TAC

ID документа: 118012

Обновлено: 20 мая 2015

Внесенный Nazmul Rajib, специалистом службы технической поддержки Cisco.

PDF загрузки
Печать
[+] Feedback

Родственные продукты

- Центр управления Cisco FireSIGHT 750
- Центр управления Cisco FireSIGHT 3500
- Центр управления Cisco FireSIGHT 1500
- Центр управления Cisco FireSIGHT
- Виртуальное устройство центра управления Cisco FireSIGHT

Содержание

Введение

Этот документ описывает, как определить основную причину и решить проблему, когда события подключения исчезают из Центра управления FireSIGHT после системных выполнений в течение нескольких дней. Это могло бы произойти из-за параметров конфигурации центра управления.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с Центром управления FireSIGHT.

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Центр управления FireSIGHT
- Версия программного обеспечения 5.2 или позже

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.

Устранение неполадок

Шаг 1: Определите количество сохраненных событий

Для определения количества Событий подключения, которые сохранены на Центре управления FireSIGHT,

1. Выберите **Analysis> Connections> Table View of Connection Events**.
2. Разверните Временное окно до широкого диапазона, который охватывает все текущие события, например 12 месяцев.
3. Обратите внимание на общее число строк внизу страницы. Нажмите последнюю страницу и обратите внимание на штамп времени последнего доступного События подключения.

Эта информация дает вам общее представление о том, сколько и сколько времени вы в состоянии сохранить События подключения со своей текущей конфигурацией.

Шаг 2: Определите параметр регистрации

Анализ, какие соединения зарегистрированы, и где в потоке, что зарегистрированы соединения. Необходимо регистрировать соединения в соответствии с безопасностью и потребностями соответствия организации. Если ваша цель состоит в том, чтобы ограничить количество событий, вы генерируете, только enable logging для правил, важных по отношению к вашему анализу. Однако, если вы хотите широкое представление своего сетевого трафика, вы можете enable logging для дополнительных правил управления доступом или для действия по умолчанию. Можно отключить Регистрацию Соединения для несущественного трафика, чтобы помочь сохранять События подключения для более длинного периода времени.

Совет: Для оптимизации производительности Cisco рекомендует регистрировать или

начало или конец соединения, но не обоих.

Примечание: Для одиночного соединения конец события подключения содержит всю информацию в начале события подключения, а также информацию, которая была собрана по продолжительности сеанса. Для Доверия и Позволяют правила, рекомендуется, чтобы использовался Конец Соединения.

Эта диаграмма объясняет другие параметры регистрации, доступные для каждого Действия Правила:

Действие правила или параметр регистрации	Журнал вначале	Журнал в конце
Доверие Действие по умолчанию: доверие Allow	X	X
Действие по умолчанию: проникновение	X	X
Действие по умолчанию: обнаружение Монитор		X (Требуемый)
Блок Блок со сбросом Действие Defaut: блок	X	
Интерактивный блок Интерактивный блок со сбросом	X	X (если обойдено)
Интеллектуальная информационная безопасность	X	

Шаг 3: Отрегулируйте размер подключения базы данных

События подключения сокращены зависящие от значения Событий Максимального числа подключений в системной политике. Для изменения настроек:

1. Выберите **System> Local> System Policy**.
2. Нажмите *значок карандаша* для редактирования в настоящее время прикладной политики.
3. Выберите **Database> Connection Database> Maximum Connection Events**.
4. Измените значение для **Событий Максимального числа подключений**.
5. Нажмите **Save Policy и Exit**, и затем **Примените** политику к своим устройствам.

Максимальное количество Событий подключения, которые могут быть сохранены, зависит от модели Центра управления:

Примечание: Предел максимального количества событий разделен между событиями Security Intelligence и событиями подключения; сумма настраиваемых максимальных значений для этих двух событий не может превысить предел максимального количества событий.

Модель центра управления	Максимальное число событий
FS750, DC750	50 миллионов
FS1500, DC1500	100 миллионов
FS2000	300 миллионов
FS3500, DC3500	500 миллионов
FS4000	1 миллиард

Виртуальное устройство	10 миллионов

> **Внимание:** Увеличение Пределов Базы данных может иметь неблагоприятное влияние на производительность на устройстве. Для улучшения производительности необходимо адаптировать пределы события количеству событий, с которыми вы регулярно работаете.

Для виджетов, которые отображают количество события по временному диапазону, общее число событий не могло бы отразить количество событий, для которых подробных данных доступно в конечном счете средство просмотра. Это происходит, потому что система иногда сокращает более старые подробные данные события для управления использованием дискового пространства. Для уменьшения возникновения подробного отсечения события можно подстроить регистрацию событий для регистрации только тех событий, самых важных для развертываний.

Дополнительные сведения

- Пределы события Database Настройки
- Cisco Systems – техническая поддержка и документация

Связанные обсуждения Сообщества Cisco Support

Сообщество Cisco Support является форумом для вас, чтобы спросить и ответить на вопросы, общие предложения, и сотрудничать с вашими узлами.

Обновлено: 20 мая 2015
ID документа: 118012