Политика KES для Windows Server

Общие

Состояние политики - **Активная политика**

Наследование параметров

- Наследовать параметры родительской политики - **выключить**
- Обеспечить принудительное наследование параметров для дочерних политик - **выключить**

Настройка событий

- Регистрация событий
  - Хранить в базе данных Сервера администрирования в течении (сут) - до 30
  - **Экспортировать в SIEM-систему по протоколу Syslog**
- События, которые стоит отправлять в SIEM

Тип события	Время хранения на KSC	Отправка в SIEM
:drop_of_blood: Критические события		Да :tick: / Нет :cross:
Обнаружен зараженный объект или объект другого типа	30 дней	
Обнаружен объект, недоверенный в KSN	30 дней	
Обнаружен возможно зараженный объект	30 дней	
Обнаружена попытка шифрования	30 дней	

Объект не вылечен	30 дней	
Объект не удален	30 дней	
Объект не обработан	30 дней	
Ошибка установки объекта на удаление при перезагрузке	30 дней	
Базы программы сильно устарели	30 дней	
Срок действия лицензии истек	30 дней	
Превышен максимальный размер резервного хранилища	30 дней	
Превышен максимальный размер карантина	30 дней	
Не применено обновление модулей	30 дней	
Не удалось отозвать обновление модулей программы	30 дней	
Не удалось выполнить откат последнего обновления баз программы	30 дней	
Задача не запущена под указанной учетной записью	30 дней	
Заблокировано соединение / Обнаружена почтовая угроза	30 дней	
Ошибка подключения интерфейса управления к службам защиты	30 дней	
Ошибка создания обработчика запросов на проверку объектов от сетевых хранилищ	30 дней	
Ошибка регистрации устройства с Kaspersky Security 11.0.1 для Windows Server в качестве сервера антивирусной защиты для сетевого хранилища	30 дней	
Превышено максимальное количество попыток восстановления соединения с сетевым хранилищем	30 дней	
Сетевое хранилище разорвало связь с программой	30 дней	
Ошибка соединения с сетевым хранилищем	30 дней	
Запуск программы запрещен	30 дней	
Обнаружено и запрещено недоверенное устройство	30 дней	
Сетевой экран заблокировал соединение	30 дней	

Сработало правило анализа журналов	30 дней	
Обнаружена возможная попытка взлома пароля	30 дней	
Обнаружены признаки компрометации журналов Windows	30 дней	
В системе установлена новая служба	30 дней	
Обнаружена подозрительная аутентификация с явным указанием учетных данных	30 дней	
Обнаружены признаки атаки Kerberos forged PAC (MS14-068)	30 дней	
Ищменена политика брандмауэра Windows	30 дней	
Обнаружены подозрительные изменения привелигерованной группы Администраторы	30 дней	
Обнаружена подозрительная активность во время сетевого сеанса входа	30 дней	
Запрещенная файловая операция в контролируемой области	30 дней	
Обнаружена и заблокирована попытка компрометации журнала USN	30 дней	
Файловая система на указанном томе не поддерживается	30 дней	
Ошибка модификации хранилища эталонов задачи Мониторинг целостности файлов	30 дней	
Несовпадение хеша файлов с эталоном	30 дней	
Файл, присутствующий в эталоне, удален	30 дней	
Процесс терминирован: обнаружена попытка эксплуатации уязвимости	30 дней	
Выполняется уязвимый процесс: обнаружен факт эксплуатации уязвимости	30 дней	
:cross: Отказ функционирования		Да :tick: / Нет :cross:
Внутренняя ошибка	30 дней	
Не обновлено	30 дней	

Нарушено Лицензионное соглашение	30 дней	
Нарушено Лицензионное соглашение для задачи	30 дней	
Базы программы повреждены	30 дней	
Невозможно запустить задачу, область защиты пуста	30 дней	
Ошибка сброса статуса устройства с Kaspersky Security 11.0.1 для Windows Server	30 дней	
Запуск программы не обработан	Не хранить	
Правило для файла не сформировано	30 дней	
Не создан XML файл по сформированным правилам	30 дней	
Не удалось отправить запрос в KSN	Не хранить	
Целостность модулей программы нарушена	30 дней	
Подключение устройства не обработано	30 дней	
Мониторинг отключен для тома	30 дней	
Ошибка соединения с сервером Syslog	30 дней	
Ошибка отсылки события на сервер Syslog	30 дней	
:warning: Предупреждение		Да :tick: / Нет :cross:
Объект не проверен	Не хранить	
Объект не помещен на карантин	30 дней	
Объект не помещен в резервное хранилище	30 дней	
Обнаружен объект	30 дней	
Объект будет удален при перезагрузке	30 дней	
Обнаружен возможно зараженный объект	30 дней	
Проверка важных областей защищаемого устройства давно не выполнялась	30 дней	
Базы программы устарели	30 дней	
Срок действия лицензии скоро истечет	30 дней	

