ЛАБОРАТОРИЯ КАСПЕРСКОГО

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition

СРАВНЕНИЕ С АНТИВИРУСОМ КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS

АНТИВИРУС КАСПЕРСКОГО 6.0 ДЛЯ WINDOWS SERVERS ENTERPRISE EDITION

Сравнение с Антивирусом Касперского 6.0 для Windows Servers

Тел., факс: +7 (495) 797-8700, +7 (495) 645-7939, +7 (495) 956-7000
http://www.kaspersky.ru

Дата редакции: сентябрь 2007 г.

Содержание

ГЛАВА 1. ЧТО НОВОГО В ЭТОЙ ВЕРСИИ ПРИЛОЖЕНИЯ

Удобные средства управления

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition использует в качестве основного средства управления Microsoft Management Console (MMC). Это стандартное средство для управления серверными приложениями. Консоль может применяться для локального и удаленного управления. Также возможно локальное и удаленное управление через Kaspersky Administration Kit и командную строку.

Подробнее см. раздел «О консоли Антивируса в MMC» и главы «Управление Антивирусом из командной строки» и «Настройка и управление через Kaspersky Administration Kit» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Защита терминальных серверов

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition разработан с учетом требований для защиты терминальных серверов. Приложение обеспечивает защиту терминальных серверов Microsoft Terminal, Citrix Metaframe XPe FR 3 и Citrix Presentation Server. Поддерживаются режимы публикации рабочего стола и публикации приложений. Оптимизировано потребление ресурсов, обеспечивается корректное ведение статистики и журналов.

Подробнее см. главу «Введение» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Защита высокопроизводительных серверов

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition позволяет хранить и обрабатывать большое число записей в журнале и большое число объектов в карантине и резервном хранилище. Создана мощная и удобная система поиска и фильтрации записей в журнале.

Подробнее см. раздел «Способы регистрации событий» и главы «Изолирование подозрительных объектов. Использование карантина» и «Резервное копирование объектов перед лечением / удалением. Использование резервного хранилища» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Корректная работа на кластерах

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition может устанавливаться и работать на серверах, входящих в кластер. Поддерживается корректная работа сервера при миграции кластерных ресурсов (failover/failback).

Подробнее см. главу «Введение» Руководства по установке для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Индивидуальные значения параметров защиты для разных областей

Появилась возможность установки разных значений параметров защиты для разных защищаемых областей (дисков, папок).

Подробнее см. разделы «Настройка параметров безопасности выбранного узла» в главе «Проверка по требованию» и в главе «Постоянная защита» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Шаблоны настроек

Реализована возможность сохранения параметров защиты, установленных для какой-либо области, в шаблон. Этот шаблон может использоваться для оперативной настройки параметров защиты других областей. Шаблонов может быть несколько.

Подробнее см. разделы «Работа с шаблонами в задаче *Постоянная защита файлов*» и «Работа с шаблонами в задачах проверки по требованию» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Действие над объектом в зависимости от типа угрозы

Предусмотрена возможность настройки действий над объектом (лечить, помещать на карантин, удалять) в зависимости от типа обнаруженной в объекте угрозы (вирус, троянская программа и т.п.). Для угроз разных типов могут быть назначены разные действия.

Подробнее см. раздел «Действия в зависимости от типа угрозы» в приложении «Описание общих параметров Антивируса, параметров его функций и задач» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Разграничение полномочий администраторов

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition позволяет разграничить права администраторов. При этом используется стандартная система учетных записей на уровне операционной системы (локальные и доменные учетные записи). Например, может быть создана учетная запись, которая будет работать только с отчетами или объектами в карантине и резервном хранилище.

Подробнее см. раздел «Разграничение прав доступа к функциям Антивируса» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Блокирование доступа к серверу с зараженных узлов

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition предоставляет возможность блокировать доступ к сетевым ресурсам защищаемого сервера с зараженных сетевых узлов (рабочих станций) на определенное время. Данная опция может быть включена администратором и гибко настраивается.

Подробнее см. раздел «О блокировании доступа с компьютеров к защищаемому серверу» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Проверка скриптов

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition проверяет выполняемые скрипты на 32-х и 64-х битных системах.

Подробнее см. раздел «О задачах постоянной защиты» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Использование SNMP-протокола

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition поддерживает передачу информации о текущем состоянии защиты при помощи Simple Network Management Protocol (SNMP). SNMP-протокол активно используется в крупных сетях для мониторинга состояния серверов, сетевого оборудования и всей сети в целом.

Подробнее см. главу «Счетчики и ловушки SNMP Антивируса» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Сохранение метаинформации для объектов, помещаемых в карантин и резервное хранилище

Антивирус Касперского 6.0 для Windows Servers Enterprise Edition сохраняет метаинформацию (права доступа и атрибуты) для файлов, помещаемых в карантин или резервное хранилище. При восстановлении файла метаинформация восстанавливается.

Подробнее см. разделы «Восстановление объектов из карантина» и «Восстановление файлов из резервного хранилища» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

Совместимость с системами резервного копирования

Предусмотрена возможность отключения проверки файлов, обращение к которым производится программами резервного копирования.

Подробнее см. раздел «Отключение постоянной защиты файлов на время резервного копирования» Руководства администратора для Антивируса Касперского 6.0 для Windows Servers Enterprise Edition.

ГЛАВА 2. ТАБЛИЦА ОСНОВНЫХ ОТЛИЧИЙ

Описание возможности	Антивирус Касперского 6.0 для Windows Servers	Антивирус Касперского 6.0 для Windows Servers Enterprise Edition
Защита от угроз (вирусов, троянских программ и т.п.)		
Проверка и лечение архивированных файлов		
Удаленное и локальное управление через MMC		
Управление через Kaspersky Administration Kit		
Защита терминальных серверов		
Балансировка нагрузки		
Работа на кластерах		
Индивидуальные параметры защиты для каждой области		
Шаблон параметров		
Действие над объектом в зависимости от типа обнаруженной угрозы		

Описание возможности	Антивирус Касперского 6.0 для Windows Servers	Антивирус Касперского 6.0 для Windows Servers Enterprise Edition
Блокирование доступа к серверу с зараженных узлов	○	●
Проверка скриптов	○	●
Поддержка SNMP-протокола	○	●
Разграничение полномочий администраторов	◐	●
Сохранение прав доступа для файлов и папок при помещении их в карантин или резервное хранилище	○	●