System Center Endpoint Protection

Инструкция по установке и руководство пользователя

Red Hat Enterprise Linux Server 5, 6
SUSE Linux Enterprise 10, 11
CentOS 5, 6
Debian Linux 5, 6
Ubuntu Linux 10.04, 12.04
Oracle Linux 5, 6

Microsoft

Microsoft® System Center Endpoint Protection

Содержание

Введение

Благодарим за использование System Center Endpoint Protection. Современный модуль сканирования от Microsoft отличается непревзойденными скоростью сканирования и эффективностью обнаружения в сочетании с очень низким влиянием на производительность компьютера, что делает его идеальным выбором для любого сервера под управлением ОС Linux.

Основная функциональность

Модуль сканирования по требованию

Модуль сканирования по требованию может быть запущен пользователем с правами (обычно это администратор системы) через интерфейс командной строки, веб-интерфейс или с помощью средства автоматического планирования операционной системы (например, cron). Под термином По требованию понимается, что объекты файловой системы сканируются по запросу пользователя или системы.

Защита в режиме реального времени

Защита в режиме реального времени вызывается каждый раз, когда пользователь и (или) операционная система предпринимает попытку доступа к объектам файловой системы. Это также объясняет использование термина По требованию, так как сканирование запускается любой попыткой доступа к объектам файловой системы.

Основные функции системы

Современные алгоритмы модуля

Алгоритмы модуля сканирования защиты от вирусов от Microsoft обеспечивают высочайшую эффективность обнаружения и самое быстрое время сканирования.

Многопроцессорная работа

Программный продукт System Center Endpoint Protection разработан для работы как на однопроцессорных, так и на многопроцессорных машинах.

Расширенная эвристика

В System Center Endpoint Protection используется уникальная расширенная эвристика для червей Win32, заражений backdoor и других форм вредоносных программ.

Встроенные функции

Встроенные архиваторы распаковывают заархивированные объекты, избавляя от необходимости использовать какие-либо внешние программы.

Скорость и эффективность

Для повышения скорости и эффективности системы архитектура System Center Endpoint Protection основана на работающем демоне (резидентной программе), которому посылаются все запросы на сканирование.

Усовершенствованная безопасность

Все исполнительные демоны (за исключением scep_dac) работают под учетной записью пользователя без специальных прав, что призвано повысить безопасность.

Выборочная конфигурация

Система поддерживает выборочную конфигурацию в зависимости от пользователя или клиента/сервера.

Несколько уровней детализации

Можно сконфигурировать несколько уровней детализации журналов для получения информации о работе системы и о заражениях.

Веб-интерфейс

Конфигурирование и администрирование осуществляются с помощью интуитивно понятного удобного в использовании веб-интерфейса.

Отсутствие внешних библиотек

Для установки System Center Endpoint Protection не нужны внешние библиотеки и программы (за исключением LIBC).

Задаваемые пользователем уведомления

Систему можно сконфигурировать таким образом, чтобы определенные пользователи получали уведомления в случае обнаружения заражения и при возникновении других важных событий.

Умеренные системные требования

Для эффективной работы System Center Endpoint Protection нужно всего 16 МБ дискового пространства и 32 МБ оперативной памяти. Этот программный продукт отлично работает в системах Linux с ядром версий 2.2.x, 2.4.x и 2.6.x.

Производительность и масштабируемость

Идет ли речь о не слишком мощных малых офисных серверах или о серверах корпоративного класса интернет-провайдеров, обслуживающих тысячи пользователей, System Center Endpoint Protection обеспечивает производительность и масштабируемость, которых вы ожидаете от решения на базе UNIX в сочетании с непревзойденной безопасностью продуктов от Microsoft.

Терминология и сокращения

В этом разделе мы рассмотрим термины и сокращения, используемые в данном документе. Обратите внимание на то, что полужирный шрифт используется только для имен компонентов программного продукта, а также для вновь вводимых терминов и сокращений. Термины и сокращения, определения которых даны в этой главе, подробнее описываются далее в данном документе.

SCEP

SCEP — это стандартная аббревиатура, используемая для обозначения программного продукта обеспечения безопасности, разработанного Microsoft для операционных систем Linux. Также это название программного пакета, содержащего продукты.

SCEP daemon

Главный демон управления системой и сканирования SCEP: scep_daemon.

Базовый каталог SCEP

Каталог, в котором хранятся загружаемые модули SCEP, содержащие базу данных сигнатур вирусов. Для обозначения данного каталога в дальнейшем будет использоваться аббревиатура @BASEDIR@. Возможные значения @BASEDIR@ (в зависимости от операционной системы) перечислены далее.

```
Linux: /var/opt/microsoft/scep/lib
```

Каталог конфигурации SCEP

Каталог, в котором хранятся все файлы, связанные с конфигурацией System Center Endpoint Protection. Для обозначения данного каталога в дальнейшем будет использоваться аббревиатура @ETCDIR@. Возможные значения @ETCDIR@ (в зависимости от операционной системы) перечислены далее.

```
Linux: /etc/opt/microsoft/scep
```

Файл конфигурации SCEP

Главный файл конфигурации System Center Endpoint Protection. Абсолютный путь к файлу такой:

@ETCDIR@/scep.cfg

Каталог двоичных файлов SCEP

Каталог, в котором хранятся необходимые двоичные файлы System Center Endpoint Protection. Для обозначения данного каталога в дальнейшем будет использоваться аббревиатура @BINDIR@. Возможные значения @BINDIR@ (в зависимости от операционной системы) перечислены далее.

```
Linux: /opt/microsoft/scep/bin
```

Каталог системных двоичных файлов SCEP

Каталог, в котором хранятся необходимые системные двоичные файлы System Center Endpoint Protection. Для обозначения данного каталога в дальнейшем будет использоваться аббревиатура @SBINDIR@. Возможные значения @SBINDIR@ (в зависимости от операционной системы) перечислены далее.

```
Linux: /opt/microsoft/scep/sbin
```

Каталог объектных файлов SCEP

Каталог, в котором хранятся необходимые объектные файлы и библиотеки System Center Endpoint Protection. Для обозначения данного каталога в дальнейшем будет использоваться аббревиатура @LIBDIR@. Возможные значения @LIBDIR@ (в зависимости от операционной системы) перечислены далее.

```
Linux: /opt/microsoft/scep/lib
```

Установка

System Center Endpoint Protection распространяется в виде двоичного файла:

```
scep.i386.ext.bin
```

В указанном выше двоичном файле 'ext' представляет собой суффикс, зависящий от дистрибутива ОС Linux, например «deb» для Debian, «rpm» для RedHat и SuSE, «tgz» для других дистрибутивов ОС Linux.