Доступно плановое обновление модулей	30 дней	
Доступно критическое обновление модулей программы	30 дней	
Обновление модулей программы должно быть отозвано	30 дней	
Для завершения обновления требуется перезагрузить защищаемое устройство	30 дней	
Превышен порог доступного пространства в резервном хранилище	30 дней	
Превышен порог доступного пространства карантина	30 дней	
Присоединенное сетевое хранилище дало команду завершить работу сервера антивирусной защиты	30 дней	
Все присоединенные сетевые хранилища завершили работу, задача защиты сетевых хранилищ по протоколу RPC будет остановлена	30 дней	
Только статистика: запуск программы запрещен	30 дней	
Формирование правила по файлу не поддерживается	30 дней	
Компьютер добавлен в список недоверенных	30 дней	
Компьютер не добавлен в список недоверенных	30 дней	
Ошибка регистрации в качестве FPolicy-сервера	30 дней	
Только статистика: обнаружено недоверенное устройство	30 дней	
Не запущена задача проверки по требованию для подключенного устройства	30 дней	
Программа остановлена	30 дней	
Не установлено соединение с KSN	30 дней	
Подозрительная файловая операция в контролируемой области	30 дней	
Появился файл, отсутствующий в эталоне	30 дней	
Отсутствует соединение с клиентом Outlook	Не хранить	

:information: Информационное сообщение		Да :tick: / Нет :cross:
Объект вылечен	30 дней	
Объект удален	30 дней	
Объект помещен на карантин	30 дней	
Объект заблокирован (Процесс терминирован)	30 дней	
Объект обнаружен (выполняется уязвимый процесс)	30 дней	
Объект помещен в резервное хранилище	30 дней	
Уровень безопасности постоянной защиты изменен	30 дней	
Проверка важных областей защищаемого устройства успешно завершена	30 дней	
Программа запущена	Не хранить	
Объект не проверен	Не хранить	
Доступ к объекту разрешен	Не хранить	
Доступ к объекту заблокирован	30 дней	
Соединение разрешено / Письмо разрешено к загрузке	Не хранить	
Инициирована сессия управления службами защиты через интерфейс	Не хранить	
Установлено соединение с сетевым хранилищем	30 дней	
Только статистика: обнаружено доверенное устройство	Не хранить	
Только статистика: запоминающее устройство извлечено	Не хранить	
Сетевой экран разрешил соединение	Не хранить	
Программа будет разрешена к запуску как часть доверенного пакета установки	Не хранить	
Обнаружено устройство	30 дней	
Обнаружено устройство, подключенное к защищаемому устройству	30 дней	
Разрешена файловая операция в контролируемой области	Не хранить	

Хранилище эталонов задачи Мониторинг целостности файлов создано	30 дней	
Отправлен запрос в KSN	Не хранить	
Установлено соединение с KSN	Не хранить	
Сформирован пакет статистики KSN	Не хранить	
Компьютер исключен из списка недоверенных	Не хранить	
Выполнена регистрация в качестве FPolicy-сервера	Не хранить	

Параметры программы

- **Масштабируемость, интерфейс и настройки сканирования**
  - Общие
    - Определять параметры масштибмруемости ватоматически - **включить**
    - Показывать значет в области уведомлений - **включить**
  - Сканирование
    - Восстанавливать атрибуты файлов после сканирования - **включить**
    - Ограничить сканирующий поток в использовании CPU **80%** - **включить**
  - Иерархическое хранилище
    - Не HSM-система - **включить**
- **Безопасность и надежность**
  - Самозащита - Защищать процессы программы от внешних угроз - **включить**
  - Параметры применения пароля - Использовать защиту паролем - **включить**
  - Параметры надежности - выполнять восстановление задач проверки по требованию не более (раз) **2** - **включить**
  - Действия при переходе на ИБП - **выключить все**
- **Параметры соединения**
  - Не использовать прокси-сервер - **включить**
  - Не использовать прокси-сервер для локальных адресов - **включить**
  - Не использовать аутентификацию

    - Использовать KSC в качестве прокси-сервера для активации программы - **включить**

- **Запуск локальных системных задач**
    - Задачи проверки по требованию - **включить**
    - Задачи обновления и копирования обновлений - **выключить**

Дополнительные возможности

- **Доверенная зона**
    - Исключения - **по умолчанию**

        Возможно имеет смысл убрать исключения для продуктов которые мы не используем, вроде MS Lync или MCMS

    - Доверенные процессы
        - Не проверять файловые операции резервного копирования - **включить**
        - Не проверять файловую активность указанных процессов - **выключить**

