Задачи KES для Linux Servers 12.2

Задача инвентаризации KES Linux Servers 12.2

- **Тип задачи:** Инвентаризация
- **Общее**
  - Распределить по подгруппам - **включить**
- **Уведомление**
  - Сохранять информацию о результатах
    - На сервере администрирования - **15 суток**
    - Хранить в журнале событий ОС на устройстве - **выключить**
    - Хранить в журнале событий ОС на Сервере - **выключить**
    - Сохранять все события - **включить**
- **Расписание:**
  - Еженедельно - **Воскресенье. 09:00**
  - Запускть пропущеные задачи - **выключить**
  - Использовать автоматическое определение случайного интервала между запусками задачи - **включить**
- **Параметры**
  - Добавлять файлы в категорию Золотой образ - **выключить**
  - Проверять все исполняемые файлы - **включить**
  - Проверять двоичные файлы - **включить**
  - Проверять скрипты - **включить**
  - Области проверки
    - **/usr/bin**
- Исключения

    - Не заданы

- Исключения из областей действия задач
    - Не заданы

Задача поиск вредоносного ПО KES Linux Servers 12.2

- **Тип задачи:** Поиск вредоносного ПО
- **Общее**
    - Распределить по подгруппам - **включить**

- **Уведомление**

- Сохранять информацию о результатах
    - На сервере администрирования - **15 суток**
    - Хранить в журнале событий ОС на устройстве - **выключить**
    - Хранить в журнале событий ОС на Сервере - **выключить**
    - Сохранять все события - **включить**

- **Расписание**
    - Ежедневно - 21:00

- **Параметры**
    - Область проверки - **"/"**
    - Параметры области проверки
        - Проверять файлы - **включить**
        - Проверять загрузочные секторы - **включить**
        - Проверять память ядра и запущенные процессы - **выключить**
        - Проверять объекты автозапуска - **включить**
        - Устройство для проверки - **/****
        - Использовать глобальные исключения - **включить**
        - Использовать исключения Защиты от файловых угроз - **включить**

    - Действия при обнаружении угрозы
        - Первое - **Выполнять рекомендованное действие**
        - Второе - **Пропускать**

- **Исключения**

    - **Не заданы, потому что должны подтягиваться из основной политики, иначе придется дублировать.**

- **Исключения из областей действия задачи**
    - Не задано

Задача Обновления ПО KES Linux Servers 12.2

- **Тип задачи:** Обновление
- **Общее**
    - Распределить по подгруппам - **включить**

- **Уведомление**

- Сохранять информацию о результатах
    - На сервере администрирования - **15 суток**
    - Хранить в журнале событий ОС на устройстве - **выключить**
    - Хранить в журнале событий ОС на Сервере - **выключить**
    - Сохранять все события - **включить**

- **Расписание**
    - Запуск по расписанию - **Каждые 60 мин**

- **Источники обновлений - Kaspersky Security Center**
    - Использовать серверы обновлений "Лаборатория Касперского", если другие источники обновления не доступны - **включить**

- **Параметры**
    - Максимальное время ожидания ответа от источника обновлений (сек) - **10**
    - Режим загрузки обновлений - Загружать и устанавливать

- **Исключения из областей действия задачи**
    - Не задано

Задача Проверка важных областей KES Linux Servers 12.2

- **Тип задачи:** Проверка важных областей
- **Общее**
  - Распределить по подгруппам - **включить**

- **Уведомление**

- Сохранять информацию о результатах
  - На сервере администрирования - **15 суток**
  - Хранить в журнале событий ОС на устройстве - **выключить**
  - Хранить в журнале событий ОС на Сервере - **выключить**
  - Сохранять все события - **включить**

- **Расписание**
  - Запуск по расписанию - **Ежедневно 20:00**
  - Запускать пропущеные задачи - **выключить**
  - Использовать автоматическое определение случайного интервала между запусками задачи - **включить**

- **Параметры**
  - **Области проверки**
  - **/etc/**
  - **/etc/fstab**
  - **/etc/systemd/**
  - **/etc/sysctl.conf**
  - **/bin/**
  - **/sbin/**
  - **/usr/bin/**
  - **/usr/sbin/**

- **Параметры области проверки**
  - Проверять файлы - **включить**
  - Проверять загрузочные секторы - **включить**
  - Проверять память ядра и запущенные процессы - **включить**
  - Проверять объекты автозапуска - **включить**
  - Устройства для проверки - **/****
  - Использовать глобальные исключения - **включить**
  - Использовать исключения Защиты от файловых угроз - **включить**

- **Параметры проверки**

    - Проверять архивы - **включить**
    - Проверять почтовые базы - **выключить**
    - Проверять файлы почтовых форматов - **выключить**
    - Пропускать файл, если его проверка длится более (сек) - **0**
    - Пропускать файл, если его размер более (МБ) - **0**
    - Сообщать о незараженных обхектах - **выключить**
    - Сообщать о небработанных объектах - **выключить**
    - Использовать технологию iChecker - **включить**
    - Использовать эвристический анализ - **включить**
        - Уровень эвристического анализа - **Рекомендованный**
    - Действия при обнаружении угрозы
        - Первое - **Выполнять рекомендованное действие**
        - Второе - **Пропускать**