Чтобы установить или обновить программный продукт, воспользуйтесь командой

```
sh ./scep.i386.ext.bin
```

для вывода на экран лицензионного соглашения. После подтверждения согласия с условиями соглашения установочный пакет помещается в текущий рабочий каталог, а на экран выводится соответствующая информация по установке, удалению или обновлению пакета.

После установки пакета можно убедиться в том, что основная служба SCEP работает, воспользовавшись такой командой:

```
ps -C scep_daemon
```

Если нажать клавишу ВВОД, на экран должно быть выведено такое (или аналогичное) сообщение:

```
 PID TTY TIME CMD
2226 ? 00:00:00 scep_daemon
2229 ? 00:00:00 scep_daemon
```

В фоновом режиме работает не менее двух процессов демона SCEP. Первый идентификатор процесса представляет процесс и менеджер потоков системы. Второй представляет процесс сканирования SCEP.

Установка языкового пакета

Установить языковой пакет для System Center Endpoint Protection можно с помощью следующей команды:

```
sh ./scep-lang.lng.bin
```

Здесь 'lng' необходимо заменить языковым кодом файла, который требуется импортировать.

После появления на экране уведомления Installation completed successfully измените соответствующим образом системную переменную LANG и при необходимости обновите среду. На этом установка языкового пакета завершена.

Каждый языковой пакет содержит:

- локализованный веб-интерфейс;
- локализованный консольный вывод агентов и команд SCEP;
- локализованную документацию в формате PDF.

Общие сведения об архитектуре

После успешной установки System Center Endpoint Protection нужно ознакомиться с архитектурой этого программного продукта.

Система состоит из следующих частей.

ЯДРО

Ядром System Center Endpoint Protection является демон SCEP (scep_daemon). Этот демон использует библиотеку API SCEP libscep.so и загрузочные модули SCEP em00X_xx.dat для выполнения базовых системных задач, таких как сканирование, обслуживание процессов демона агента, обслуживание системы отправки образцов, ведение журналов, уведомления и т. п. Для получения дополнительных сведений см. страницу справочника man scep_daemon(8).

АГЕНТЫ

Цель модулей агента SCEP заключается в том, чтобы интегрировать SCEP в среду сервера Linux.

УТИЛИТЫ

Модули утилит обеспечивают простое и эффективное управление системой. Они отвечают за системные задачи, такие как управление карантином, настройка и обновление системы.

КОНФИГУРАЦИЯ

Правильная конфигурация — основная составляющая системы обеспечения безопасности. Оставшаяся часть этой главы посвящена описанию всех связанных с ней компонентов. Также рекомендуется разобраться с файлом scep.cfg, поскольку в нем содержится информация, имеющая принципиально важное значение для конфигурации System Center Endpoint Protection.

После успешной установки программного продукта все компоненты конфигурации сохраняются в каталог конфигурации SCEP. Этот каталог содержит следующие файлы.

@ETCDIR@/scep.cfg

Это самый главный файл конфигурации, поскольку он контролирует все основные аспекты функциональности продукта. Файл scep.cfg состоит из нескольких разделов, каждый из которых содержит различные параметры. В этом файле есть один глобальный раздел и несколько разделов «агентов», причем имена разделов указываются в квадратных скобках. Параметры в глобальном разделе используются для задания параметров конфигурации для демона SCEP, а также значений по умолчанию для конфигурации модуля сканирования SCEP. Параметры в разделах агентов используются для задания ключей конфигурации модулей, используемых для перехвата различных типов потоков данных на компьютере и (или) в его окружении и подготовки к сканированию. Обратите внимание на то, что в дополнение к различным параметрам, используемым для конфигурирования системы, существуют также правила, которые управляют организацией файла. Для получения дополнительных сведений относительно наиболее эффективного способа организации этого файла см. страницы справочника man scep.cfg(5) и scep_daemon(8), а также страницы соответствующих агентов.

@ETCDIR@/certs

Этот каталог используется для хранения сертификатов, используемых веб-интерфейсом SCEP для аутентификации. Для получения дополнительных сведений см. страницу справочника man scep_wwwi(8).

@ETCDIR@/scripts/daemon_notification_script

Если этот сценарий активирован параметром 'exec_script' файла конфигурации SCEP, он выполняется системой защиты от вирусов в случае обнаружения заражения. Он используется для отправки по электронной почте уведомления об этом событии администратору системы.

Интеграция со службами файловой системы

В этом разделе описывается конфигурация защиты по требованию и защиты в режиме реального времени, которая обеспечивает наиболее эффективную защиту от заражения файловой системы вирусами и червями. Мощность сканирования System Center Endpoint Protection получается из команды модуля сканирования по требованию 'scep_scan' и команды модуля сканирования при доступе 'scep_dac'. В версии System Center Endpoint Protection для Linux есть дополнительный метод модуля сканирования при доступе, который использует предварительно загруженный модуль библиотеки libscep_pac.so. Все эти команды описываются в следующих разделах.

Модуль сканирования по требованию

Модуль сканирования по требованию может быть запущен пользователем с правами (обычно это администратор системы) через интерфейс командной строки, веб-интерфейс или с помощью средства автоматического планирования операционной системы (например cron). Под термином По требованию понимается, что объекты файловой системы сканируются по запросу пользователя или системы.

Для работы модуля сканирования по требованию не нужна какая-либо особая конфигурация. После правильной установки пакета SCEP модуль сканирования по требованию можно сразу же запустить с помощью интерфейса командной строки или планировщика. Для запуска модуля сканированию по требованию из командной строки воспользуйтесь таким описанным далее синтаксисом.

```
@SBINDIR@/scep_scan [option(s)] FILES
```

Здесь FILES — это список каталогов и (или) файлов, подлежащих сканированию.

При использовании модуля сканирования по требованию SCEP доступны многочисленные ключи командной строки. Полный перечень ключей доступен на странице справочника man scep_scan(8).

Защита в режиме реального времени на платформе Dazuko

Защита в режиме реального времени вызывается, когда пользователь и (или) операционная система осуществляет доступ к объектам файловой системы. Это также объясняет суть термина По требованию, так как модуль сканирования запускается при любой попытке осуществить доступ к выбранному объекту файловой системы.