- **Проверка съемных дисков**
    - Проверять съемные диски при подключении к USB
    - Проверять если объем содержащихся на диске данных не превышает порог - **32768 МБ**
    - Запускать проверку с уровнем безопасности - **Рекомендуемый**

- **Права пользователей на управление программой**
- **Права пользователей на управление службой Kaspersky Security Service**
- **Хранилища**
    - Резервное хранилище - **по умолчанию**
    - Карантин - **по умолчанию**
    - Заблокированные узлы
        - Автоматически разблокировать через - **2 ч**

Постоянная защита сервера

Постоянная защита файлов

- Общие
  - Режим защиты объектов - **При открытии и изменении**
  - Углубленный анализ запускаемых процессов (запуск процессов блокируется до окончания анализа) - **включить**
  - Использовать эвристический анализ - **включить (Средний)**
  - Интеграция - Применять доверенную зону - **включить**
  - Интеграция - Использовать KSN для защиты - **включить**
  - Интеграция - Блокировать доступ к сетевым файловым ресурсам для узлов, с которых ведется вредоносная активность - **включить**
  - Запустить сканирование важных областей при обнаружении активного заражения - **включить**
  - Отарпалять объекты в Kaspersky Sandbox - **выключить**

- Области защиты
  - **Мой компьютер** - уровень **Рекомендуемый**

- Управление задачей
  - Запускать задачу по расписанию - **включить**
  - Частота запуска - **При запуске программы**

Использование KSN

- Обработка данных - Службы - Принять условия положения Kaspersky Security Network - **включить**
- Обработка данных - Статистика - Разрешить отправку статистики Kaspersky Security Network - **включить**
- Обработка данных - Kaspersky Managerd Protection - Принять условия Предложения о KMP - **выключить**

- Настройка
  - Общее
    - Действия над объектом, недоверенным KSN - **удалять**
    - Не рассчитывать контрольную сумму для отправки в KSN, если размер файла превышает **10 Мб** - **включить**
    - Использовать Kaspersky KSC в качестве прокси-сервера KSN - **включить**
  - Управление задачей
    - Запускать задачу по расписанию - **При запуске программы**

Защита трафика

-

- Список правил
  - Веб-контроль - по умолчанию
  - Категоризация
    - Применять правила категоризации ресурсов - **включить**
    - Разрешать загрузку веб-страниц, если не удалось присвоить категорию - **включить**
    - Разрешать загрузку легальных веб-ресурсов, которые могут быть использованы для нанесения вреда защищаемому устройству - **включить**
    - Разрешать загрузку легальных рекламных веб-ресурсов - **включить**

- Настройка
  - Режим работы
    - Режим работы - Драйверный перехват
    - Параметры соединения с ICAP-службой - **по умолчанию**
    - Параметры режима работы
      - Проверять безопасное соединение по протоколу HTTPS - **включить**
      - Использовать версию крипто-протокола TLS: 1.0, 1.1, 1.2 - **включить**

        - Не доверять веб-сервису с невалидным сертификатом - **включить** (если много внутренних сервисов с самоподписанным сертификатом, то лучше выключить)
        - Настроить области перехвата - **индивидуальная настройка для групп серверов.**

- Обработка веб-ресурсов
    - Проверять ссылки по базе вредоносных веб-ресурсов - **включить**
    - Проверять ссылки по базе фишинговых веб-адресов - **включить**
    - Использовать KSN для защиты - **включить**
    - Использовать Доверенную зону - **включить**

- Управление задачей
    - Запускать задачу по расписанию - **При запуске программы**

- Защита от почтовых угроз
    - Защита устройства от почтовых угроз - **выключить**

- Антивирусная защита
    - Использовать эвристический анализ - **включить** (Средний)
    - Уровень безопасности - **Рекомендуемый**

Защита от эксплойтов

- Параметры защиты от эксплойтов
    - Защищать процессы от эксплуатации уязвимостей в режиме - **включить**
        - Завершать скомпрометированный процессы

    - Сообщать о скомпрометированных процессах посредством службы терминалов - **включить**
    - Защищать процессы от эксплуатации уязвимостей вне зависимости от статуса службы KSS - **включить**

- Защищаемые процессы - **по умолчанию**

Защита от сетевых угроз

- Общие
  - Блокировать соединение при обнаружении атаки - **включить**
  - Не останавливать анализ трафика, если задача не исполняется - **выключить**

- Исключения
  - Не контролировать IP-адреса, указанные в исключениях - **выключить** (Можно добавить серверную подсеть)

- Управление задачей
  - Запускать задачу по расписанию - **включить**
    - Частота запуска: **При запуске программы**

Проверка скриптов

- Общее
  - Действие над опасными скриптами: **Блокировать выполнение**
  - Эвристический анализ - **включить** (Средний)
  - Применять доверенную зону - **включить**

