System Center Пакет мониторинга для Endpoint Protection для Linux

Корпорация Майкрософт

Дата публикации: 10/26/2015

Отзывы и предложения по этому документу отправляйте по адресу mpgfeed@microsoft.com. Просим вас указывать в них название руководства по использованию пакета управления.

Коллектив разработчиков Operations Manager будет благодарен вам, если вы оставите отзыв о пакете мониторинга на соответствующей странице в каталоге пакетов управления (http://go.microsoft.com/fwlink/?LinkID=82105).

Содержание

Руководство по использованию пакета управления SCEP

Этот пакет управления позволяет централизованно администрировать System Center Endpoint Protection (SCEP) с помощью System Center 2012 Operations Manager в сетевой среде, в том числе на рабочих станциях и серверах. Система управления задачами Operations Manager дает возможность управлять SCEP на удаленных компьютерах, просматривать предупреждения и состояния работоспособности системы, а также своевременно реагировать на возникающие проблемы и угрозы.

Сам менеджер System Center 2012 Operations Manager не обеспечивает какую-либо иную защиту от злонамеренного кода. System Center 2012 Operations Manager зависит от решения SCEP на компьютерах с системой Linux.

Это руководство составлено на основе данных о версии 4.5.10.1 пакета управления для SCEP.

История руководства

Версия	Дата выпуска	Изменения
4.5.9.1	05/16/2012	Исходная версия этого руководства.
4.5.10.1	11/06/2012	Новые поддерживаемые версии Linux. Улучшенное описание для некоторых средств пакета управления.

Изменения в версии 4.5.10.1

Версия 4.5.10.1 пакета управления для System Center Endpoint Protection включает в себя следующие изменения.

- Новые поддерживаемые версии Linux:
  - Red Hat Enterprise Linux Server 5;
  - SUSE Linux Enterprise 10;
  - CentOS 5, 6;
  - Debian Linux 5, 6;
  - Ubuntu Linux 10.04, 12.04;
  - Oracle Linux 5, 6.

  Примечание. Эти новые версии будут поддерживаться только при использовании System Center 2012 Operations Manager с пакетом обновления 1 и выше.
- Улучшено описание для:
  - монитора активных вредоносных программ;
  - предупреждения об активных вредоносных программах (из правила).

Поддерживаемые конфигурации

Общие сведения о поддерживаемых конфигурациях см. в статье Поддерживаемые конфигурации Operations Manager 2007 R2 (http://go.microsoft.com/fwlink/?LinkId=90676).

Для использования этого пакета управления необходим продукт System Center 2012 Operations Manager 2007 R2 или более поздней версии. В приведенной ниже таблице указаны поддерживаемые пакетом операционные системы.

Название операционной системы	x86	x64
Red Hat Enterprise Linux Server 5, 6	Да	Да
SUSE Linux Enterprise 10, 11	Да	Да
CentOS 5, 6	Да	Да
Debian Linux 5, 6	Да	Да
Ubuntu Linux 10.04, 12.04	Да	Да
Oracle Linux 5, 6	Да	Да

Требования

Чтобы можно было запустить этот пакет управления, должны быть выполнены указанные ниже требования.

- Накопительное обновление 5 для System Center Operations Manager 2007 R2 (http://support.microsoft.com/kb/2449679)

Указанные ниже пакеты управления для SCEP интегрированы в систему System Center 2012 Operations Manager 2007 R2 или предлагаются для загрузки в интернет-каталоге.

ИД	Имя	Версия

Microsoft.Linux.Library	Библиотека операционной системы Linux	6.1.7000.256
Microsoft.SystemCenter.InstanceGroup.Library	Библиотека группы экземпляров	6.1.7221.0
Microsoft.SystemCenter.Library	Библиотека ядра System Center	6.1.7221.0
Microsoft.SystemCenter.WSManagement.Library	Библиотека службы WS-Management	6.1.7221.0
Microsoft.SystemCenter.DataWarehouse.Library	Библиотека хранилища данных	6.1.7221.0
Microsoft.Unix.Library	Библиотека ядра Unix	6.1.7000.256
Microsoft.Unix.Service.Library	Библиотека шаблонов служб Unix	6.1.7221.0
Microsoft.Windows.Library	Библиотека ядра Windows	6.1.7221.0
System.Health.Library	Библиотека работоспособности	6.1.7221.0
System.Library	Системная библиотека	6.1.7221.0

Внимание! Необходимо сначала включить отслеживание продукта Linux SCEP с помощью System Center 2012 Operations Manager в файле конфигурации */etc/opt/microsoft/scep/scep.cfg* 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**.

Файлы в этом пакете управления

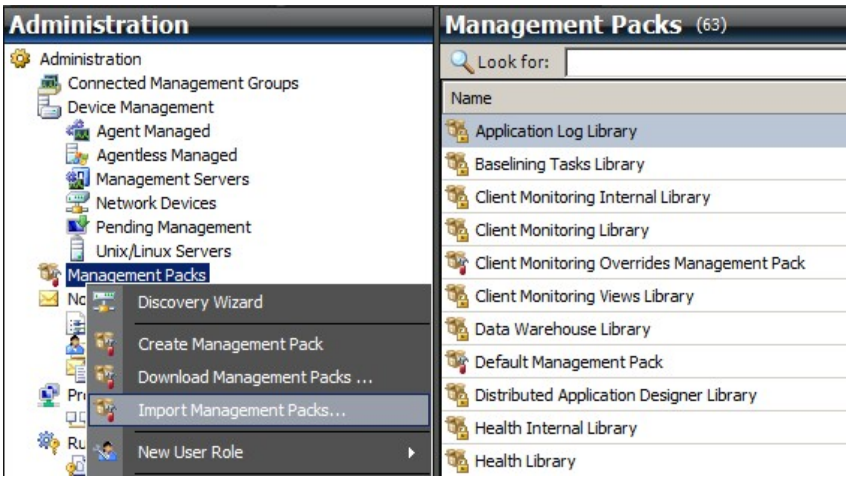
Пакет управления для SCEP содержит указанные ниже файлы.

Имя файла	Описание
Microsoft.SCEP.Linux.Library.mp	Содержит определения классов и описания связей между ними, а также определения типов мониторов и модулей.
Microsoft.SCEP.Linux.Application.mp	Содержит реализацию отслеживания, предупреждений, задач и представлений.

Быстрый запуск

Чтобы приступить к наблюдению за системой SCEP, необходимо импортировать пакеты управления в среду Operations Manager и указать компьютеры, за которыми следует наблюдать (этот процесс называется обнаружением).