Метод, используемый модулем сканирования по требованию SCEP, работает на платформе модуля ядра Dazuko (да-цу-ко) и основан на перехвате вызовов ядра. Проект Dazuko является проектом с открытым исходным кодом, что означает, что его исходный код распространяется свободно. Это дает пользователям возможность компилировать модуль ядра для своих собственных ядер. Обратите внимание на то, что модуль ядра Dazuko не является частью какого-либо продукта SCEP. Его нужно скомпилировать и установить в ядро, прежде чем использовать команду при доступе scep_dac. Метод Dazuko делает сканирование по требованию независимым от используемого типа файловой системы. Он также подходит для сканирования объектов файловой системы с помощью Network File System (NFS), Nettalk и Samba.

Внимание! Прежде чем мы предоставим подробную информацию относительно конфигурации и использования модуля сканирования по требованию, следует обратить внимание на то, что данный модуль сканирования был разработан и протестирован в первую очередь для защиты файловых систем с внешним подключением. При наличии нескольких файловых систем не с внешним подключением нужно будет исключить их из управления доступом к файлам, чтобы предотвратить зависание системы. В качестве примера стандартного каталога, который нужно исключить, можно назвать '/dev' и все каталоги, используемые SCEP.

Принцип действия

Защита в режиме реального времени scep_dac (SCEP Dazuko-powered file Access Controller) представляет собой резидентную программу, которая обеспечивает постоянное наблюдение и контроль за файловой системой. Каждый объект файловой системы сканируется на основе настраиваемых типов событий доступа к файлам. В текущей версии поддерживаются следующие типы событий.

События Open

Для того чтобы активировать этот тип доступа к файлам, укажите для параметра 'event_mask' значение «open» в разделе **[fac]** файла scep.cfg. При этом будет активирован бит ON_OPEN маски доступа Dazuko.

События Close

Для того чтобы активировать этот тип доступа к файлам, укажите для параметра 'event_mask' значение «close» в разделе **[fac]** файла scep.cfg. При этом будет активирован бит ON_OPEN маски доступа Dazuko. При этом будут активированы биты ON_CLOSE и ON_CLOSE_MODIFIED маски доступа Dazuko.

Примечание. Некоторые версии ядра ОС не поддерживают перехват событий ON_CLOSE. В этих случаях события закрытия не

будут отслеживаться scep_dac.

События Exec

Для того чтобы активировать этот тип доступа к файлам, укажите для параметра 'event_mask' значение «exec» в разделе **[fac]** файла scep.cfg. При этом будет активирован бит ON_EXEC маски доступа Dazuko.

Суть защиты в режиме реального времени заключается в том, что все открываемые, закрываемые и исполняемые файлы сначала сканируются scep_daemon на предмет наличия вирусов. В зависимости от результатов сканирования доступ к конкретным файлам запрещается или разрешается.

Установка и конфигурирование

Модуль ядра Dazuko нужно скомпилировать и установить в работающем ядре, прежде чем инициализировать scep_dac. Для получения дополнительных сведений о компиляции и установке Dazuko посетите веб-сайт

http://www.dazuko.org

После установки Dazuko проверьте и отредактируйте разделы **[global]** и **[fac]** файла конфигурации SCEP (scep.cfg). Имейте в виду, что работоспособность защиты в режиме реального времени зависит от настройки параметра 'agent_type' в разделе **[fac]** этого файла. Дополнительно нужно задать объекты файловой системы (т. е. каталоги и файлы), которые должны контролироваться функцией защиты в режиме реального времени. Это можно сделать, определив параметры ключей 'ctl_incl' и 'ctl_excl', которые также находятся в разделе **[fac]**. После внесения изменений в файл scep.cfg можно принудительно выполнить повторное считывание созданной конфигурации, перезагрузив демон SCEP.

Рекомендации

Для обеспечения загрузки модуля Dazuko до инициализации демона scep_dac выполните следующие действия.

Поместите копию модуля Dazuko в один из каталогов, зарезервированных для модулей ядра:

```
/lib/modules
```

или

```
/modules
```

Используйте утилиты ядра 'depmod' и 'modprobe' (для ОС BSD воспользуйтесь 'kldconfig' и 'kldload'), чтобы работать с зависимостями и успешно инициализировать вновь добавленный модуль Dazuko.

В сценарии инициализации scep_daemon '/etc/init.d/scep_daemon' вставьте такую строку перед оператором инициализации демона:

```
/sbin/modprobe dazuko
```

Для ОС BSD строку

```
/sbin/kldconfig dazuko
```

нужно вставить в сценарий '/usr/local/etc/rc.d/scep_daemon.sh'.

Внимание! Чрезвычайно важно, чтобы эти действия выполнялись именно в таком порядке. Если модуль ядра находится не в каталоге модулей ядра, он не будет корректно загружаться, в результате чего система будет зависать.

Защита в режиме реального времени с использованием предварительно загруженной библиотеки LIBC

В предыдущих разделах описывалась интеграция защиты в режиме реального времени на платформе Dazuko со службами файловых систем Linux/BSD. Использование Dazuko может не быть обоснованным во всех ситуациях. В том числе это верно для администраторов, обслуживающих критические системы, отличающиеся следующими характеристиками.

- Недоступны исходный код и (или) файлы конфигурации, связанные с работающим ядром.
- Ядро в большей степени является единым, нежели модульным.
- Модуль Dazuko просто не поддерживает конкретную ОС.

Во всех этих случаях нужно использовать метод сканирования по требованию, основанный на предварительно загруженной библиотеке LIBC. Подробные сведения приводятся в следующих главах данного раздела. Обратите внимание на то, что этот раздел относится только к пользователям ОС Linux и содержит информацию по эксплуатации, установке и конфигурированию модуля сканирования по требованию, использующего предварительно загруженную библиотеку 'libscep_pac.so'.

Принцип действия

Защита в режиме реального времени libscep_pac.so (SCEP Preload library based file Access Controller) представляет собой библиотеку общих объектов, которая активируется при загрузке системы. Эта библиотека используется для вызовов LIBC серверами файловой системы, такими как FTP-сервер, сервер Samba и т. д. Каждый объект файловой системы сканируется на основе настраиваемых типов событий доступа к файлам. В текущей версии поддерживаются следующие типы событий.

События Open

Этот тип доступа к файлу активируется, если в файле esest.cfg (раздел **[fac]**) в параметре 'event_mask' есть слово 'open'.

События Close

Этот тип доступа к файлу активируется, если в файле scep.cfg (раздел **[fac]**) в параметре 'event_mask' есть слово 'close' . В этом случае перехватываются все функции закрытия дескрипторов файлов и потока FILE LIBC.