- Управление задачей
  - Запускать задачу по расписанию - **выключить**

Контроль активности на серверах

Контроль запуска программ

- Режим работы - **Только статистика**
    - Обрабатывать повторные запуски контролируемых программ по схеме обработки первого запуска - **включить**

- Запрещать запуск командных интерпретаторов без команды к исполнению - **выключить**
- Список правил - **по умолчанию** (Можно согласовать с админами запуск скриптов только из доверенной папки, например C:\Scripts, у которой будут права доступа только для администраторов сервера
    - Применение правил - **Заменить правилами политики локальные правила**

- Область применения правио
    - Использовать правила для исполняемых файлов - **включить**
    - Контролировать загрузку DLL-модулей - **выключить**
    - Использовать правила для скриптов и пакетов MSI - **включить**

- Использование KSN
    - Запрещать запуск программ, недоверенных в KSN - **включить**
    - Разрешать запуск программ, доверенных в KSN - **выключить**

- Контроль пакетов установки
    - **По умолчанию**

- Управление задачей
    - Запускать задачу по расписанию - **выключить**
    - Частота запуска - **При запуске программы**

Контроль устройств

- Режим работы - **только статистика**
- Разрешать использование всех запоминающих устройств, если задача Контроль устройств не выполняется - **выключено**
- Управление задачей
    - Запускать задачу по расписанию - **выключить**
    - Частота запуска - **При запуске программы**

Защита сетевых хранилищ

Защита RPC-подключаемых сетевых хранилищ

- **Не актуально, выключить**

Защита ICAP-подключаемых сетевых хранилищ

- **Не актуально, выключить**

Защита от шифрования для NetApp

- **Не актуально, выключить**

Контроль активности в сети

Управление сетевым экраном

- Слишком индивидуальная задача, возможно стоит разделять политику на группы серверов (Файловые шары, AD и т.д)

Защита от шифрования

- Общие
  - Режим работы - **Активный**
  - Эвристический анализатор - **включить** (Средний)
- Область защиты
  - **Все общие сетевые папки защищаемого устройства**
- Исключения
  - Учитывать список исключений - **включить**
- Управление задачей
  - Запускать задачу по расписанию - **включить**
  - Частота запуска - **При запуске программы**

Диагностика системы

Мониторинг файловых операций

- Параметры мониторинга файловых операций
  - Фиксировать события о файловых операциях, выполненных в период обрыва мониторинга - **включить**
  - Блокировать попытки компрометации журналов USN - **включить**

- Управление задачей
  - Запускать задачу по расписанию - **включить**
  - Частота запуска - **При запуске программы**

Анализ журналов

- Пользовательские правила
  - Обнаружено всплывающее окно приложения 26
  - В системе установлена служба 7045
  - Создана задача, выполняемая по расписанию 4696, 602
  - Создание новой учетной записи 4720
  - Добавление пользователя в привилегированную группу 4728
  - Добавление в локальную группу 4732
  - Изменение имени учетной записи 4781
  - Очищен журнал событий 1102

- Предзаданные правила
  - Использовать предзаданные правила для анализа журналов - **включить**
    - Обнаружена возможная попытка взлома пароля с помощью подбора - **включить**
    - Обнаружены признаки компрометации журналов Windows - **включить**
    - Обнаружена подозрительная активность со стороны новой установленной службы - **включить**
    - Обнаружена подозрительная аутентификация с явным указанием учетных данных - **включить**
    - Обнаружены признаки атаки Kerberos forged PAC (MS14-068) - **включить**

    - Обнаружены подозрительные изменения привелигерованной группы Администраторы - **включить**
    - Обнаружена подозрительная активность во время сетевого сеанса входа - **включить**

- Управление задачей
    - Запускать задачу по расписанию - **включить**
    - Частота запуска - **При запуске программы**

Журналы уведомления

Журналы выполнения задач

- Интеграция с SIEM
    - Отправлять события по протоколу syslog на внешний syslog-сервер - выключить
    - Конвертировать события в формат структурированных данных - выключить
    - Параметры подключения
        - Адрес: нет

Уведомления о событиях

- Уведомления
    - Уведомление пользователей - **Средствами службы терминалов**

- Пороги формирования
    - Базы программы устарели (сут) - **7**
    - Базы программы сильно устарели (сут) - **14**
    - Проверка важных областей защищаемого устройства давно не выполнялись (сут) - **30**

Взаимодействие с сервером администрирования

- Данные об объектах карантина - **включить**
- Данные об объектах резервного хранилища - **включить**
- Данные о блокированных хостах - **включить**

Профили политики

Revision #1
Created 18 June 2025 18:54:31 by admin_mf
Updated 18 June 2025 18:56:10 by admin_mf