Импорт пакетов управления

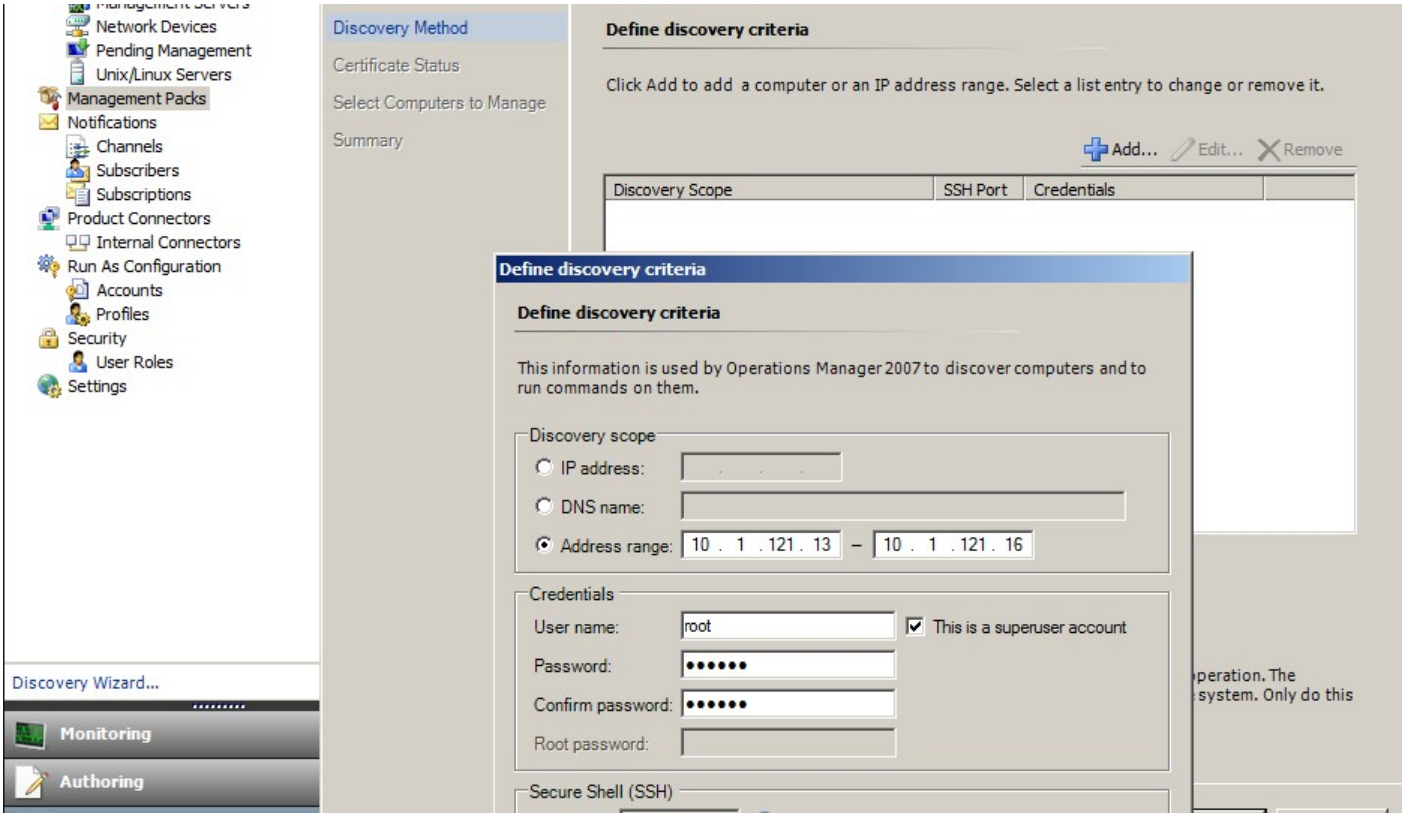


1. Щелкните рабочую область **Administration** на левой панели окна консоли управления.
2. Щелкните пункт **Management Packs** правой кнопкой мыши и выберите в контекстном меню команду **Import Management Packs...**.
3. В окне пакетов управления нажмите кнопку **Add** и выберите в раскрывающемся меню команду **Add from disk...**.
4. Подтвердите, что вы хотите, чтобы система Operations Manager находила и устанавливала зависимости не только на локальных дисках. Для этого нажмите кнопку **Yes** во всплывающем окне **Online Catalog Connection** .
5. Выделите оба указанных файла (Microsoft.SCEP.Linux.Application.mp и Microsoft.SCEP.Linux.Library.mp) и нажмите кнопку **Install**.

Примечание. Дополнительные инструкции по импорту пакета управления см. в статье Импорт пакета управления в Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkId=142351).

Обнаружение

После успешного импорта MP-файлов необходимо выполнить обнаружение компьютеров.



1. В рабочей области **Administration** (на левой панели окна консоли управления) щелкните ссылку **Discovery wizard…** (в нижней части).
2. В мастере управления компьютерами и устройствами выберите параметр **Unix/Linux computers** и нажмите кнопку **Next**, чтобы продолжить.
3. В разделе определения критериев обнаружения нажмите кнопку **Add**.
4. Укажите сканируемый **Address range** IP и **Credentials** SSH, относящиеся к компьютерам, на которые System Center 2012 Operations Manager установит свой агент.
5. Подтвердите диапазон и учетные данные с помощью кнопки **OK** и нажмите кнопку **Discover**, чтобы начать обнаружение.
6. После его завершения на экране появится список, в котором можно будет выбрать системы для отслеживания и управления.

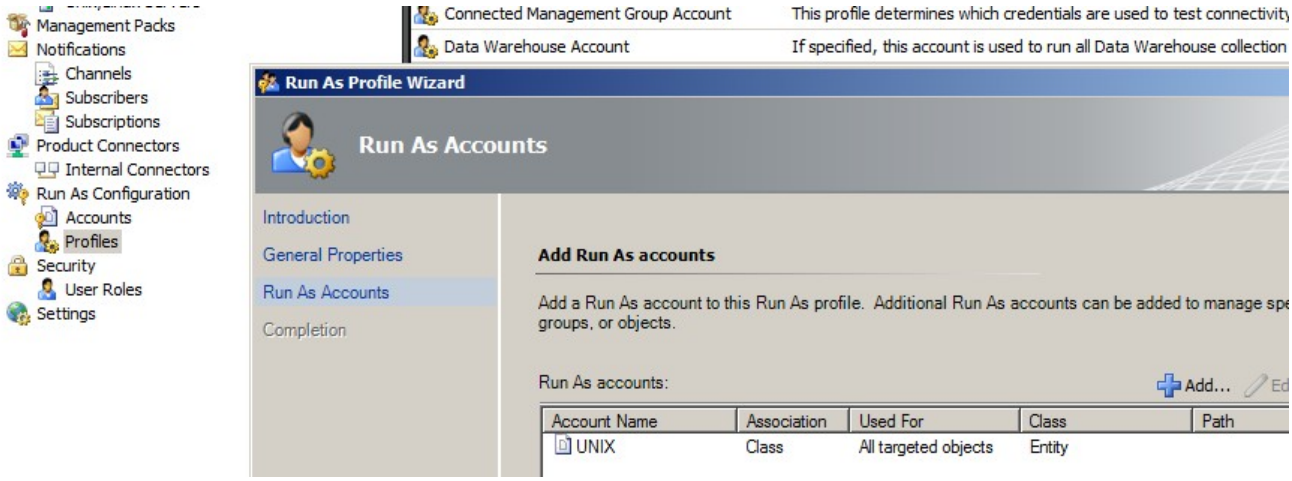
Примечание. Возможность установки агента для Linux поддерживается в этих версиях системы Linux. Если установить агент для Linux с помощью функции обнаружения невозможно, ознакомьтесь с инструкциями по его установке вручную в статье Майкрософт Установка кроссплатформенных агентов вручную (http://technet.microsoft.com/ru-ru/library/dd789016.aspx).

Примечание.Обнаружение серверов Linux с помощью системы SCEP автоматически повторяется каждые восемь часов для всех компьютеров с системой Linux, управляемых в среде Operations Manager (то есть компьютеров, на которых установлен пакет управления для соответствующей версии Linux). В процессе обнаружения создаются все объекты сервисного модуля: защищенный сервер Linux и вложенные объекты либо незащищенный сервер Linux (см. соответствующие разделы). Установка SCEP считается полностью завершенной при наличии службы scep_daemon (остановленной или работающей). Таким образом, первое обнаружение выполняется при установке пакета управления, а следующее — через восемь часов (в соответствии с циклом обнаружения). При удалении продукта SCEP соответствующий сервер автоматически переводится в число незащищенных (серверов без SCEP) и наоборот.

Настройка учетных записей запуска от имени

Чтобы создать учетную запись Unix, воспользуйтесь приведенными ниже инструкциями.