События Exec

Этот тип доступа к файлу активируется, если в файле scep.cfg (раздел **[fac]**) в параметре 'event_mask' есть слово 'exec' . В этом случае перехватываются все функции exec LIBC.

Все открываемые, закрываемые и исполняемые файлы сканируются демоном SCEP на наличие вирусов. На основе результатов такого сканирования доступ к конкретным файлам запрещается или разрешается.

Установка и конфигурирование

Модуль библиотеки libscep_pac.so устанавливается с помощью стандартного механизма установки предварительно загруженных библиотек. Нужно задать переменную среды 'LD_PRELOAD', содержащую абсолютный путь к библиотеке libscep_pac.so. Для получения дополнительных сведений см. страницу справочника man ld.so(8).

Примечание. Важно, чтобы переменная среды 'LD_PRELOAD' определялась только для процессов демона сетевого сервера (ftp, Samba и т. д.), которые будут контролироваться защитой в режиме реального времени. В целом не рекомендуется предварительно загружать вызовы LIBC для всех процессов операционной системы, так как это может значительно замедлить производительность системы и даже привести к ее зависанию. Именно поэтому не следует использовать файл '/etc/ld.so.preload', а также выполнять глобальный экспорт переменной среды 'LD_PRELOAD'. И в том, и в другом случае будут изменены все соответствующие вызовы LIBC, что может привести к зависанию системы при инициализации.

Чтобы перехватывались только необходимые вызовы доступа к файлам в рамках конкретной файловой системы, исполняемые операторы можно скорректировать с помощью такой строки:

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

Здесь 'COMMAND COMMAND-ARGUMENTS' является исходным исполняемым оператором.

Проверьте и отредактируйте разделы **[global]** и **[fac]** файла конфигурации SCEP (scep.cfg). Чтобы модуль сканирования при доступе работал корректно, нужно задать объекты файловой системы (т. е. каталоги и файлы), которые должны контролироваться предварительно загруженной библиотекой. Это можно сделать, задав параметры ключей 'ctl_incl' и 'ctl_excl' в разделе **[fac]** файла конфигурации SCEP. После внесения изменений в файл scep.cfg можно принудительно выполнить повторное считывание созданной конфигурации, перезагрузив демон SCEP.

Рекомендации

Для того чтобы активировать защиту в режиме реального времени сразу после запуска файловой системы, нужно задать переменную среды 'LD_PRELOAD' в соответствующем сценарии инициализации сетевого файлового сервера.

Пример. Предположим, нужно, чтобы модуль сканирования при доступе отслеживал все события доступа файловой системы сразу после запуска сервера Samba. В сценарии инициализации демона Samba (/etc/init.d/smb) следует заменить оператор

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

на строку

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

В таком случае выбранные объекты файловой системы, контролируемые Samba, будут сканироваться при запуске системы.

Важные механизмы SCEP

Политика обработки объектов

Механизм политики обработки объектов обеспечивает фильтрацию просканированных объектов в зависимости от их статуса. Эта функциональность основана на использовании следующих ключей конфигурации.

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

Для получения дополнительных сведений об этих ключах см. страницу справочника man scep.cfg(5).

Каждый обрабатываемый объект сначала обрабатывается в соответствии с конфигурацией ключа 'action_av'. Если для этого ключа выбрано значение 'accept' (или 'defer', 'discard', 'reject'), объект принимается (или задерживается, отменяется, отклоняется). Если же для ключа выбрано значение 'scan', то данный объект сканируется на наличие заражений вирусами, а если для ключа 'av_clean_mode' указано значение 'yes', то этот объект также очищается. Кроме того, ключи конфигурации 'action_av_infected', 'action_av_notscanned' и 'action_av_deleted' также учитываются, чтобы оценить дальнейшую обработку объекта. Если на основе этих трех ключей действий было выполнено действие 'accept', объект принимается. В противном случае он блокируется.

Пользовательская конфигурация

Цель механизма пользовательской конфигурации заключается в том, чтобы обеспечить более высокий уровень пользовательской настройки и обширную функциональность. Он позволяет администратору системы задать параметры модуля сканирования защиты от вирусов SCEP в зависимости от пользователя, осуществляющего доступ к объектам файловой системы.

Подробное описание этой функциональности приводится на странице справочника man scep.cfg(5). В этом разделе мы приведем лишь краткий пример пользовательской конфигурации.

В данном примере цель заключается в том, чтобы использовать модуль scep_dac для управления событиями доступа ON_OPEN и ON_EXEC для внешнего диска, подключаемого через каталог /home. Этот модуль можно сконфигурировать в разделе **[fac]** файла конфигурации SCEP. См. далее.

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

Для того чтобы указать параметры сканирования для отдельного пользователя, в параметре 'user_config' должно быть указано имя особого файла конфигурации, в котором будут храниться индивидуальные правила сканирования. В показанном здесь примере особый файл конфигурации называется 'scep_dac_spec.cfg' и расположен в каталоге конфигурации SCEP (сам каталог зависит от вашей операционной системы, см. страницу Терминология и сокращения).

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

Когда параметр файла 'user_config' указан в разделе **[fac]**, нужно создать файл 'scep_dac_spec.cfg' в каталоге конфигурации SCEP. Наконец, добавьте нужные правила сканирования.

```
[username]
action_av = "reject"
```

В верхней части особого раздела введите имя пользователя, к которому будут применяться индивидуальные правила. Эта конфигурация позволит осуществить нормальную обработку всех прочих пользователей, которые пытаются получить доступ к файловой системе. Это значит, что все объекты файловой системы, к которым осуществляют доступ другие пользователи, будут сканироваться на предмет заражений, а пользователь 'username' будет исключением: ему будет отказано в доступе (он будет заблокирован).

Планировщик

Среди функций планировщика можно назвать выполнение запланированных задач в указанное время или при возникновении определенного события, управление задачами с предопределенной конфигурацией и свойствами и их запуск и многое другое. Конфигурацию и свойства задачи можно использовать для изменения дат и времени запуска, а также для расширения применения задач путем внедрения собственных профилей при выполнении задач.

Ключ 'scheduler_tasks' комментируется по умолчанию, вызывая применение конфигурации планировщика по умолчанию. В файле конфигурации SCEP все параметры и задачи разделяются точкой с запятой. Все прочие точки с запятой (и обратные косые черты) должны отделяться обратной косой чертой. У каждой задачи есть 6 параметров, синтаксис которых описан далее.

