Реализация централизованного сбора событий журналов аудита ОС Windows с удаленных серверов и АРМов является актуальной темой. В качестве одного из продуктов, используемых для централизованного сбора и корреляции событий внедряется SIEM система Symantec Security Information Manager. В виду инициирования окончания поддержки вендором данного продукта перестают выпускаться обновления для коллекторов SSIM, предназначенных для сбора событий с журналов ОС Windows, что сказывается на стабильности их работы. А так же учитывая существующие проблемы в работе данных коллекторов и сложности настройки компонентов ОС Windows для корректной работы коллекторов SSIM (данной теме посвящено множество статей на оф. форуме Symantec: <http://www.symantec.com/connect/articles/installation-troubleshooting-articles-windows-2008-vista-collector-ssim> ), предлагается использовать для сбора событий журналов ОС Windows вариант связки сервера SSIM с агентом Arcsight Smart Connector. Агент Arcsight Smart Connector, в отличии от коллекторов SSIM, имеет унифицированную платформу, позволяющую производить сбор событий с Windows систем всех версий, агент стабилен в работе и не требует сложной настройки компонентов ОС Windows. Так же использование данной связки позволяет быстро организовать сбор событий аудита журналов ОС Windows с большого множества источников. Агент Arcsight Smart Connector не требует лицензирования.

В данной статье предлагается схема по установке агента Arcsight Smart Connector на 1 из предполагаемых источников событий (сервер или АРМ под управлением ОС Windows), его настойке для сбора событий журналов ОС Windows cудаленных серверов или АРМов, и пересылка собранных событий для анализа и хранения на сервер SSIM. События, собранные агентом Arcsight Smart Connector нормализуются в унифицированный формат CEF и передаются на сервер SSIM, где их принимает и обрабатывает коллектор Microsoft CEF Event Collector.

Таким образом достигается цель повышения стабильности работы схемы сбора и анализа событий безопасности с серверов и АРМов под управлением Windows 2000/XP/2003/Vista/7/2008/2012/8.

Проверка настроек компонентов ОС Windows для реализации сбора событий с журналов адудита ОС

Для возможности чтения событий журналов ОС Windows с локального сервера или АРМа, на котором установлен агент **Arcsight Smart Connector,** а так же чтения журналов ОС на удаленных серверах и АРМах под управлением ОС Windows создается доменная учётная запись «**SSIMLOGREADER**» в службе каталога Active Directory домена предприятия **adm.test.ru**. Если источники событий не включены в домен, то данного пользователя необходимо будет создать локально на всех предполагаемых источниках - серверах и АРМах, и добавить данного пользователя во встроенную локальную группу «**Читатели журнала событий**».

1. Проверка конфигурации учётной записи**:**
2. Проверить, что доменная учетная запись **SSIMLOGREADER** добавленав группу «**Читатели журнала событий**» (Event Log Readers) (встроенная доменная группа);
3. Проверка службы **«Удаленный вызов процедур (RPC)»** для исполнения удаленных запросов на доступ к журналам событий от **Arcsight Smart Connector**:
4. Запустить оснастку «**управления компьютером (локальным)**» и перейти в поле управления службами;
5. Убедиться , что служба **«Удаленный вызов процедур (RPC)»** запущена и работает в автоматическом режиме (в случае доменных источников – создать GPO, явно определяющую параметры запуска данной службы)**.**
6. Проверка правил межсетевого экранирования между источниками событий и агентом **Arcsight Smart Connector**, а так же между **Arcsight Smart Connector** и сервером сбора и корреляции событий **SSIM**:
7. Проверка доступности порта **445/TCP** между источниками событий и агентом **Arcsight Smart Connector**
8. Проверка доступности портов **514/UDP** или **10519/TСP** (в зависимости от протокола пересылки событий) между агентом **Arcsight Smart Connector** и сервером **SSI**M

Установка и настройка коннектора **Arcsight Smart Connector.**

**Объем работ**

**В объем работ входит:**

1. Установка ПО **Arcsight Smart Connector 7.0.7** на контроллеры домена;
2. Установка обновления временных зон **tzupdater-1\_4\_8-2014h** для ПО **Arcsight Smart Connector 7.0.7.**