1. В рабочей области **Administration** (левая панель) откройте раздел **Run As Configuration** > **Accounts**.
2. Чтобы создать новую учетную запись, откройте раздел **Actions** на панели **Действия** (правая панель) и выберите команду **Создать учетную запись запуска от имени...**.
3. В окне общих свойств выберите пункт **Basic Authentication** в раскрывающемся меню **Run As Account type**.
4. Созданную учетную запись необходимо добавить в профиль для ее дальнейшего распространения. Для этого щелкните правой кнопкой мыши профиль **Unix Privileged Account** в разделе **Run As Configuration** > **Profiles**, выберите пункт **Properties** и выполните назначение учетной записи, следуя инструкциям мастера.



Примечание. Дополнительные сведения о создании учетной записи запуска от имени см. в статье Настройка кроссплатформенной учетной записи запуска от имени (http://go.microsoft.com/fwlink/?LinkId=160348) в интернет-библиотеке System Center 2012 Operations Manager 2007 R2.

После выполнения описанных действий обнаруженные серверы Linux вскоре (в течение нескольких минут) появятся в разделе **Monitoring** > **System Center Endpoint Protection Linux** > **Сервера с SCEP**.

Установка языкового пакета для SCEP

Языковой пакет имеет следующий формат:
Microsoft.SCEP.Linux.Application.LNG.mp и Microsoft.SCEP.Linux.Library.LNG.mp

Языковой пакет устанавливается с помощью действий, описанных в разделе **Импорт пакетов управления** выше. Чтобы отобразить установленный язык в System Center 2012 Operations Manager, выполните указанные ниже действия.

1. Нажмите кнопку **Пуск** в Windows и выберите пункт **Панель управления**.
2. На панели управления щелкните пункт **Язык и региональные стандарты**.
3. Измените региональные настройки системы для программ, не поддерживающих Unicode, на вкладке **Администрирование**. На вкладке **Расположение** выберите текущее расположение в соответствии с установленным языковым пакетом.

Назначение пакета управления

Пакет управления для SCEP обеспечивает указанные ниже возможности.

- Наблюдение за инцидентами в системе безопасности и ее работоспособностью и генерирование соответствующих предупреждений в режиме реального времени.
- Удаленное выполнение связанных с безопасностью задач на серверах для устранения проблем с доступностью.

Режимы просмотра

Администратор сервера может с помощью консоли Operations Manager наблюдать за всеми компьютерами, на которых установлена система SCEP. Ниже указаны режимы просмотра System Center Endpoint Protection Linux.

- **Активные предупреждения** — все активные предупреждения SCEP всех уровней серьезности. Закрытые предупреждения не учитываются.
- **Панель мониторинга** — вкладки «Сервера с SCEP» и «Активные предупреждения».
- **Сервера с SCEP** — все защищенные серверы Linux.
- **Сервера без SCEP** — все незащищенные серверы Linux.
- **Состояние задачи** — список всех выполненных задач.

При наблюдении за состоянием SCEP с помощью пакета управления для System Center 2012 Operations Manager можно

мгновенно оценить работоспособность SCEP.

Не ожидая возникновения предупреждения, можно в любой момент просмотреть сводное состояние компонентов SCEP, щелкнув панель **Monitoring** > **System Center Endpoint Protection Linux** > **Сервера с SCEP** в консоли мониторинга Operations Manager. Состояние компонента указывается в поле «Состояние» с помощью цветных значков.

Значок	Состояние	Описание
	Healthy	Зеленый значок указывает на успешное выполнение операции или наличие информации, не требующей вмешательства.
	Warning	Желтый значок обозначает ошибку или предупреждение.
	Critical	Красный значок обозначает критическую ошибку или проблему с безопасностью либо недоступность службы.
	Not monitored	Отсутствие значка говорит о том, что не собрано никаких данных, влияющих на состояние.

Список объектов в режиме просмотра может быть довольно длинным. Для поиска нужного объекта или группы объектов можно использовать кнопки «Область», «Поиск» и «Найти» на панели инструментов Operations Manager. Дополнительные сведения см. в статье Управление данными наблюдения с помощью кнопок «Область», «Поиск» и «Найти» (http://go.microsoft.com/fwlink/?LinkId=91983).

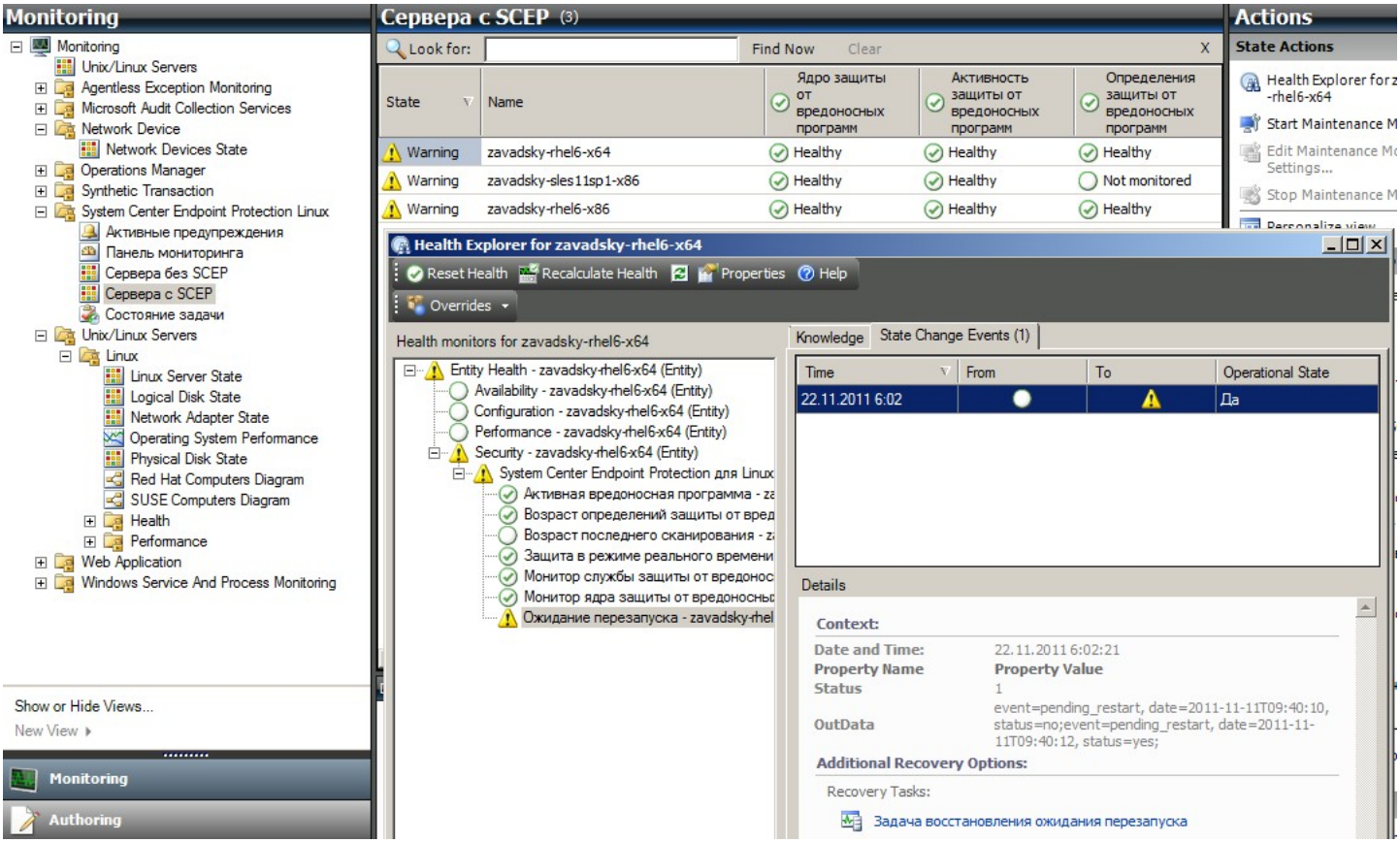
Мониторы

В среде Operations Manager 2007 с помощью мониторов можно оценивать состояние контролируемых объектов.