- id — уникальный номер.
- name — описание задачи.
- flags — параметр, позволяющий задать особые флаги для отключения указанной задачи планировщика.
- failstart — инструкция относительно того, что следует делать, если задачу не удалось выполнить в запланированный день.
- datespec — обычный формат даты с шестью полями (расширенный формат года наподобие crontab), повторяющаяся дата или имя события.
- command — абсолютный путь к команде, за которым следуют ее аргументы, или особое имя команды с префиксом «@» (например, обновление защиты от вирусов: @update).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

Вместо ключа datespec можно использовать перечисленные далее имена событий.

- start — запуск демона.
- startonce — запуск демона не чаще одного раза в день.
- engine — успешное обновление модуля.
- login — запуск веб-интерфейса путем осуществления входа.
- threat — обнаружена угроза.
- notscanned — непросканированный файл.

Для вывода на экран текущей конфигурации планировщика используйте веб-интерфейс или выполните такую команду:

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

Подробное описание планировщика и его параметров см. в разделе «Планировщик» страницы справочника man, посвященной scep_daemon(8).

Веб-интерфейс

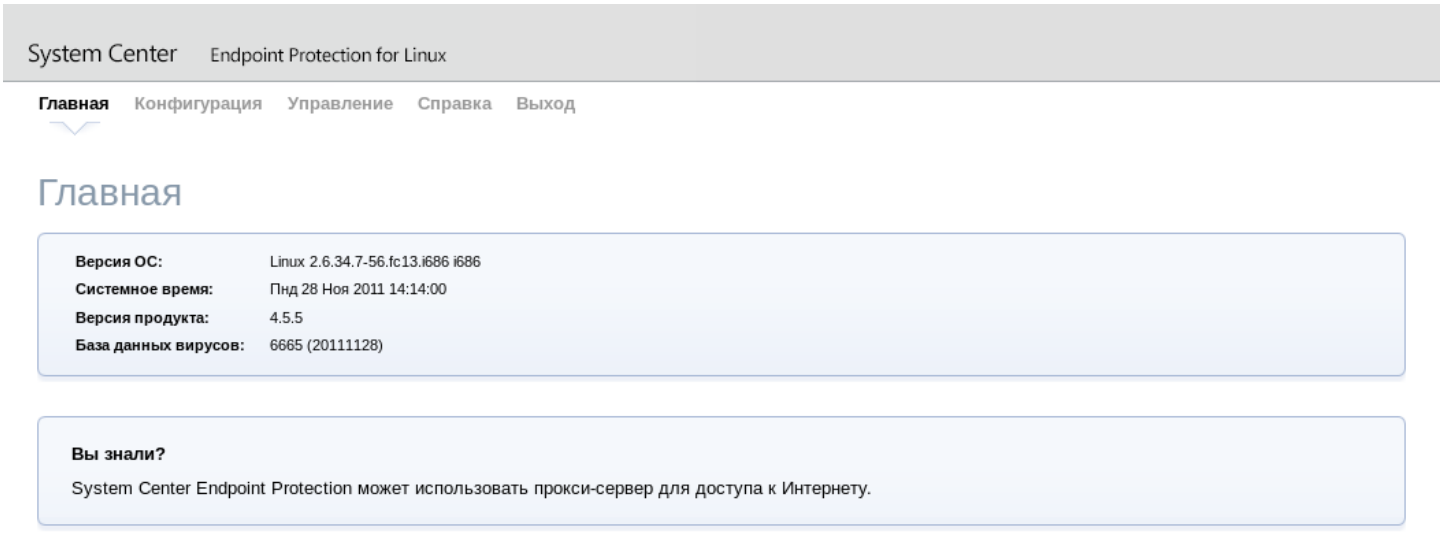
Веб-интерфейс дает пользователю возможность легко выполнять конфигурирование и администрирование систем обеспечения безопасности SCEP. Этот модуль является отдельным агентом и должен быть явным образом включен. Для того чтобы быстро сконфигурировать веб-интерфейс, задайте следующие ключи в файле конфигурации SCEP и перезапустите демон SCEP.

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

Замените показанный курсивом текст своими собственными значениями и укажите в адресной строке браузера 'https://address:port' (обратите внимание на https). Осуществите вход в систему, указав 'имя пользователя и пароль'. Базовые указания по использованию можно найти на странице справки, а технические сведения о scep_wwwi приводятся на странице справочника man scep_wwwi(1).

Веб-интерфейс позволяет получать удаленный доступ к демону SCEP и легко осуществлять его развертывание. Эта мощная утилита позволяет легко считывать и записывать значения конфигурации.

Рисунок 6-1. System Center Endpoint Protection: главный экран.



Окно веб-интерфейса System Center Endpoint Protection разделено на две главные части. В основном окне отображается содержимое выбранного пункта меню и главное меню. Эта горизонтальная панель в верхней части окна позволяет переходить между описанными далее основными разделами.

- **Главная**: раздел с базовыми сведениями о системе и программном продукте Microsoft.
- **Конфигурация**: раздел, где можно изменить конфигурацию системы System Center Endpoint Protection.
- **Управление**: здесь можно выполнять простые задачи и просматривать глобальную статистику по объектам, которые обрабатывает scep_daemon.
- **Справка**: раздел с подробными инструкциями по использованию веб-интерфейса System Center Endpoint Protection.
- **Выход**: возможность закончить текущий сеанс.

Внимание! Не забудьте нажать кнопку **Сохранить изменения** после внесения любых изменений в разделе **Конфигурация** веб-интерфейса, чтобы сохранить новые параметры. Для того чтобы применить параметры, нужно будет перезапустить демон SCEP, нажав кнопку **Применить изменения** в левой части экрана.