**Основные этапы работ:**

1. Установка ПО **Arcsight Smart Connector 7.0.7** на сервер или АРМ под управлением ОС Windows:
2. Скопировать дистрибутив **ArcSight-7.0.7.7279.0-Connector-Win64.exe (**или новее**)** на диск C:\Temp сервера/АРМа-источника событий. Запустить данный файл на исполнение с правами администратора;
3. Путь установки ПО оставить без изменений. Выбрать «**Typical**» тип установки и нажать «**Next**»;
4. На этапе установки ПО в появившемся окне «**Connector setup**» выбрать пункт **«Add a Connector»**. В выпадающем списке выбрать тип коннектора **«Microsoft Windows Log - Unified»;**
5. В окне настройки конфигурации **«Forwarded Events Collection»** нажать **«Next»;**
6. В окне выбора способа настройки источников событий выбрать тип **«Enter Device Manually»;**
7. В окне настройки списка источников событий внести в соответствующие поля следующую информацию:

**- Domain Name**: имя домена, в котором состоит сервер/АРМ-источник событий (если источник не состоит в домене, то это поле оставить не заполненным)

**- Host Name**: имя сервера/АРМа, с которого будут собираться события (или IP-адрес)

**- User Name**: ssimlogreader

**- Password**: пароль доменного пользователя ssimlogreader

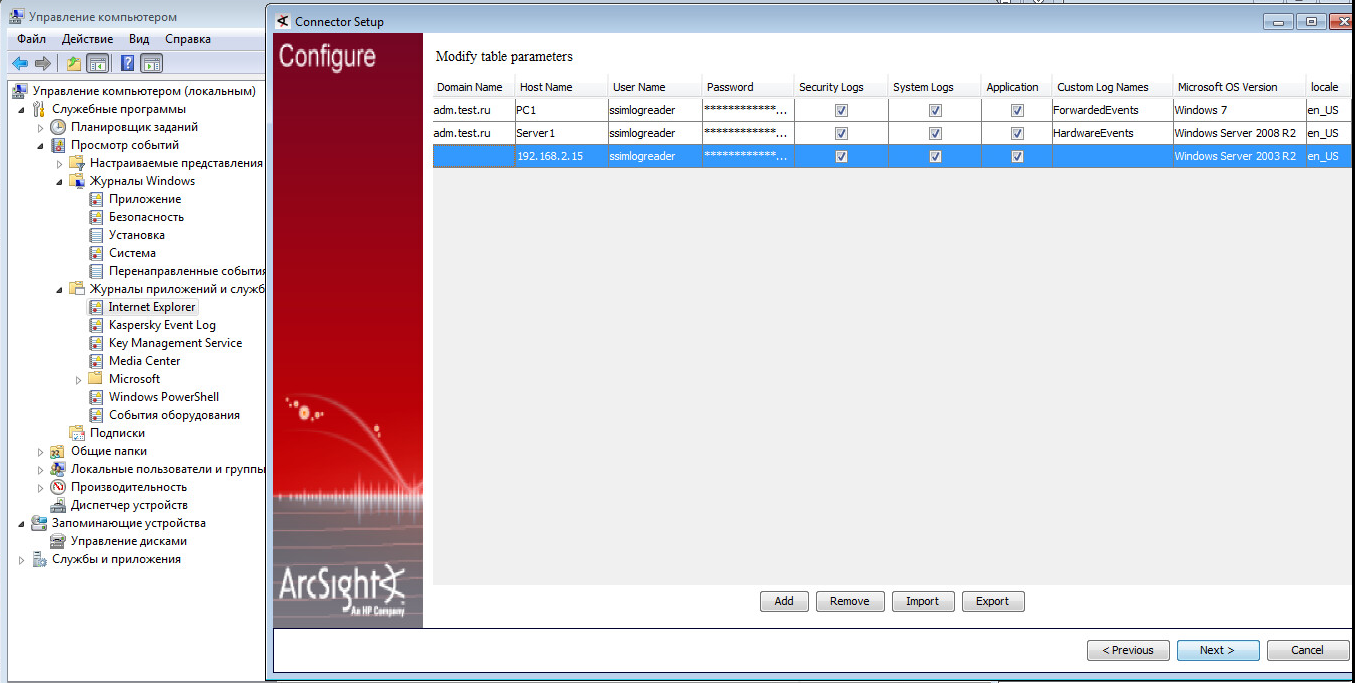
- Установить флаги в полях **Security Logs**, **Application Logs**, **System Logs ( Примечание:** Для сбора событий с произвольных журналов событий, которые отображены в оснастке «**Просмотр событий**» целевых серверов/АРМов, необходимо через запятую ввести названия этих журналов в поле «**custom log names**»)

