тексте Названия Требования введите уникальное имя, которое передает действие конечному пользователю.Это название видимо пользователям в Чистых диалоговых окнах Агента Доступа. Данный пример использует *Загрузку ClamAV*.
8. В текстовом поле Описания введите описание требования и инструкций для

направления пользователей, которые не в состоянии удовлетворять требование.
9. Нажмите флажок **Mac OS**, перечисленный в разделе Операционной системы.
10. **Нажмите Add Требование** для добавления требования к Списку Требования.

Новое требование добавлено к Списку Требования.

Шаг 3. Сопоставьте требование распределения ссылки с правилом установки AV

1. Нажмите **Чистую вкладку Agent Доступа**, и затем нажмите **Requirements**.
2. Нажмите **Requirement-Rules**.
3. От выпадающего списка Названия Требования выберите требование, которое вы создали в Шаге 2.
4. Выберите **Mac OSX** из выпадающего списка Операционной системы.Правила, созданные для выбранной операционной системы, отображены внизу страницы.
5. Нажмите флажок для правила, которое вы создали в Шаге 1, и затем нажмите **Update**.

Шаг 4. . Настройте Правило Проверить, обновлен ли ClamAV

1. Перейдите **к Управлению устройствами> Чистый Доступ> Чистый Агент Доступа> Правила> Новое Правило AV**.
2. Введите имя для правила. Данный пример использует *Is_ClamAV_Updated_OSX*.**Примечание:** Будьте описательными так, чтобы можно было легко определить цель правила. Можно использовать цифры и подчеркивания на название, но никакие пробелы.
3. Выберите **ClamWin** из Антивирусного выпадающего списка Поставщика.
4. Выберите **Virus Definition** из выпадающего списка Типа.
5. Выберите **Mac OSX** из выпадающего списка Операционной системы.Проверки Определения вируса для таблицы MAC OSX внизу страницы заполнены.
6. Проверьте флажок **Installation** для 1. x.
7. Введите описание в текстовом поле Описания Правила и нажмите **Save Rule**.

Новое правило AV добавлено к нижней части Списка Правила.

Шаг 5. . Настройте Требование, чтобы Повторно добиться Пользователей, если не Обновлен ClamAV

Если Чистый Агент Доступа обнаруживает тот ClamAV 1.1.0, не обновлен на клиентском компьютере, он изолирует пользователя. На этом этапе пользователю предоставляют кнопку Update, чтобы повторно посредничать.

Как только пользователь нажимает кнопку Update, Чистый агент Доступа связывается с базовым программным обеспечением ClamAV и просит, чтобы ClamAV обновил себя.

Можно настроить тип требования Обновления Определения AV для реализации этой функциональности.

1. Нажмите **Чистую вкладку Agent Доступа**, и затем нажмите **Requirements**.
2. Нажмите **New Requirement**.
3. Выберите **AV Definition Update** из выпадающего списка Типа Требования.

4. Выберите **Mandatory** из Принуждать выпадающий список Типа.В данном примере конечному пользователю сообщают об этом требовании и не может продолжиться или иметь доступ к сети, пока система клиента не удовлетворяет требование.См. Настройку Дополнительное / Требование аудита для получения информации о других типах осуществления.
5. Выберите уровень приоритета выполнения для этого требования на клиентском компьютере.Высокий приоритет (например, 1) означает, что это требование проверено в системе перед всеми другими требованиями (и появляется в Чистых диалоговых окнах Агента Доступа в том заказе). Данный пример предполагает, что проверка обновления ClamWin является вторым требованием положения и устанавливает приоритет в два (2).**Примечание:** Агент MAC OS X не поддерживает автоматическое исправление. Поэтому тип исправления установлен в руководство. Кроме того, обратите внимание, что Тип Исправления, Интервал и опции Retry Count, которые появляются на Новой странице конфигурации Требования, не служат никакой цели при создании типов требования для исправления Macintosh - клиента.
6. Выберите **ClamWin – (Mac OS)** от Антивирусного выпадающего списка Имени поставщика.**Внимание. :** Удостоверьтесь, что вы выбираете опцию *ClamWin - (Mac OS)*, не опцию ClamWin.**Примечание:** С выпуска Cisco NAC 4.5 тип требования Обновления AV поддерживается только с ClamAVon Mac OSX. Если их определения вируса не обновлены, для всего другого AV/AS на MAC OSX Распределение Ссылки или Локальный тип требования Проверки могут быть настроены, чтобы повторно добиться пользователей.
7. В текстовом поле Названия Требования введите уникальное имя, которое передает действие конечному пользователю.Это название видимо пользователям в Чистых диалоговых окнах Агента Доступа. Данный пример использует *Обновление ClamAV*.
8. В текстовом поле Описания введите описание требования и инструкций для направления пользователей, которые не в состоянии удовлетворять требование.
9. Нажмите флажок **Mac OS**, перечисленный в разделе Операционной системы.
10. **Нажмите Add Требование** для добавления требования к Списку Требования.