Всего в SCEP есть 17 мониторов.

- Девять базовых мониторов: основные компоненты системы мониторинга, которые используются для наблюдения за счетчиками, событиями, скриптами и службами.
- Два составных монитора: используются для группировки нескольких базовых мониторов в один, который затем применяется для указания состояния работоспособности и создания предупреждений.
- Шесть мониторов зависимостей — ссылки на сведения о состоянии существующих мониторов.

Примечание. Дополнительные сведения о мониторах см. в справке к Operations Manager 2007 R2 (нажмите клавишу F1 в System Center 2012 Operations Manager).



Ниже приведено описание структуры и свойств мониторов работоспособности SCEP.

Активная вредоносная программа

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Отслеживает текстовый файл журнала: /var/log/scep/eventlog_scom.dat
Интервал	При событии
Предупреждение	Да. Автоматическое разрешение не выполняется.
Алгоритм сброса	Автоматический возврат в работоспособное состояние через 8 часов. Предупреждение остается активным, чтобы сохранить сведения о необработанной вредоносной программе.
Примечания	Состояние этого монитора будет изменено на «Критическое», если вредоносная программа была обнаружена, но не была удалена. Состояние будет автоматически изменено на «Работоспособное» через 8 часов (поскольку невозможно точно определить, была вредоносная программа удалена или нет). Для рассмотрения обстоятельств и закрытия запроса вручную необходимо вмешательство администратора.
Состояние	Работоспособное: нет вредоносных программ Критическое: активная вредоносная программа
Включен	Да
Задача восстановления	Нет

Этот монитор отслеживает неудавшиеся операции очистки вредоносных программ. Он возвращает критическое состояние, если клиент сообщает, что удалить вредоносную программу не удалось.

Возраст определений защиты от вредоносных программ

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Команда для получения данных мониторинга: /opt/microsoft/scep/sbin/scep_daemon --status
Интервал	Каждые восемь часов
Предупреждение	Да. Выполняется автоматическое разрешение.
Состояние	Работоспособное: возраст не более трех дней Предупреждение: возраст более трех и не более пяти дней. Критическое: возраст более пяти дней
Включен	Да
Задача восстановления	Да, вручную (автоматическое восстановление не выполняется).

Актуальные определения помогают обеспечить защиту компьютера от новейших угроз, представляемых вредоносными программами.

Ядро защиты от вредоносных программ

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Отслеживает текстовый файл журнала: /var/log/scep/eventlog_scom.dat
Интервал	При событии
Предупреждение	Да. Выполняется автоматическое разрешение.
Состояние	Работоспособное: включен Предупреждение: отключен
Включен	Да
Задача восстановления	Да, вручную (автоматическое восстановление не выполняется).

Рекомендуется, чтобы защита от вредоносных программ была включена непрерывно.
Примечание. Этот монитор отслеживает состояние защиты от вирусов, которую следует отличать от защиты в режиме реального времени. Когда ядро защиты от вредоносных программ отключено, запустить сканирование по требованию невозможно.

Служба защиты от вредоносных программ

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Отслеживает состояние следующего процесса: scep_daemon
Интервал	Каждые 10 минут
Предупреждение	Да. Выполняется автоматическое разрешение.
Состояние	Работоспособное: работает Критическое: не работает

Включен	Да
Задача восстановления	Да, вручную (автоматическое восстановление не выполняется).

Этот монитор возвращает критическое состояние, если служба защиты от вредоносных программ (scep_daemon) на клиентском компьютере не работает или не отвечает либо ядро защиты от вредоносных программ работает неправильно.

Возраст последнего сканирования

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Команда для получения данных мониторинга: /opt/microsoft/scep/sbin/scep_daemon --status
Интервал	Каждые восемь часов
Предупреждение	Нет
Состояние	Работоспособное: возраст не более семи часов Предупреждение: возраст более семи часов
Включен	Да
Задача восстановления	Да, вручную (автоматическое восстановление не выполняется).

Этот монитор отслеживает время, прошедшее с момента последнего сканирования компьютера (независимо от типа сканирования). Рекомендуется выполнять сканирование еженедельно.

Ожидание перезапуска

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Отслеживает текстовый файл журнала: /var/log/scep/eventlog_scom.dat
Интервал	При событии
Предупреждение	Да. Выполняется автоматическое разрешение.
Состояние	Работоспособное: нет Предупреждение: да
Включен	Да
Задача восстановления	Да, вручную (автоматическое восстановление не выполняется).

Этот монитор отслеживает необходимость перезапуска системы для того, чтобы изменения конфигурации вступили в силу (обычно после включения или отключения защиты в режиме реального времени). Для обновления этого состояния по требованию монитор использует следующую команду: /opt/microsoft/scep/sbin/scep_daemon --status.

Защита в режиме реального времени

Тип монитора	Базовый монитор
Цель	Защищенный сервер Linux
Источник данных	Отслеживает текстовый файл журнала: /var/log/scep/eventlog_scom.dat Для обновления этого состояния по требованию монитор также может использовать следующую команду: /opt/microsoft/scep/sbin/scep_daemon --status.
Интервал	При событии
Предупреждение	Да. Выполняется автоматическое разрешение.
Состояние	Работоспособное: включен Предупреждение: отключен
Включен	Да
Задача восстановления	Да, вручную (автоматическое восстановление не выполняется).

Отслеживает состояние защиты в режиме реального времени. Защита в режиме реального времени предупреждает, когда обнаруживается попытка установки на компьютере вирусов, шпионских программ и другого потенциально нежелательного программного обеспечения.

System Center Endpoint Protection для Linux

Тип монитора	Составной монитор
Цель	Защищенный сервер Linux
Условие	Наихудшее
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Этот монитор возвращает сводный показатель работоспособности (наихудшее состояние) всех базовых мониторов системы

безопасности SCEP 7 защищенного сервера Linux. Если состояние не инициализировано, то отслеживание для данного объекта не началось либо для него не определены мониторы безопасности.

Ядро защиты от вредоносных программ

Тип монитора	Монитор зависимостей
Цель	Ядро защиты от вредоносных программ
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Возвращает состояние базового монитора «защищенный сервер Linux / ядро защиты от вредоносных программ» в списке отслеживаемых компьютеров.

Служба защиты от вредоносных программ

Тип монитора	Монитор зависимостей
Цель	Ядро защиты от вредоносных программ
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Отображает состояние базового монитора «защищенный сервер Linux/служба защиты от вредоносных программ» в списке отслеживаемых компьютеров.

Определения защиты от вредоносных программ

Тип монитора	Монитор зависимостей
Цель	Определения защиты от вредоносных программ
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Отображает состояние монитора «защищенный сервер Linux/возраст определений защиты от вредоносных программ» в списке отслеживаемых компьютеров.

Активная вредоносная программа

Тип монитора	Монитор зависимостей
Цель	Активность защиты от вредоносных программ
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Возвращает состояние монитора «защищенный сервер Linux / активные вредоносные программы» в анализаторе работоспособности для активности защиты от вредоносных программ.

Проверка связи с компьютером

Тип монитора	Базовый монитор
Цель	Активность защиты от вредоносных программ
Интервал	Каждые 60 минут
Предупреждение	Нет
Состояние	Работоспособное: компьютер доступен Критическое: компьютер недоступен
Включен	Нет
Задача восстановления	Нет

Изменяет состояние на критическое при отсутствии ответа от сервера.