**- Microsoft OS Version**: указать версию ОС источника событий

- **Locale**: en\_US

Нажать «**Next**»;

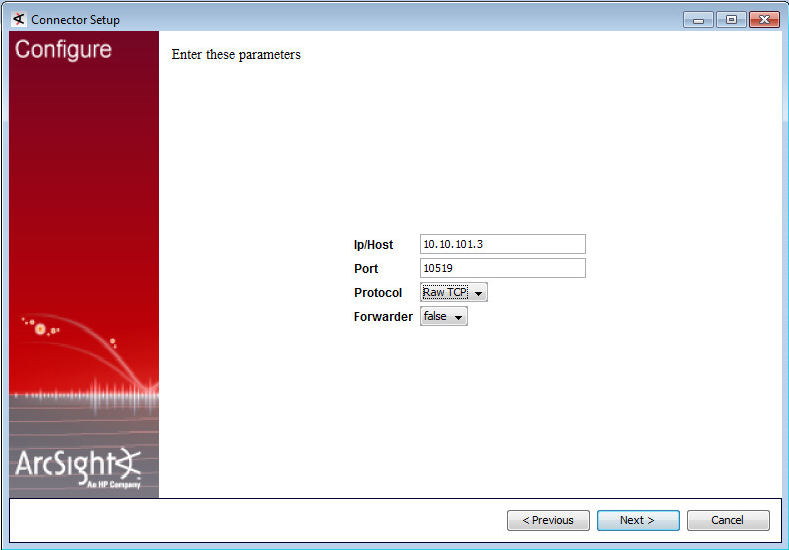
Рис.1 – Пример настройки списка источников событий и журналов аудита для сбора событий в оснастке агента Arcsight Smart Connector 7.0.7

****

1. Далее необходимо выбрать тип передачи собранных агентом Arcsight событий на сервер SSIM. В связке с сервером SSIM агент Arcsight может работать в 2 вариантах:

1 - **CEF Syslog**; 2 – **Raw TCP.**

Рис.2 – Пример настройки параметров пересылки событий в оснастке агента Arcsight Smart Connector 7.0.7



1. Указать **IP-адрес** сервера SSIM. Указать порт **514** (в случае выбора протокола CEF Syslog) или порт **10519** (в случае выбора протокола Raw TCP). Указать протокол. Параметр **forwarder** оставить в значении **false**.
2. Заполнить поля описания установленного коннектора - Name: **ArcConnector** , Location: **Administration Building**. Нажать «**Next**»;
3. После удачной регистрации коннектора и цели доставки событий указать тип установки коннектора в качестве сервиса «**Install as a service**», нажать «**Next**»;
4. По окончании установки коннектора нажать «**Exit**».
5. С помощью оснастки управления «**Службы**» локального сервера/АРМа запустить сервис **«Arcsight Microsoft Windows Event Log - Unified**» и убедиться ,что тип запуска сервиса имеет значение «автоматически».

**Примечание:** для последующего внесения изменений в настройки агента Arcsight Smart Connector необходимо запустить его визард с помощью **runagentsetup.bat** фйла, находящегося в директории, в которую установлен агент: **С:\arcsight\current\bin** .

