IPS 5.x и более поздние версии: Различные методы слежения за развитием событий

Содержание

Введение

Этот документ предоставляет различные методы для слежения за развитием событий IPS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на IPS 5.x и 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.

Условные обозначения

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

Методы следят за развитием событий IPS

В настоящее время существует четыре опции для мониторинга датчиков:

1. IPS Manager Express (IME) доступен от загрузки программного обеспечения в Cisco.com. Это приложение в состоянии надежно подписаться на сенсор IPS с SDEE и получить события/журналы, которые генерировались в результате любых проблем или подписей, которые сработали из-за соответствия.Диспетчера устройств IPS (IDM) вызывают при доступе к датчику непосредственно через HTTPS.Просмотрите хранилище события непосредственно на датчике с Мониторингом IDM или программных средствах Мониторинга событий IME. IDM и IME не являются допустимыми решениями, если необходимо сохранить длительный срок событий, поскольку хранилище локального события датчика является кольцевым буфером на 30 МБ и начинает сверхобвинять себя, как только достигнут предел на 30 МБ. Этот предел неизменяем.
2. Используйте устройство MARS CS, чтобы обычно вытягивать и коррелировать события от датчика. MARS CS использует протокол SDEE, чтобы установить безопасное соединение с датчиком для получения событий и получает новые события каждые несколько секунд.Свяжитесь со своей командой по работе с корпоративными заказчиками/reseller/SE для получения дополнительной информации, если вы интересуетесь демонстрацией устройства MARS CS.Для Cisco IPS 5.x и 6.x устройства, MARS вытягивает журналы с SDEE по SSL. Поэтому MARS должен иметь доступ HTTPS к датчику. Для подготовки датчика необходимо позволить Трафик HTTPS от станции управления IDM/IME и удостовериться, что IP-адрес MARS определен как позволенный хост на датчике.
```
sensor#conf t
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#access-list x.x.x.x/subnet_mask
sensor(config-hos-net)#exit
sensor(config-hos)#exit
Apply Changes?[yes]:
sensor(config)#
```
3. Следите за развитием событий с IEV. ПО IDS Event Viewer представляет собой Java-приложение, позволяющее просматривать и управлять сигнальными уведомлениями до 5 датчиков одновременно. С помощью IDS Event Viewer осуществляется просмотр событий в режиме реального времени или в импортированных файлах журналов. Управление уведомлениями осуществляется с помощью различных фильтров и режимов просмотра. Предусмотрена возможность импорта и экспорта сообщений о событиях для последующего анализа. Как MARS, IEV устанавливает безопасное соединение с датчиком и получает события каждые несколько секунд. IEV хранит эти события в базе данных по серверу, на котором установлен IEV. DB включен с IEV и установлен наряду с приложением. Нажмите IEV для загрузки.**Примечание:** Документация для IEV найдена через меню справки после установки его. readme содержит информацию об установке.
4. Настройте подписи на своем датчике, чтобы иметь действие **trap-сообщения snmp запроса** и настроить датчик для передачи trap-сообщений к серверу SNMP. Можно тогда использовать этот сервер для передачи сообщений как системных журналов к другой машине.SNMP является протоколом уровня приложений, который упрощает обмен данными для управления между сетевыми устройствами. SNMP позволяет администраторам сети управлять производительностью сети, найти и решить проблемы сети и план относительно расширения сети.SNMP является простым запросом/протоколом отклика. Система управления сетью выполняет запрос, и управляемые устройства возвращают ответы. Это поведение внедрено с

использованием одной из четырех операций протокола:Get
_____GetNext
НаборTrap-сообщениеМожно настроить датчик для мониторинга SNMP. SNMP определяет стандартный способ для станций управления сетью для мониторинга состояния и статуса многих типов устройств, который включает коммутаторы, маршрутизаторы и датчики.

Дополнительные сведения

- Cisco IPS 4200 Series Sensors
- Cisco Intrusion Prevention System
- Уведомления о дефекте для специалистов по продуктам безопасности (включая обнаружение несанкционированного доступа CiscoSecure)
- Cisco Systems – техническая поддержка и документация