Активность вредоносных программ

Тип монитора	Базовый монитор
Цель	Активность защиты от вредоносных программ
Источник данных	Отслеживает текстовый файл журнала: /var/log/scep/eventlog_scom.dat
Интервал	При событии

Предупреждение	Нет
Состояние	Работоспособное: нет вредоносных программ Критическое: обнаружена активность вредоносных программ
Включен	Да
Задача восстановления	Нет

Этот монитор переходит в критическое состояние в течение пяти минут с момента обнаружения вредоносной программы (как очищенной впоследствии, так и не очищенной) и остается в нем в течение следующих 60 минут. Критическое состояние восстанавливается при каждом новом случае обнаружения, при этом отсчет периода предупреждения начинается заново. Иначе говоря, если в системе в течение 60 минут не обнаружено никаких вредоносных программ, монитор возвращается в работоспособное состояние.

Вспышка заражения вредоносными программами на сервере

Тип монитора	Составной монитор
Цель	Активность защиты от вредоносных программ
Условие	Лучшее
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Составные мониторы: активность вредоносных программ, проверка связи с компьютером.
Изменяет состояние на критическое при отсутствии ответа от сервера в течение 60 минут с момента обнаружения вредоносной программы (как очищенной впоследствии, так и не очищенной). Этот монитор также может перейти в критическое состояние при обнаружении вредоносной программы в течение короткого времени с момента восстановления соединения после отсутствия ответа от сервера.

Вспышка заражения вредоносными программами

Тип монитора	Монитор зависимостей
Цель	Наблюдатель за защищенными серверами
Условие	Наихудшее из 95%
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

Возвращает состояние монитора «активность защиты от вредоносных программ / вспышка заражения вредоносными программами на сервере».
Если на более чем 5 % всех компьютеров с системой Linux (как защищенных, так и незащищенных) регистрируется случай обнаружения вредоносной программы за последние 60 минут, монитор изменяет состояние на критическое.

Сведение работоспособности роли компьютера SCEP Linux

Тип монитора	Монитор зависимостей
Цель	Компьютер с системой Linux
Предупреждение	Нет
Включен	Да
Задача восстановления	Нет

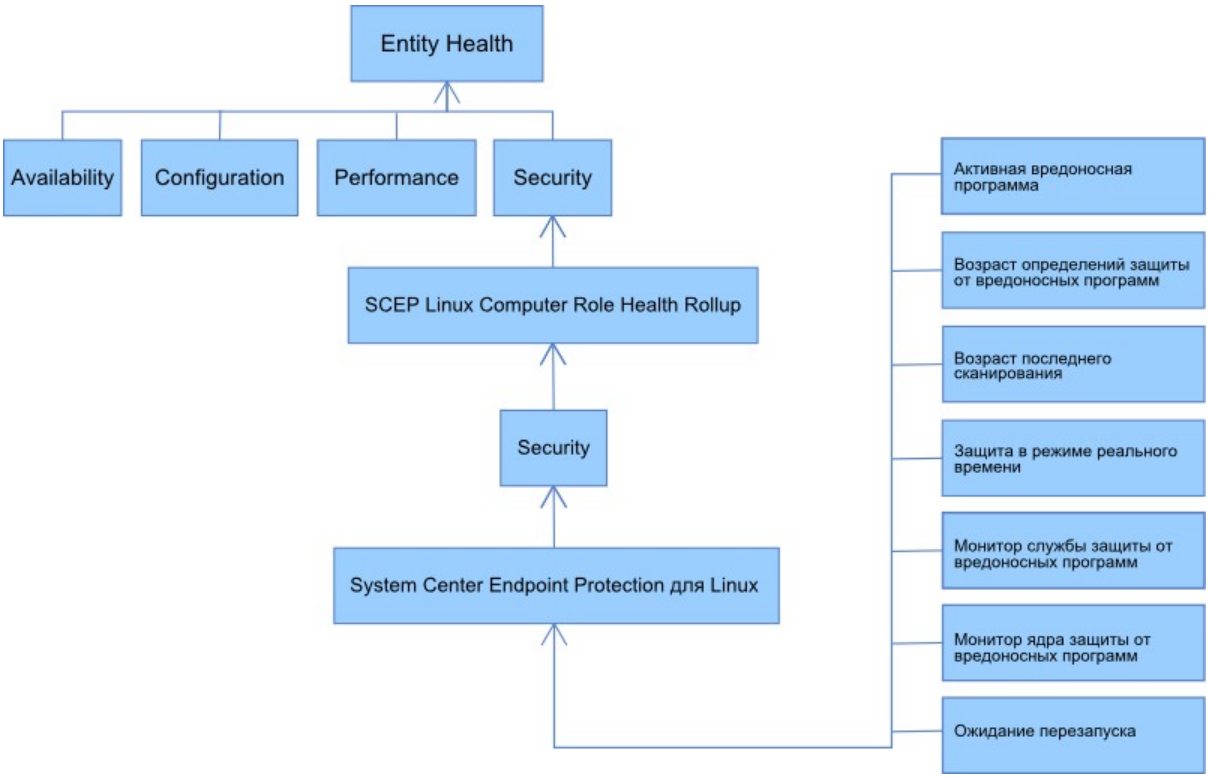
Распространяет состояние объекта защищенного компьютера Linux на родительский монитор безопасности компьютера Linux.

Каскадное изменение состояния работоспособности

Этот пакет управления расширяет комплекс мониторинга операционной системы Linux в виде многоуровневой структуры, в которой работоспособность каждого следующего уровня зависит от предыдущего. Наверху этой структуры располагается вся среда управления работоспособностью объектов, а на нижнем уровне среды контроля безопасности находятся все мониторы. Когда изменяется состояние одного из уровней, состояние уровня над ним также изменяется соответствующим образом. Эта операция называется каскадным изменением состояния работоспособности.

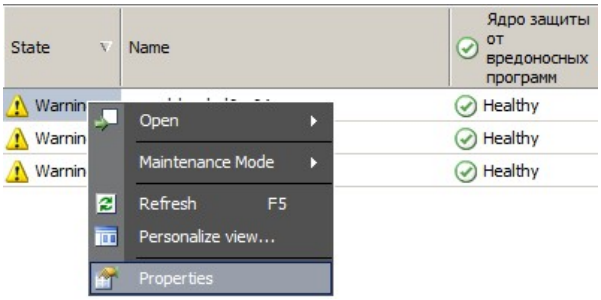
Например, если система защиты в режиме реального времени возвращает состояние «Предупреждение», а все остальные компоненты находятся в работоспособном состоянии, состояние «Предупреждение» передается по древовидной структуре к корню («Работоспособность объектов»), который также переходит в состояние «Предупреждение».

На схеме ниже показано, как каскадно изменяются состояния работоспособности объектов в этом пакете управления.



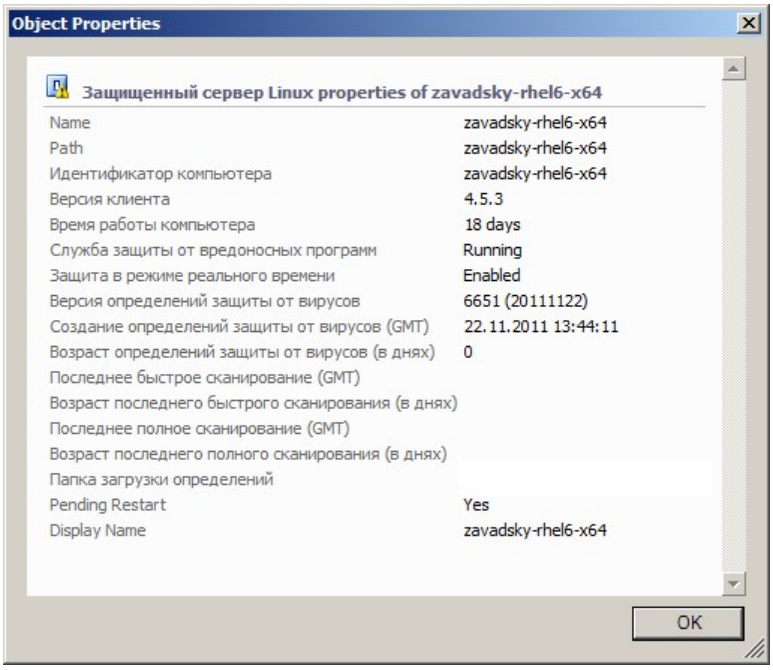
Свойства объекта

Чтобы просмотреть свойства объекта, щелкните его правой кнопкой мыши и выберите в меню пункт **Properties**.