- **Исключения**
    - Не заданы

- **Исключения из областей действия задач**
    - Не заданы

Задача проверка контейнеров KES Linux Servers 12.2

- **Тип задачи:** Проверка контейнеров
- **Общее**
    - Распределить по подгруппам - **включить**

- **Уведомление**

- Сохранять информацию о результатах
    - На сервере администрирования - **15 суток**
    - Хранить в журнале событий ОС на устройстве - **выключить**
    - Хранить в журнале событий ОС на Сервере - **выключить**
    - Сохранять все события - **включить**

- **Расписание**
    - Запуск по расписанию - **Ежедневно 07:00**

- Запускать пропущеные задачи - **выключить**
- Использовать автоматическое определение случайного интервала между запусками задачи - **включить**

- **Параметры**
  -
  - Параметры проверки контейнеров
    - Проверять контейнеры по маске - *****
    - **Остановить, если не удалось вылечить**
  - Параметры проверки образов
    - Проверять образы по маске - *****
    - При обнаружении угрозы - **Пропустить образ**
  - Проверять каждый слой - **выключить**
  - Общие параметры проверки
    - Проверять архивы - **включить**
    - Проверять почтовые базы - **выключить**
    - Проверять файлы почтовых форматов - **выключить**
    - Пропускать файл, если его проверка длится более (сек) - **0**
    - Пропускать файл, если его размер более (МБ) - **0**
    - Сообщать о незараженных обхектах - **выключить**
    - Сообщать о небработанных объектах - **выключить**
    - Использовать технологию iChecker - **включить**
    - Использовать эвристический анализ - **включить**
      - Уровень эвристического анализа - **Рекомендованный**
    - Действия при обнаружении угрозы
      - Первое - **Выполнять рекомендованное действие**
      - Второе - **Пропускать**

- **Исключения**
  - Не заданы
  - Использовать глобальные исключения - **включить**

- **Исключения из областей действия задач**
  - Не заданы

Задача проверка целостности системы KES Linux Servers 12.2

- **Тип задачи:** Проверка целостности системы
- **Общее**
  - Распределить по подгруппам - **включить**

- **Уведомление**

- Сохранять информацию о результатах
  - На сервере администрирования - **15 суток**
  - Хранить в журнале событий ОС на устройстве - **выключить**
  - Хранить в журнале событий ОС на Сервере - **выключить**
  - Сохранять все события - **включить**

- **Расписание**
  - Запуск по расписанию - **Еженедельно, воскресенье 15:00**
  - Запускать пропущеные задачи - **выключить**
  - Использовать автоматическое определение случайного интервала между запусками задачи - **включить**

- **Параметры**
  - Обновлять снимок состояния системы при каждом запуске задачи - **выключить**
  - Использовать хеш SHA256 для проверки - **включить**
  - Проверять директории в областях мониторинга - **выключить**
  - Отслеживать время последнего доступа к файлу - **включить**
  - Области мониторинга

Название области	Путь	Комментарий
Внутренние объекты Kaspersky	/opt/kaspersky/kesl	
Системная конфигурация	/etc	
Данные пользователей	/etc/passwd	
Пароли пользователей	/etc/shadow	
Группы пользователей	/etc/group	
Правила повышения привилегий	/etc/sudoers	
Точки монтирования	/etc/fstab	
Доступ по SSH	/etc/ssh/sshd_config	
Автозагрузка служб	/etc/systemd/	
Системные бинарники	/bin	

Системные бинарники	/sbin	
Пользовательские бинарники	/usr/bin	
Пользовательские бинарники	/usr/sbin	
Библиотеки	/lib	
Библиотеки	/lib64	
Библиотеки	/usr/lib	
Библиотеки	/usr/lib64	
Модули ядра	/lib/modules	
Ядро и загрузка	/boot	
Планировщик заданий	/etc/crontab	
Планировщик заданий	/etc/cron.d/	
Планировщик заданий	/var/spool/cron	
Модули аутентификации PAM	/etc/pam.d/	
Настройки аудита	/etc/audit	
Автозагрузка служб	/etc/init.d/	

- **Исключения**
  - Не заданы
  - Использовать глобальные исключения - **включить**

- **Исключения из областей действия задач**
  - Не заданы

Задача запуска приложения KES Linux Servers 12.2

- **Тип задачи:** Запуск приложения kesl
- **Общее**
  - Распределить по подгруппам - **включить**

- **Уведомление**

- Сохранять информацию о результатах
  - На сервере администрирования - **7 суток**

- Хранить в журнале событий ОС на устройстве - **выключить**
- Хранить в журнале событий ОС на Сервере - **выключить**
- Сохранять все события - **включить**

- **Расписание**
  - Запуск по расписанию - **Ежедневно 06:00**
  - Запускать пропущеные задачи - **выключить**
  - Использовать автоматическое определение случайного интервала между запусками задачи - **включить**

- **Параметры**
  - Kaspersky Endpoint Security 12.2. для Linux - **включить**
  - Команда - **Запустить приложение**

- **Исключения из областей действия задач**
  - Не заданы

Revision #1
Created 18 June 2025 18:58:10 by admin_mf
Updated 18 June 2025 18:58:50 by admin_mf