Пример конфигурации защиты в режиме реального времени

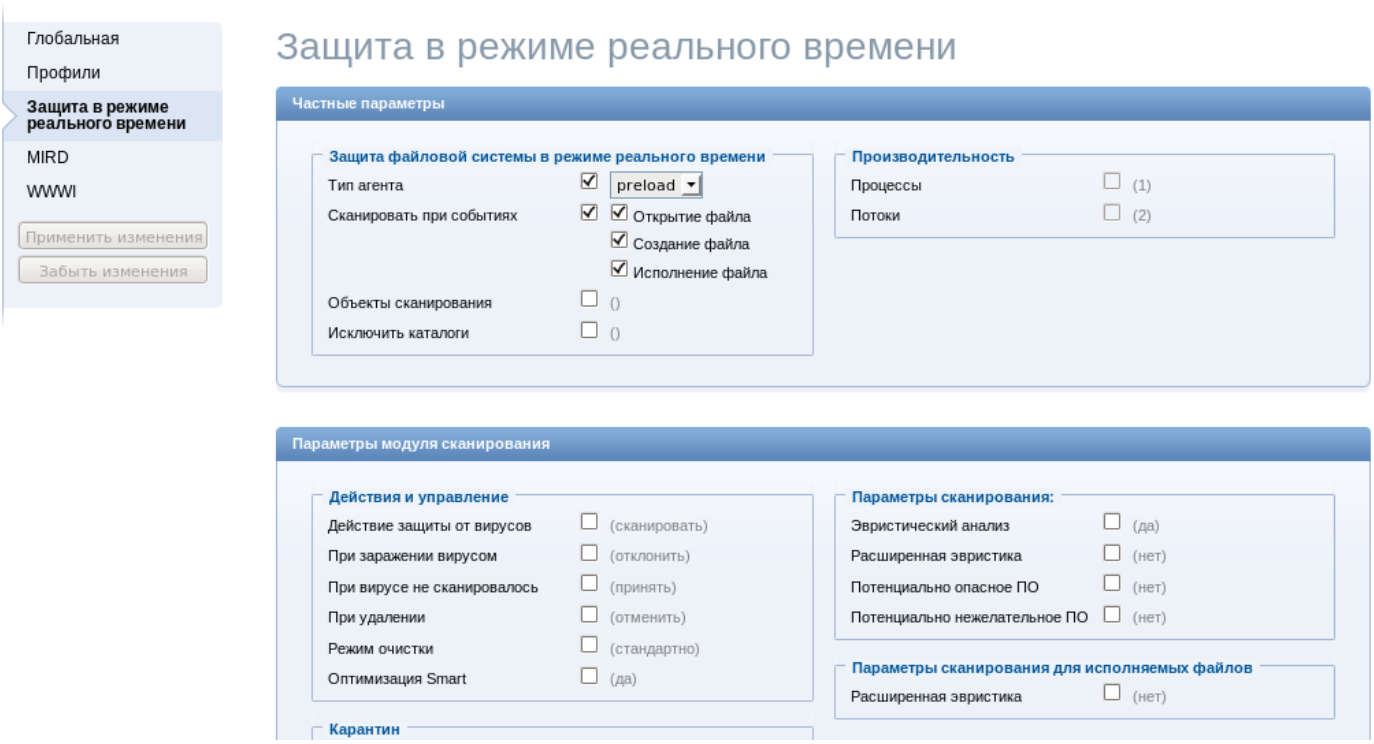
Конфигурировать SCEP можно одним из двух способов. В нашем примере будет продемонстрировано, как с помощью любого из них настроить модуль управления доступом, который описан в главе Защита в режиме реального времени с использованием предварительно загруженной библиотеки LIBC. Можно выбрать тот вариант, который лучше вам подходит.

- Использование файла конфигурации SCEP

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- Использование веб-интерфейса

Рисунок 6-3. SCEP: Конфигурация > Модуль сканирования при доступе.



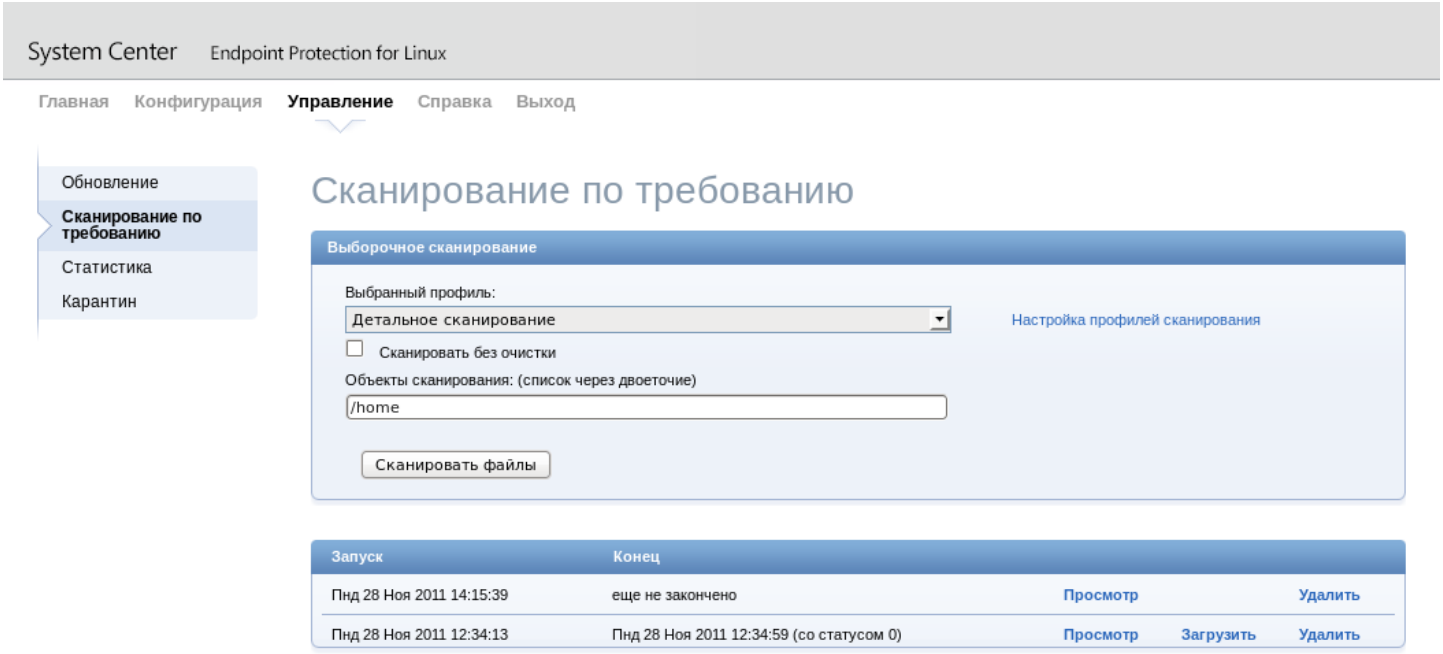
При изменении параметров с помощью веб-интерфейса нужно не забывать сохранять конфигурацию, нажимая для этого кнопку **Сохранить изменения**. Для того чтобы применить внесенные изменения, нажмите кнопку **Применить изменения** на панели разделов **Конфигурация**.

Модуль сканирования по требованию

В этом разделе приводится пример того, как следует запускать модуль сканирования по требованию, чтобы выполнять сканирование на наличие вирусов.