У объекта защищенного сервера Linux есть указанные ниже свойства.

- **Идентификатор компьютера** — идентификатор сервера, доменное имя.
- **Отображаемое имя** — имя сервера, доменное имя.
- **Версия клиента** — версия установленного продукта SCEP.
- **Время работы компьютера** — время непрерывной работы сервера (интервал времени, в течение которого компьютер не отключался) является важнейшим параметром, необходимым для работы пакета управления, и его отсутствие может указывать на ошибку в пакете.
- **Служба защиты от вредоносных программ** — состояние службы защиты от вредоносных программ (работает или не работает).
- **Защита в режиме реального времени** — состояние защиты в режиме реального времени; отсутствие этого параметра указывает на неполадки в работе SCEP.
- **Определения защиты от вирусов...** — сведения о состоянии базы данных сигнатур вирусов (версия, дата создания, давность обновления); отсутствие этого параметра указывает на неполадки в работе SCEP.
- **Последнее быстрое/полное сканирование...** — сведения о последнем сканировании компьютера. Если сканирование (быстрое или полное) еще не выполнялось, это значение не отображается.
- **Папка загрузки определений** — адрес или имя сервера обновлений. Эти сведения появляются после первого успешного обновления.
- **Ожидание перезапуска** — сведения о необходимости перезапуска системы для применения изменений (например, после новой установки или изменения конфигурации SCEP).



Предупреждения

Предупреждение уведомляет о возникновении некоторой ситуации определенной степени опасности (серьезности) с контролируемым объектом. Предупреждения определяются правилами. В одном из режимов просмотра в консоли Operations Manager (**Monitoring** > **System Center Endpoint Protection Linux** > **Активные предупреждения**) отображаются предупреждения при условии, что у пользователя достаточно прав для просмотра определенного объекта.

Примечание. Если один сервер выдал несколько предупреждений одного типа (например, «активная вредоносная программа»), отображается только первое из них.

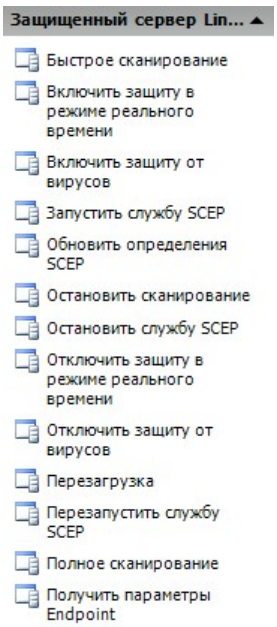
Предупреждение	Интервал	Приоритет	Серьезность	Описание
Повторное заражение вредоносной программой	При событии	Высокий	Критическое	Это предупреждение выдается в случае неоднократного (от 3 раз) обнаружения вредоносной программы в течение определенного интервала времени (30 минут). Оно содержит данные о сервере и основные сведения о вредоносной программе.
Вредоносная программа очищена	При событии	Низкий Средний	Информация: вредоносная программа успешно очищена Предупреждение: необходимо вмешательство пользователя (например, для перезапуска сервера)	Предупреждение о том, что вредоносная программа успешно удалена. Содержит все доступные данные об этой программе. Для каждой вредоносной программы создается собственное событие. SCEP Linux назначает приоритет и серьезность по указанным ниже правилам, исходя из успешности процесса очистки. Очищено: низкий приоритет, информация. Очищено, но требуется вмешательство (например, для перезапуска): средний приоритет, предупреждение.
Активная вредоносная программа (из монитора)	При событии	Высокий	Критическое	Предупреждение о том, что вредоносная программа не удалена. Содержит все доступные данные об этой программе.
Активная вредоносная программа (из правила)	При событии	Высокий/ Средний/ Низкий	Критическое/Средний/ Низкий: на основе типа вредоносной программы	См. выше. Используется для средств подключения к другим системам мониторинга или отправки запросов. **Примечание.** Это правило (предупреждение) по умолчанию отключено.

Служба защиты от вредоносных программ System Center Endpoint Protection не работает	300 секунд	Средний	Критическое	Предупреждение о том, что служба защиты от вредоносных программ SCEP (scep_daemon) недоступна. Содержит имя соответствующего сервера и версию SCEP.
Защита от вредоносных программ отключена	При событии	Средний	Предупреждение	Предупреждение о том, что служба защиты от вредоносных программ отключена. Содержит имя соответствующего сервера.
Защита в режиме реального времени отключена	При событии	Средний	Предупреждение	Предупреждение о том, что защита в режиме реального времени отключена. Содержит имя соответствующего сервера.
Определения устарели	Каждые восемь часов	Средний	Предупреждение (возраст более трех И не более пяти дней) Критическое (возраст более пяти дней)	Предупреждение о том, что база данных сигнатур вирусов не обновлялась в течение трех дней или более. Содержит имя соответствующего сервера и сведения о давности обновления базы данных.
Вспышка заражения вредоносными программами	При событии	Высокий	Критическое	Система Forefront Endpoint Protection обнаружила активные вредоносные программы более чем на 5 % компьютеров. Возможно, в компьютерной сети распространяется вредоносное программное обеспечение. Рекомендуется обновить определения вирусов на всех серверах. Чтобы изменить количество активных угроз, при котором выдается это предупреждение, переопределите параметр монитора вспышки заражения вредоносными программами (см. раздел Переопределения).

Задачи

В пакете управления для SCEP реализовано 13 задач. Они запускаются на выполнение мгновенно. Сразу же после их завершения выдаются результаты, которые также можно просмотреть позднее в окне состояния задач. Максимальное время выполнения задачи составляет 180 секунд. Переопределить этот параметр нельзя. Все задачи представляют собой команды оболочки BASH, выполняемые через SSH.

Задачи можно вызвать из раздела **Monitoring** > **System Center Endpoint Protection Linux** > **Сервера с SCEP** на правой панели окна консоли управления.



- **Отключить защиту от вирусов** — отключение всех компонентов системы антивирусной защиты и сканирования по требованию.
- **Включить защиту от вирусов** — включение всех компонентов системы антивирусной защиты.
- **Отключить защиту в режиме реального времени** — отключение защиты в режиме реального времени.
- **Включить защиту в режиме реального времени** — включение защиты в режиме реального времени.
- **Полное сканирование** — обновление базы данных сигнатур вирусов и запуск полного сканирования компьютера.
- **Быстрое сканирование** — обновление базы данных сигнатур вирусов и запуск быстрого сканирования компьютера.
- **Остановить сканирование** — остановка всех процессов сканирования компьютера.
- **Получить параметры сервера** — вывод на экран текущего состояния продукта SCEP (выводимые параметры соответствуют свойствам объекта защищенного сервера Linux). Отображаемые данные не передаются на защищенный сервер Linux.
- **Перезапустить службу защиты от вредоносных программ** — перезапуск службы защиты от вредоносных программ SCEP (scep_daemon).
- **Остановить службу защиты от вредоносных программ** — остановка службы защиты от вредоносных программ SCEP (scep_daemon).
- **Запустить службу защиты от вредоносных программ** — запуск службы защиты от вредоносных программ SCEP (scep_daemon).
- **Обновить определения защиты от вредоносных программ** — запуск обновления базы данных сигнатур вирусов.
- **Перезагрузка** — перезагрузка компьютера с системой Linux.