1. Установка обновления временных зон **tzupdater-1\_4\_8-2014h** для ПО **Arcsight Smart Connector 7.0.7** для корректировки времени java компонента агнета (переход в Росии на зимнее время в октябре 2014г.)**.**
   1. Скопировать в директорию **C:/Temp** сервера/АРМа, где установлен агент Arcsight Smart Connector, файл-архив обновления **tzupdater-1\_4\_8-2014h.zip (**патч должен быть не старее версии **h)**;
   2. Остановить сервис **«Arcsight Microsoft Windows Event Log - Unified**»;
   3. Распаковать **tzupdater.jar** файл из **tzupdater-1\_4\_8-2014h.zip** архива в  директорию коннектора Arcsight : **C:\Program Files\ArcSightSmartConnectors\current\jre\bin;**
   4. Запустить командную строку **CMD** с правами администратора и перейти в директорию **C:\Program Files\ArcSightSmartConnectors\current\jre\bin**. Запустить обновление временных зон java компонента с помощью команды:

**java -jar tzupdater.jar -u -v -f -bc**

* 1. Дождаться окончания установки обновления (об успешном обновлении будет свидетельствовать сообщение “**Time zone data update is complete**” и версия временных зон java будет указана, как **2014h**.
  2. Запустить сервис **«Arcsight Microsoft Windows Event Log - Unified**»;

Настройка и отладка сбора событий ИБ с источников под управлением ОС Windows на сервере сбора  
SSIM

**Объем работ**

**В объем работ входит:**

1. Установка на сервер **SSIM** коллектора **Windows\_CEF\_Event\_Collector\_5.0.10\_AllWin\_AllLinux\_EN.**
2. Выполнение функции **Live Update** на сервере **SSIM**;
3. Создание и настройка конфигураций коллектора **Windows CEF Event Collector 5.0.10** на прием событий с агента **Arcsight Smart Connector**;
4. Создание отчета по принятым событиям.
5. **Установка на сервер SSIM коллектора Windows\_CEF\_Event\_Collector\_5.0.10\_AllWin\_AllLinux\_EN:**
6. Зайти на вэб-интерфейс сервера SSIM под учетной записью администратора;
7. Перейти во вкладку **Maintenance -> System Update->Install;**
8. Выбрать путь к установочному файлу коллектора **Windows CEF Event Collector 5.0.10**. Нажать «**Upload and Install**». Дождаться окончания установки коллектора.
9. **Выполнение функции Live Update на сервере SSIM:**
10. Зайти c помощью браузера на вэб-интерфейс сервера SSIM;
11. Перейти в меню **Maintenance->Live Update** и выбрать следующие компоненты SSIM, которые необходимо обновить:

**- Symantec SIM System Queries**

**- Symantec SIM Server**

**- Symantec SIM Rules, Filters and Monitors**

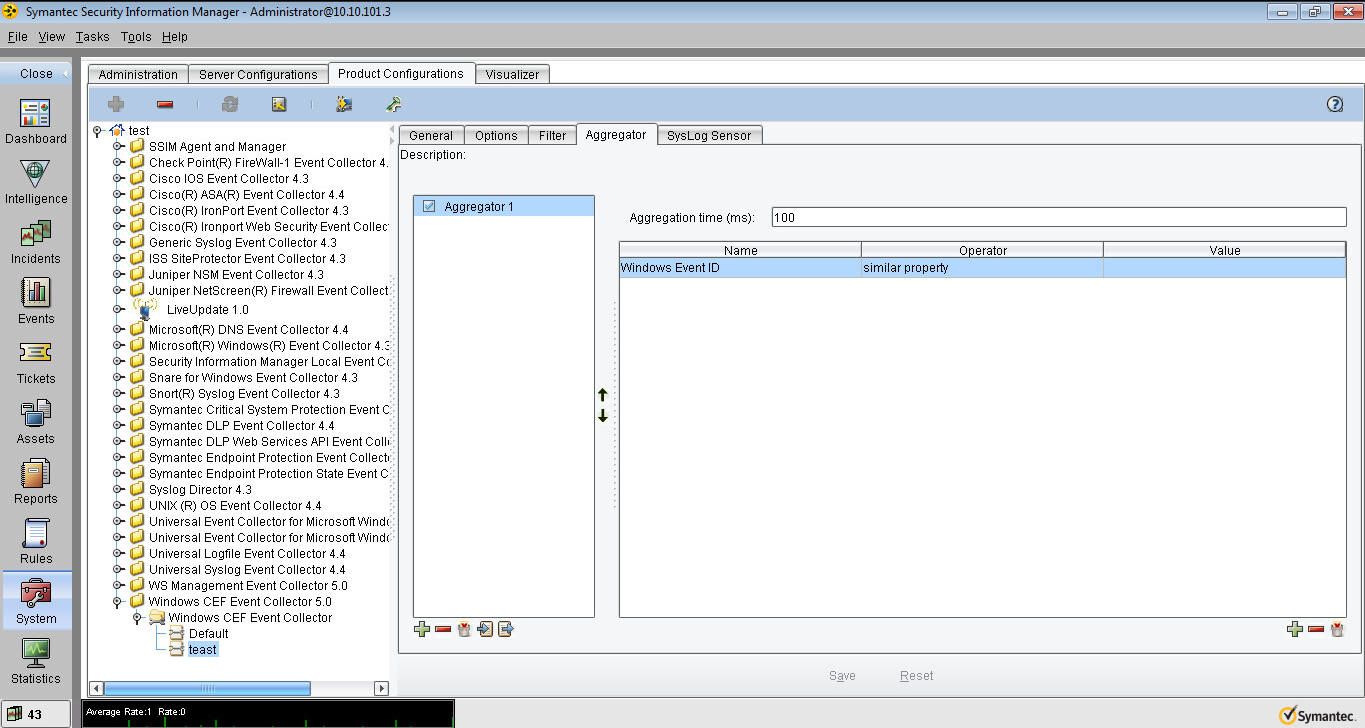
**- Symantec SIM Normalization Content**