Новое требование добавлено к Списку Требования.

Шаг 6. Сопоставьте требование обновления определения AV с правилом определения вируса

1. Нажмите **Чистую вкладку Agent Доступа**, и затем нажмите **Requirements**.
2. Нажмите **Requirement-Rules**.
3. От выпадающего списка Названия Требования выберите требование, которое вы создали в Шаге 5.
4. Выберите **Mac OSX** из выпадающего списка Операционной системы.Правила, созданные для выбранной операционной системы, отображены внизу страницы.
5. Нажмите флажок для правила, которое вы создали в Шаге 4, и затем нажмите **Update**.

Шаг 7. Сопоставьте требования с ролями

На этом этапе можно связать требования положения (которые были сопоставлены с правилами) к роли, в которую размещен конечный пользователь.

1. Нажмите **Чистую вкладку Agent Доступа**, и затем нажмите **Role-Requirements**.

2. Нажмите **Role-Requirements**.
3. Выберите **Normal Login Role** из выпадающего списка Типа Роли.
4. От выпадающего списка Роли пользователя выберите роль, где вы хотите, чтобы были применены требования положения. Данный пример применяет требования положения к роли *сотрудника*.Требования, созданные ранее в данном примере, отображены внизу страницы.
5. Проверьте флажки для требований, чтобы вы хотели примениться к этой роли и нажать **Update**.

Шаг 8. Предоставьте доступ к узлу исправления во временной роли

Как только пользователи, как находят, не соответствующи стандарту, они изолированы и размещены во временную роль. На этом этапе пользователи должны быть в состоянии достигнуть ресурсов исправления (сервер AV, веб-сайты, серверы исправления, и т.д.) так, чтобы они могли повторно добиться себя.

Для этой цели необходимо открыть соответствующий доступ во Временной Роли. В данном примере пользователи должны быть в состоянии достигнуть http://www.clamxav.com и для требований (установка и для обновления определения вируса).

1. Выберите **User Management> User Roles**, и затем нажмите вкладку **Traffic Control**.
2. Нажмите **Host**.
3. Выберите **Temporary Role** из выпадающего списка и прокрутите вниз к нижней части списка.
4. Добавьте **clamxav.com** к Позволенному списку Хоста и **нажмите Add**.Этот шаг гарантирует, что трафик от клиентов к http://www.clamxav.com позволен через серверы NAC.**Примечание:** Эти два условия важны:Сервер NAC использует DNS - ответ от сервера DNS для динамичного открытия доступа. Следовательно, ответный трафик от сервера DNS (DNS - ответ) должен пройти сервер NAC.Необходимо было определить доверяемый сервер DNS. Для оптимальных методов Cisco рекомендует добавить определенные записи сервера DNS здесь в противоположность доверию всем серверам DNS (*). Данный пример добавляет IP сервера DNS (192.168.2.44) как доверяемый сервер DNS. Можно добавить множественные доверяемые серверы DNS. Если вам не определили доверяемый сервер DNS, Менеджер NAC советует вам соответственно через сообщение как показано в этом образе:

Проверьте опыт конечного пользователя

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Этот сценарий проверки положения Mac предполагает, что ваша начальная настройка NAC (Менеджер NAC и Сервер) завершена и что Сервер NAC достижим от клиентских компьютеров. Агент чистого доступа Cisco 4.5.0.0 должен быть установлен на Mac, который выполняет OSX 10.4 или выше. Этот сценарий предполагает, что Mac не установили ClamAV до этого теста.

1. Войдите своему Чистому Агенту Доступа (версия 4.5.0.0).Вас изолируют и просят повторно посредничать.**Примечание:** Флажки ВЫПОЛНЕНИЯ проверены, но не доступные для редактирования, потому что требования являются обязательными.

Если бы требование было настроено как *Дополнительное*, то флажок RUN был бы доступен для редактирования, и можно принять решение пропустить то требование.
2. Нажмите **Remediate**.Вы перенаправлены к веб-сайту ClamAV.
3. Загрузка и установка ClamAV.Вам можно было бы предложить выполнить Механизм Антивируса Моллюска, прежде чем можно будет использовать ClamAV как показано в этом образе:
4. Придерживайтесь инструкций, выводящихся на экран для завершения установки.Чистый агент Доступа отображает статус *Загрузки* требование *ClamAV* как успешный и переходит к второму требованию (*Обновление ClamAV*).Как только ClamAV обновлен, статус *Обновления* успешные показы требования *ClamAV*.
5. Нажмите **Complete** для регистрации к сети.Как только вы успешно входите к сети, это обменивается сообщениями, появляется.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка продуктов устройства Cisco NAC (Clean Access)
- Cisco Systems – техническая поддержка и документация