Настройка пакета управления для SCEP

Рекомендации: создание пакета управления для сохранения изменений

Стандартно Operations Manager сохраняет все изменения, например переопределения, в пакете управления по умолчанию. Рекомендуется вместо этого создавать отдельный пакет управления для каждого исходного пакета, в который нужно внести изменения.

При создании пакета управления, в котором будут храниться измененные настройки, рекомендуется назначить ему имя, основанное на имени модифицируемого пакета (например, «SCEP 2012 — изменения»).

Наличие отдельного пакета управления с изменениями, внесенными в исходную версию пакета, упрощает экспорт новой конфигурации из тестовой среды в рабочую. Кроме того, такой пакет управления проще удалить, поскольку перед этим необходимо удалить все зависимости пакета. Если изменения, вносимые во все пакеты, хранятся в пакете управления по умолчанию, то в ситуации, когда необходимо удалить только один пакет, приходится удалять пакет управления по умолчанию, в результате чего пропадают изменения, которые были внесены в другие пакеты.

Настройка конфигурации безопасности

На компьютере должна быть запущена служба SSHD и открыт порт SSH (по умолчанию порт 22). System Center 2012 Operations Manager подключается через этот порт к удаленным компьютерам Linux, используя соответствующую команду Run As Account (панель **Administration** > **Run As Configuration** в консоли мониторинга Operations Manager) и тип **Basic Authentication**.

Имя профиля запуска от имени	Примечания
Unix Privileged Account	Используется для удаленного наблюдения за сервером Unix, а также для перезапуска процессов, требующих расширенных прав.

Этот пакет управления не использует Unix Action Account.

Предупреждение. Наблюдение за компьютерами с использованием учетной записи root может оказаться фактором риска для безопасности (например, в случае взлома пароля).

Если вы не хотите наблюдать за компьютерами и управлять ими с помощью учетной записи root, то можете воспользоваться стандартной учетной записью пользователя, обладающей необходимыми правами для выполнения команд *sudo*. Таким образом, на всех наблюдаемых рабочих станциях Linux, где используется протокол SCEP, в файле /etc/sudoers должна быть настроена представленная ниже конфигурация, которая позволяет выбранной учетной записи выполнять команды sudo. Вот пример конфигурации для пользователя user1.

```
#--------------------------------------------------------------------------------
# User configuration for SCEP monitoring - for a user with the name: user1

user1  ALL=(root)    NOPASSWD:     /opt/microsoft/scx/bin/scxlogfilereader -p
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /sbin/reboot
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep restart
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep start
user1  ALL=(root)    NOPASSWD:     /bin/sh -c CONSOLETYPE=serial /etc/init.d/scep stop
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C;if \[ -e /opt/microsoft/scep/sbin/
scep_daemon \] ; then echo scep_daemon installed; else echo scep_daemon unprotected; fi; kill -0
`cat /var/run/scep_daemon.pid 2>/dev/null` 2>/dev/null; if \[ $\? -eq 0 \] ; then echo scep_daemon
running; else echo scep_daemon stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime
```

```
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/sbin/scep_daemon *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c /opt/microsoft/scep/lib/scep_sci --scom *
user1  ALL=(root)    NOPASSWD:     /bin/sh -c pkill scep_sci
user1  ALL=(root)    NOPASSWD:     /bin/sh -c export LANG=C; kill -0 `cat /var/run/scep_daemon.pid 2>/
dev/null` 2>/dev/null; if \[ $? -eq 0 \] ; then echo scep_daemon running; else echo scep_daemon
stop;fi ; /opt/microsoft/scep/sbin/scep_daemon --status; uptime

# End user configuration for SCEP monitoring
#--------------------------------------------------------------------------------
```

Настройка правил предельных значений производительности

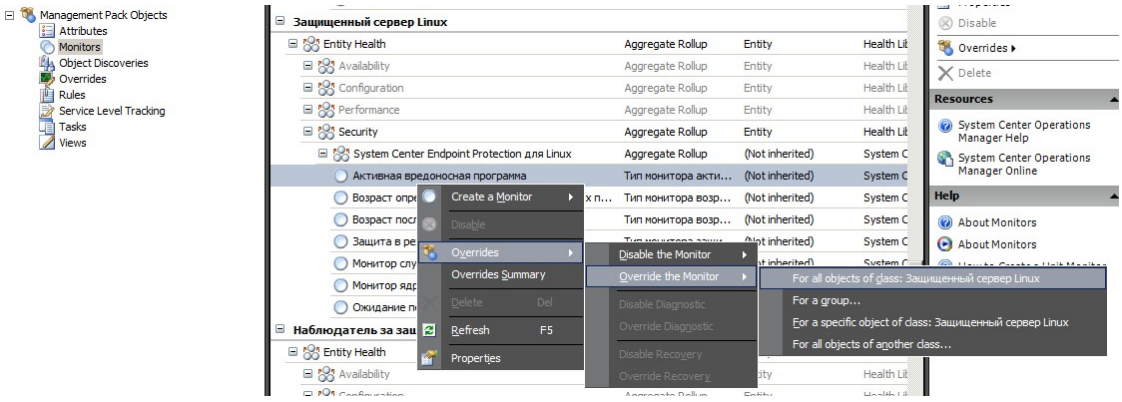
В приведенной ниже таблице указаны правила предельных значений производительности по умолчанию, которые можно настроить в соответствии с требованиями конкретной среды. Проанализируйте их на предмет соответствия пороговых значений имеющейся среде. Изменить их можно с помощью переопределений.

Имя правила	Переопределяемый параметр	Пороговое значение по умолчанию	Ограничения возможностей настройки
Правило повторного заражения вредоносной программой	Пороговое значение количества повторных заражений	3 случая	Установка значения меньше 2 делает это правило бессмысленным.
Правило повторного заражения вредоносной программой	Интервал времени повторного заражения	30 минут	Не рекомендуется устанавливать для этого параметра значение меньше продолжительности сканирования по требованию, поскольку наложение может воспрепятствовать генерированию предупреждения.
Правило предупреждения об активной вредоносной программе	Включено	Нет	Это предупреждение можно включить при использовании средств подключения к другим системам мониторинга или отправки запросов.

Переопределение параметров

С помощью функции переопределения параметров можно скорректировать настройки отслеживаемого объекта в System Center 2012 Operations Manager. Это относится к мониторам, правилам, операциям обнаружения объектов и атрибутам из импортированных пакетов управления.

Чтобы переопределить монитор, в консоли управления нажмите кнопку **Authoring** и разверните узел **Management Pack Objects** > **Monitors**. На панели мониторов найдите и полностью разверните тип объекта, а затем щелкните монитор и выберите пункт **Overrides**.



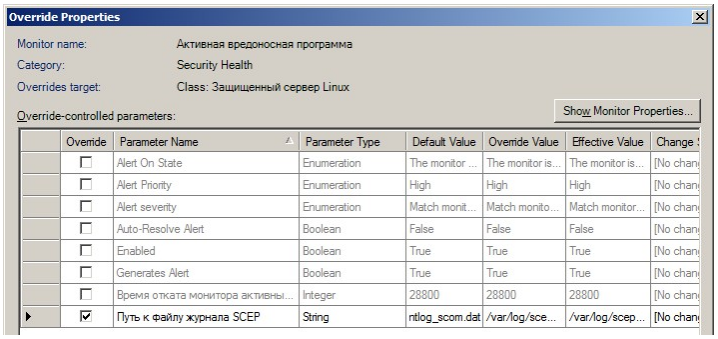
В окне переопределений создайте или измените переопределение любого из указанных ниже параметров.