- Перейдите в раздел **«Управление» > «Сканирование по требованию»**.
- Укажите путь к каталогу, который нужно просканировать
- Запустите модуль сканирования командной строки, нажав кнопку **Сканировать файлы**.

Рисунок 6-4. SCEP: Управление > Сканирование по требованию.

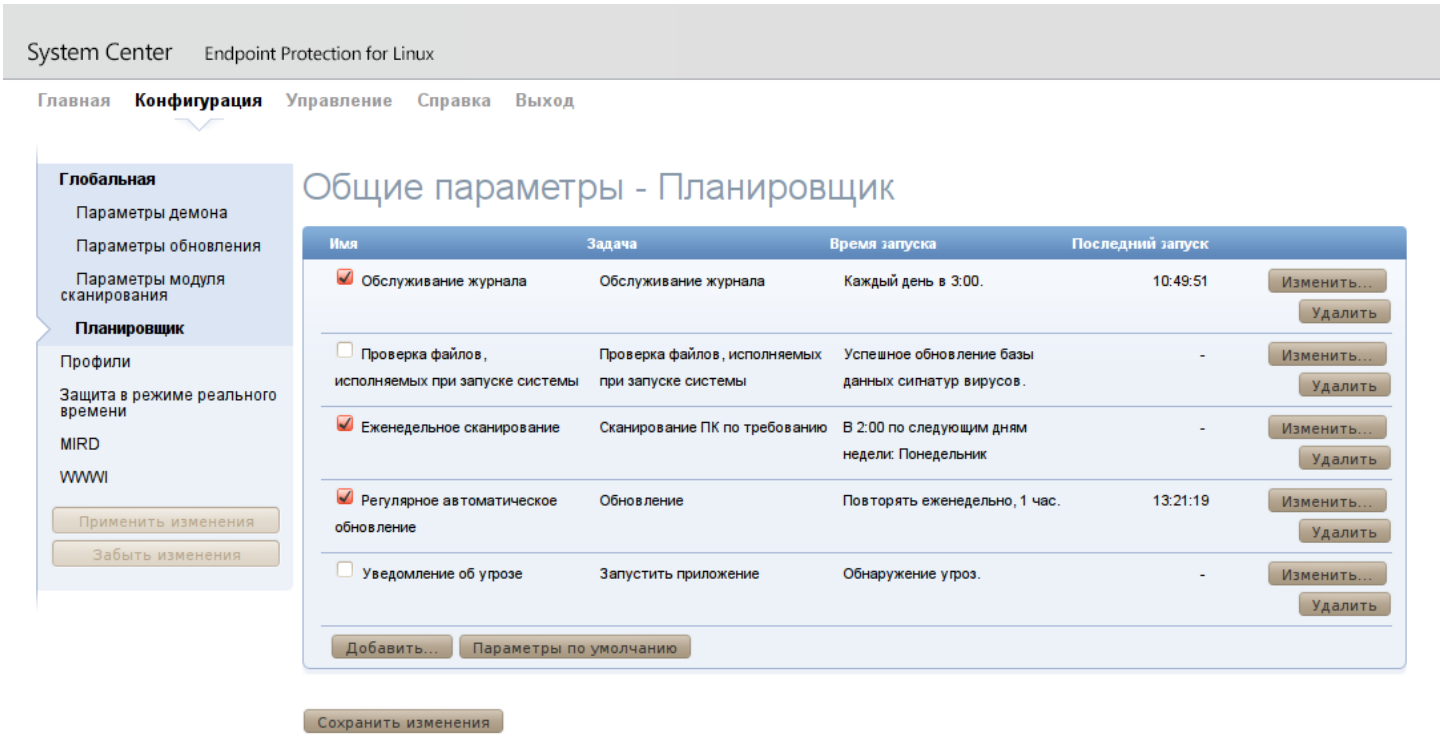


Модуль сканирования командной строки Microsoft будет автоматически запущен в фоновом режиме. Чтобы увидеть ход выполнения сканирования, нажмите ссылку **Просмотр**. Будет открыто новое окно браузера.

Планировщик

Управлять задачами планировщика можно с помощью файла конфигурации SCEP (см. раздел Планировщик) либо веб-интерфейса.

Рисунок 6-5. SCEP: Глобальная > Планировщик.



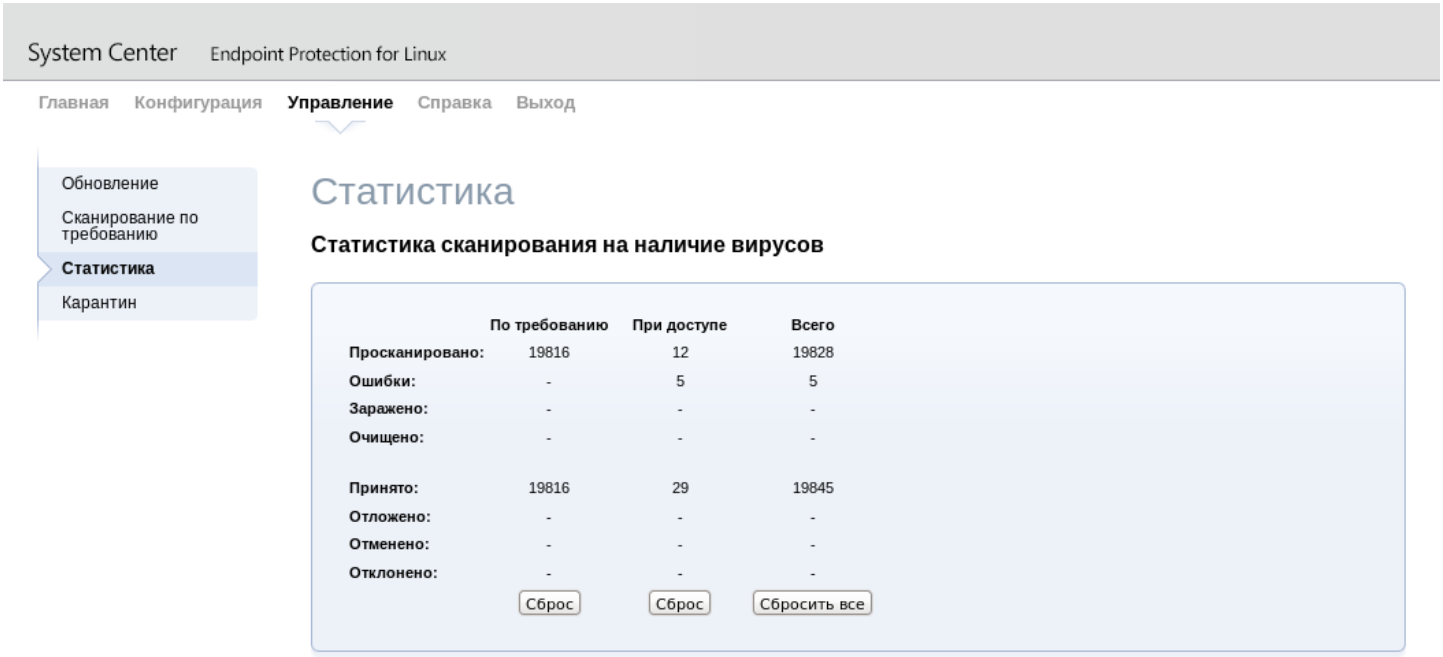
Установите флажок, чтобы включить или отключить запланированную задачу. По умолчанию в планировщике отображаются следующие запланированные задачи.