**- Symantec SIM Content**

**- Windows CEF Event Collector**

1. Нажать кнопку «**Update»** и дождаться окончания процесса обновления;
2. Проверить работоспособность сервера SSIM .
3. **Создание и настройка сенсоров коллектора Windows CEF Event Collector 5.0.10 на прием событий с агента Arcsight Smart Connector:**
4. C АРМа администратора подключиться к серверу **SSIM** с помощью консоли управления SSIM c правами администратора системы SSIM и перейти в меню **System->Product Configuration**;
5. В дереве продуктов раскрыть настройки **Windows CEF Event Collector 5.0 -> Windows CEF Event Collector** и создать с помощью команды «**new**» новую конфигурацию коллектора;
6. Задать имя и комментарий конфигурации (имя конфигурации: **test**);
7. Добавить с помощью кнопки «**Add**» агент SSIM, установленный непосредственно на сервере сбора SSIM, т.к. именно он будет перехватывать события, переданные агентом **Arcsight Smart Connector** ;
8. Во вкладке **«Aggregator**» создать спецификацию агрегации событий ИБ с помощью кнопки **«Add**». В полях настроек «**Aggregation time**» вписать значение «**100**» мс. В поле «**name**» выбрать «**windows\_event\_id**», в поле «**operator**» выбрать «**similar property**»;

Рис. 3 – Конфигурация агрегатора



1. Открыть вкладку «**Syslog Sensor**» создаваемой конфигурации и задать следующие параметры сенсора:

**-** **Protocol**: UDP (в случае использования **CEF Syslog**) или TCP (в случае использования **Raw TCP**)

**- Host Names/IP Addresses**: IP-адреса серверов, через запятую, где установлены агенты Arcsight Smart Connectorили значение **« \* »** для приема сообщений с любых агентов Arcsight Smart Connector

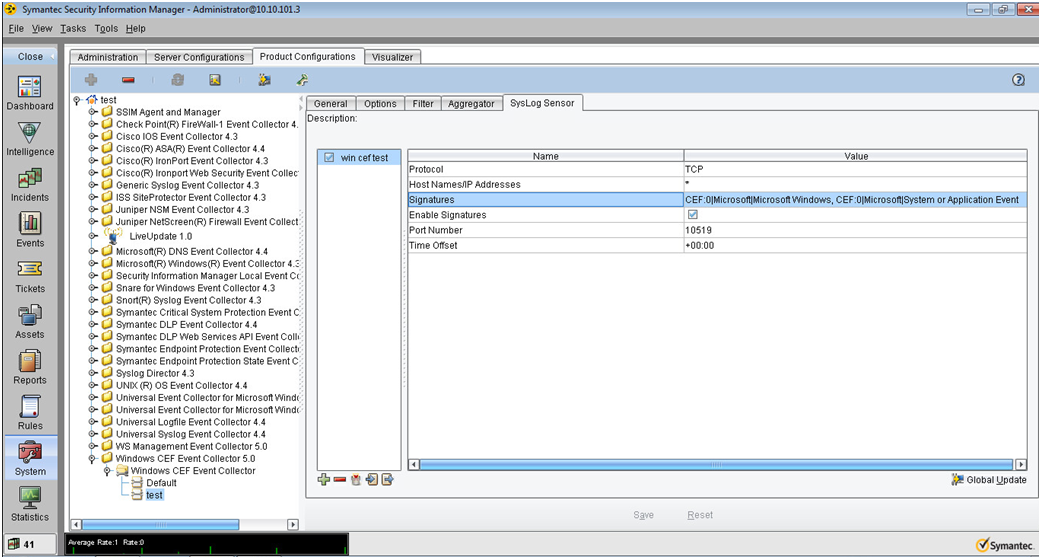
**- Signatures**: оставить без изменений