- **Время отката монитора активных вредоносных программ** (только для монитора активных вредоносных программ)
- **Возраст определений защиты от вредоносных программ** (только для монитора возраста определений защиты от вредоносных программ)
- **Интервал обнаружения** (только для монитора возраста последнего сканирования)
- **Предупреждение о состоянии**
- **Приоритет предупреждения**
- **Серьезность предупреждения**
- **Автоматически разрешить предупреждение**
- **Включено** — определяет, включен ли выбранный монитор.
- **Создает предупреждения**
- **Путь к файлу журнала SCEP**

Если значение переопределения по умолчанию не подходит для вашей среды, можно изменить пороговые значения, применив переопределение к ним.

Переопределяемый параметр	Имя монитора	Значение по умолчанию	Заметки по изменению
Интервал проверки связи	Проверка связи с компьютером	3600 секунд	Интервал проверки доступности защищенного сервера Linux. Чем он меньше, тем быстрее монитор вспышки заражения вредоносными программами на сервере переходит в состояние ошибки, если компьютер перестает отвечать на запросы из-за атаки на него. Соответственно, в этом случае возрастает нагрузка на сеть, отслеживаемый компьютер и сервер System Center 2012 Operations Manager.
Интервал времени вспышки заражения вредоносными программами	Активность вредоносных программ	3600 секунд	Интервал времени, по истечении которого монитор возвращается в работоспособное состояние после обнаружения активности вредоносных программ. Значение монитора интервала должно быть больше, чем значение интервала проверки связи с компьютером. Если в течение интервала времени вспышки заражения вредоносными программами активность таких программ регистрируется на компьютерах, число которых превышает установленную процентную долю (см. монитор вспышки заражения вредоносными программами), выдается предупреждение о вспышке. Примечание. Этот параметр отличается от монитора вспышки заражения вредоносными программами на сервере, который не выдает предупреждение.
Время отката монитора активных вредоносных программ	Активная вредоносная программа	28800 секунд	Интервал времени с момента обнаружения вредоносной программы, по истечении которого она считается очищенной.
Путь к файлу журнала SCEP	Активная вредоносная программа	/var/log/scep/ eventlog_scom.log	Путь к файлу, в котором регистрируются события System Center 2012 Operations Manager. Изменяйте этот параметр лишь в случае возникновения каких-либо проблем.
Критический возраст определений защиты от вредоносных программ	Возраст определений защиты от вредоносных программ	5 дней	По истечении этого интервала создается предупреждение об ошибке, связанной с устареванием продукта SCEP.
Работоспособный возраст определений защиты от вредоносных программ	Возраст определений защиты от вредоносных программ	3 дня	Максимально допустимый возраст определений защиты от вредоносных программ, до достижения которого они считаются актуальными. Это значение всегда должно быть меньше, чем критический возраст определений защиты от вредоносных программ.
Интервал	Возраст определений защиты от вредоносных программ	28800 секунд	Интервал проверки возраста определений защиты от вредоносных программ.
Интервал	Служба защиты от вредоносных программ	300 секунд	Интервал проверки доступности службы защиты от вредоносных программ.
Имя процесса	Служба защиты от вредоносных программ	scep_daemon	Имя службы защиты от вредоносных программ. Не изменяйте этот параметр, если монитор работоспособен.
Интервал обнаружения	Возраст последнего сканирования	28800 секунд	Интервал проверки выполнения последнего сканирования.
Максимальный возраст сканирования	Возраст последнего сканирования	7 дней	Устанавливается в соответствии с параметрами продукта SCEP. Если плановое сканирование выполняется каждые семь дней, этому параметру следует присвоить то же значение.

Путь к файлу журнала	Ожидание перезапуска	/var/log/scep/eventlog_scom.log	Путь к файлу, в котором регистрируются события System Center 2012 Operations Manager. Изменяйте этот параметр лишь в случае возникновения каких-либо проблем.
Путь к файлу журнала SCEP	Защита в режиме реального времени	/var/log/scep/eventlog_scom.log	Путь к файлу, в котором регистрируются события System Center 2012 Operations Manager. Изменяйте этот параметр лишь в случае возникновения каких-либо проблем.
Доля	Вспышка заражения вредоносными программами	95%	Процентная доля защищенных и незащищенных серверов Linux, которые должны перейти в работоспособное состояние, чтобы вся отслеживаемая группа считалась работоспособной. Если вредоносные программы регистрируются на пяти или более процентах от общего числа серверов, создается предупреждение о вспышке заражения.



Примечание. Дополнительные сведения о переопределениях см. в статье Наблюдение с помощью переопределений (http://go.microsoft.com/fwlink/?LinkID=117777).

Ссылки

Ниже приведены ссылки на веб-страницы с описанием стандартных задач, выполняемых с помощью этого пакета управления.

- Администрирование жизненного цикла пакета управления (http://go.microsoft.com/fwlink/?LinkId=211463)
- Импорт пакета управления в Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=142351)
- Наблюдение с помощью переопределений (http://go.microsoft.com/fwlink/?LinkID=117777)
- Создание учетной записи запуска от имени в Operations Manager 2007 (http://go.microsoft.com/fwlink/?LinkID=165410)
- Настройка кроссплатформенной учетной записи запуска от имени (http://go.microsoft.com/fwlink/?LinkId=160348)
- Изменение профиля запуска от имени (http://go.microsoft.com/fwlink/?LinkID=165412)
- Экспорт конфигурации пакета управления (http://go.microsoft.com/fwlink/?LinkId=209940)
- Удаление пакета управления (http://go.microsoft.com/fwlink/?LinkId=209941)
- Управление данными наблюдения с помощью кнопок «Область», «Поиск» и «Найти» (http://go.microsoft.com/fwlink/?LinkId=91983)
- Мониторинг системы Linux с помощью SCOM 2007 R2 (http://blogs.technet.com/b/birojitn/archive/2010/01/20/monitoring-linux-using-scom-2007-r2.aspx)
- Установка кроссплатформенных агентов вручную (http://technet.microsoft.com/ru-ru/library/dd789016.aspx)
- Настройка прав sudo для систем UNIX и Linux, наблюдаемых с помощью System Center 2012 — Operations Manager (http://social.technet.microsoft.com/wiki/contents/articles/7375.configuring-sudo-elevation-for-unix-and-linux-monitoring-with-system-center-2012-operations-manager.aspx)

Ответы на вопросы о среде Operations Manager и пакетах мониторинга см. на форуме сообщества System Center Operations Manager (http://go.microsoft.com/fwlink/?LinkID=179635).
В блоге System Center Operations Manager Unleashed (http://opsmgrunleashed.wordpress.com/) доступны полезные примеры использования конкретных пакетов мониторинга.

Дополнительные сведения о Operations Manager см. в перечисленных ниже блогах.

- Блог группы разработчиков Operations Manager
  (http://blogs.technet.com/momteam/default.aspx)
- Блог OpsMgr Кевина Холмана
  (http://blogs.technet.com/kevinholman/default.aspx)
- Мысли об OpsMgr
  (http://thoughtsonopsmgr.blogspot.com/)
- Блог Рафаэля Берри
  (http://rburri.wordpress.com/)
- Пространство управления Брайана Рена
  (http://blogs.technet.com/brianwren/default.aspx)
- Блог группы поддержки System Center Operations Manager
  (http://blogs.technet.com/operationsmgr/)
- Ops Mgr ++
  (http://blogs.msdn.com/boris_yanushpolsky/default.aspx)
- Замечания о System Center Operations Manager
  (http://blogs.msdn.com/mariussutara/default.aspx)

Сведения о поиске и устранении неполадок см. в указанных ниже разделах форума.

- Отсутствует библиотека Microsoft.Unix.Library
  (http://social.technet.microsoft.com/Forums/en-US/operationsmanagermgmtpacks/thread/8469d0ff-54d6-4cb4-9909-49ab62126b74/)