- **Обслуживание журнала**: программа автоматически удаляет старые журналы, чтобы сэкономить дисковое пространство. Планировщик запустит дефрагментацию журналов. При этом удаляются все пустые записи журналов, что улучшает скорость работы с журналами. Это улучшение более заметно, если в журналах содержится большое количество записей.
- **Проверка файлов, исполняемых при запуске системы**: выполняется сканирование памяти и запущенных служб после успешного обновления базы данных сигнатур вирусов.
- **Еженедельное сканирование**: каждую неделю (по умолчанию в понедельник в 02:00) сканируется вся файловая система. Пользователь может настроить эту задачу.
- **Регулярное автоматическое обновление** — лучший способ добиться максимального уровня безопасности компьютера. Дополнительные сведения см. в разделе Программа обновления SCEP.
- **Уведомление об угрозе**: по умолчанию каждая угроза регистрируется в syslog. Кроме того, SCEP можно сконфигурировать на выполнение внешнего сценария, который будет уведомлять системного администратора по электронной почте об обнаружении угрозы.

Статистика

Здесь можно просмотреть статистику для всех активных агентов SCEP. Сводная информация в разделе **Статистика** обновляется каждые 10 секунд.

Рисунок 6-6. SCEP: Управление > Статистика.



Ведение журнала

SCEP обеспечивает ведение журнала демона системы с помощью syslog. Syslog является стандартом для регистрации программных сообщений и может использоваться для ведения журнала системных событий, таких как события, связанные с сетью и с безопасностью.

Сообщения относятся к средству журнала:

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

Отправителем сообщениям присваивается приоритет или уровень:

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

В этом разделе описывается, как сконфигурировать и прочитать результат ведения журнала syslog. Ключ 'syslog_facility' (значение по умолчанию 'daemon') определяет используемое средство ведения журнала syslog. Для изменения настроек syslog отредактируйте файл конфигурации SCEP или используйте веб-интерфейс. Измените значение параметра 'syslog_class', чтобы изменить класс ведения журнала. Рекомендуется менять эти параметры только в том случае, если вы хорошо знакомы с syslog. Пример конфигурации syslog приведен ниже.

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

Имя и местонахождение файла журнала зависят от установки и конфигурации syslog (например, rsyslog, syslog-ng и т. д.). В качестве стандартных имен для выходных файлов syslog используются, например, 'syslog', 'daemon.log' и т. д. Для отслеживания работы syslog выполните одну из следующих команд с консоли:

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

Внимание! Необходимо сначала включить отслеживание продукта Linux SCEP с помощью менеджера операций System Center в файле конфигурации или веб-интерфейсе SCEP. Убедитесь, что в этом файле параметр 'scom_enabled' задан как 'scom_enabled = yes', или измените его с помощью веб-интерфейса в разделе **Конфигурация** > **Глобальная** > **Параметры демона** > **Программа SCOM включена**.

Обновление системы обеспечения безопасности SCEP

Программа обновления SCEP

Для обеспечения эффективной работы System Center Endpoint Protection нужно поддерживать актуальность базы данных сигнатур вирусов. Именно для этого была разработана программа scep_update. Для получения дополнительных сведений см. страницу справочника man scep_update(8). Если сервер получает доступ в Интернет через прокси HTTP, также нужно задать дополнительные ключи конфигурации 'proxy_addr', 'proxy_port'. Если для доступа к прокси HTTP нужны имя пользователя и пароль, также в этом разделе нужно задать ключи 'proxy_username' и 'proxy_password'. Для инициализации обновления выполните такую команду:

@SBINDIR@/scep_update

Для того чтобы обеспечить максимально высокий уровень безопасности для конечного пользователя, коллектив Microsoft постоянно собирает определения вирусов из разных стран мира, а новые шаблоны добавляются в базу данных сигнатур вирусов через очень короткие отрезки времени. Поэтому мы рекомендуем регулярно запускать процесс обновления. Чтобы указать частоту выполнения обновления, нужно сконфигурировать задачу '@update' в ключе 'scheduler_tasks' в разделе **[global]** файла конфигурации SCEP. Также можно использовать планировщик, чтобы указать частоту выполнения обновления. Демон SCEP должен работать, чтобы успешно обновлять базу данных сигнатур вирусов.

Описание процесса обновления SCEP

Процесс обновления состоит из двух этапов. На первом этапе предкомпилированные модули обновления загружаются с сервера Microsoft.

Второй этап процесса обновления заключается в компиляции модулей, загружаемых модулем сканирования System Center Endpoint Protection с тех модулей, которые хранятся на локальном зеркале. Обычно создаются следующие загрузочные модули SCEP: модуль загрузчика (em000.dat), модуль сканирования (em001.dat), модуль базы данных сигнатур вирусов (em002.dat), модуль поддержки архивов (em003.dat), модуль расширенной эвристики (em004.dat) и т. д. Эти модули создаются в следующем каталоге:

@BASEDIR@

Ваши отзывы

Мы надеемся, что это руководство помогло вам полностью понять требования, связанные с установкой, конфигурированием и обслуживанием System Center Endpoint Protection. Однако наша цель заключается в том, чтобы постоянно повышать качество и эффективность документации. Если вам кажется, что какие-либо разделы данного руководства недостаточно ясные или полные, сообщите нам об этом, обратившись в службу поддержки клиентов:

support.microsoft.com

Мы стремимся обеспечивать самый высокий уровень поддержки и с радостью поможем вам при возникновении любых проблем с этим программным продуктом.

Приложение A. Лицензия PHP