**- Enable Signatures**: включено

**- Port Number**: **10525** (в случае использования CEF SyslogUDP протокола, это внутренний порт сервера SSIM) или **10519** (в случае использования **Raw TCP** протокола)

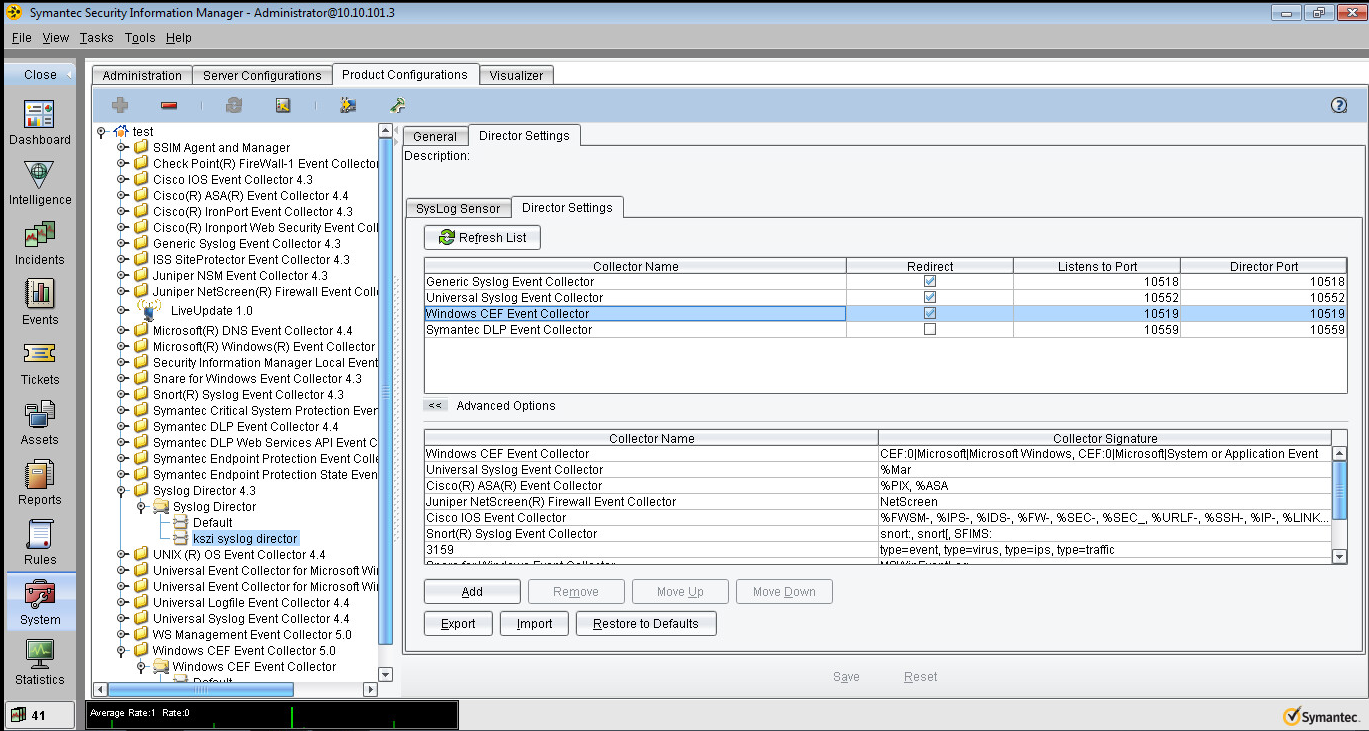
- **Time Offset**: +00:00

Рис. 4 – Конфигурация сенсора



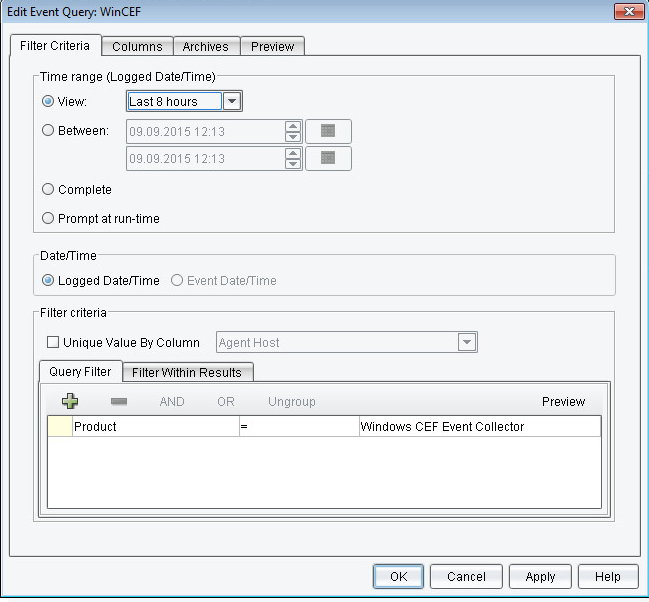
1. Нажать «**Save**»;
2. В дереве «**Product Configuration**» открыть настройки «**Advanced Options**» вкладки «**Director Settings**» компонента **Syslog Director 4.3.** С помощью кнопки «**Add**» добавить коллектор **Windows CEF Event Collector** в список сигнатур и выставить его положение на 1-ю строку (выше остальных сигнатур);
3. Нажать кнопку «**Refresh List**» и в появившейся строке настройки пересылки Syslog событий на коллектор **Windows CEF Event Collector** установить флаг в поле **«Redirect».** В полях **«Listens to Port»** и **«Director Port»** указать порт**,** используемый в сенсоре коллектора **(пункт f);**

Рис. 5 – Конфигурация Syslog Director

****

1. Нажать «**Save**» и «**Distribute Settings to Computers**». В дереве продуктов выделить конфигурацию коллектора **Windows CEF Event Collector** и так же нажать «**Save**» и «**Distribute Settings to Computers**»
2. **Создание отчета по принятым с серверов контроллеров домена событиям ИБ:**
3. В консоли управления SSIM перейти во вкладку «**Events**»;
4. С помощью операции «**Query Wizard…**» создать новый «**Event Query**» запрос в папке «**My queries**»;
5. В настройках временных рамок запроса указать период «**last 8 hours**»;
6. В настройках запроса указать параметры выборки событий ИБ по Серверам/АРМам (указать параметры фильтра **Product *=* Windows CEF Event Collector 5.0**)**;**
7. В настройках вкладки «**Columns**» задать следующий порядок отображения полей событий в отчете (Данный порядок отображения полей события является наиболее информативным. Набор полей может быть изменен в любой момент.): *Severity ID, Vendor Severity, Category ID, Event Date, Event Type ID, Description, Effects, Vendor Signature, Windows and Novell Event Type, Windows Event Source, Collector Sensor, Created Date, Ending Event Date, Symantec Event Code, Source Host Name, IP Source Address, IP Source Port, Destination Host Name, IP Destination Address, Windows User Name, User Name, Mechanisms, Target Resource, Agent Host, Logged At, Option 5,Option 1, Event Count.*
8. В настройках архива, по которому строится запрос указать архив сервера корреляции **SSIM**;

Рис. 6 – Настройка отчета в оснастке «**Events**» консоли управления SSIM



1. Запустить созданный запрос;
2. Ознакомится с механизмом «**Event mapping**» описанным в главе «**2 – Implementation notes**» документа «**SEC\_for\_WindowsCEF\_50.pdf**» (данный документ описывает механизм работы коллектора, проанализировать поступившие на сервер корреляции SSIM события от источника

Рис. 7 – Принятые сервером SSIM события журналов ОС Windows

