KASPERSKY lab

Kaspersky Security для систем хранения данных

Руководство по масштабированию для защиты ICAP-подключаемых сетевых хранилищ

Уважаемый пользователь!

Спасибо за то, что выбрали наш продукт. Мы надеемся, что этот документ поможет вам в работе и ответит на большинство возникающих вопросов.

Документ и связанные с ним графические изображения могут быть использованы только в информационных, некоммерческих или личных целях.

Документ может быть изменен без предварительного уведомления. Последнюю версию документа вы можете найти на сайте «Лаборатории Касперского» по адресу http://www.kaspersky.ru/docs.

Дата редакции документа: 26.02.2016

http://www.kaspersky.ru
https://help.kaspersky.com
http://support.kaspersky.ru

Содержание

Об этом руководстве

Руководство по масштабированию Kaspersky Security для Windows Server®, входящего в состав решения программы для защиты систем хранения данных, адресовано специалистам, которые осуществляют установку и администрирование Kaspersky Security, а также техническую поддержку организаций, использующих Kaspersky Security для защиты сетевых хранилищ.

Цель экспериментов, описанных в этом документе – измерить производительность Kaspersky Security и защищаемых ICAP-подключаемых сетевых хранилищ при разных нагрузках на серверы с установленным Kaspersky Security и конфигурациях этих серверов и защищаемых сетевых хранилищ.

Вы можете применять информацию в этом руководстве для оценки количества серверов с установленным Kaspersky Security, требующихся для защиты сетевых хранилищ организации.

В этом разделе

В этом документе

Руководство по масштабированию для защиты ICAP-подключаемых сетевых хранилищ содержит следующие разделы:

Kaspersky Security

Этот раздел содержит описание функций Kaspersky Security.

Рекомендации по защите сетевых хранилищ

Этот раздел содержит рекомендации по использованию задач Kaspersky Security для защиты ICAP-подключаемых сетевых хранилищ, а также формулы для расчета минимального и оптимального количества требующихся сереверов Kaspersky Security.

Производительность Kaspersky Security

Этот разделе содержит информацию об экспериментах по измерению производительности Kaspersky Security и защищаемых сетевых хранилищ, подключаемых по протоколу ICAP, при разных нагрузках на серверы Kaspersky Security и конфигурациях этих серверов и защищаемых сетевых хранилищ.

Масштабирование Kaspersky Security

Этот раздел содержит рекомендации по защите сетевых хранилищ с помощью Kaspersky Security, а также инструкции по расчету минимального и оптимального количества требующихся серверов Kaspersky Security.

АО «Лаборатория Касперского»

Этот раздел содержит информацию об АО «Лаборатория Касперского».

Уведомления о товарных знаках

В этом разделе перечислены товарные знаки сторонних правообладателей, использованные в документе.

Условные обозначения

В этом документе используются условные обозначения (см. таблицу ниже).

Таблица 1. Условные обозначения

Пример текста	Описание условного обозначения
Обратите внимание на то, что...	Предупреждения выделены красным цветом и заключены в рамку. Предупреждения содержат информацию о действиях, которые могут иметь нежелательные последствия.
Рекомендуется использовать...	Примечания заключены в рамку. Примечания содержат дополнительную и справочную информацию.
Пример: …	Примеры приведены в блоках на голубом фоне под заголовком «Пример».

Пример текста	Описание условного обозначения
Обновление – это... Возникает событие *Базы устарели*.	Курсивом выделены следующие элементы текста: • новые термины; • названия статусов и событий программы.
Нажмите на клавишу **ENTER**. Нажмите комбинацию клавиш **ALT**+**F4**.	Названия клавиш клавиатуры выделены полужирным шрифтом и прописными буквами. Названия клавиш, соединенные знаком + (плюс), означают комбинацию клавиш. Такие клавиши требуется нажимать одновременно.
Нажмите на кнопку **Включить**.	Названия элементов интерфейса программы, например, полей ввода, пунктов меню, кнопок, выделены полужирным шрифтом.
► *Чтобы настроить расписание задачи, выполните следующие действия:*	Вводные фразы инструкций выделены курсивом и значком «стрелка».
В командной строке введите текст `help` Появится следующее сообщение: Укажите дату в формате `ДД:ММ:ГГ`.	Специальным стилем выделены следующие типы текста: • текст командной строки; • текст сообщений, выводимых программой на экран; • данные, которые требуется ввести с клавиатуры.
<Имя пользователя>	Переменные заключены в угловые скобки. Вместо переменной требуется подставить соответствующее ей значение, опустив угловые скобки.

Kaspersky Security

Функциональные компоненты, обеспечивающие защиту подключаемых сетевых хранилищ, входят в состав решения *Kaspersky Security для систем хранения данных* для программы Kaspersky Security 10 для Windows Server.

Подробную информацию о доступных решениях Kaspersky Security для защиты вы можете найти на веб-сайте «Лаборатории Касперского» (http://www.kaspersky.ru) и в *Руководстве администратора Kaspersky Security 10 для Windows Server*.

О программе

Kaspersky Security 10 для Windows Server (ранее «Антивирус Касперского для Windows Servers Enterprise Edition») защищает серверы, работающие под управлением операционных систем Microsoft® Windows®, и сетевые хранилища от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена. Kaspersky Security предназначен для использования в локальных сетях средних и крупных организаций. Пользователями Kaspersky Security являются администраторы сети организации и сотрудники, отвечающие за антивирусную защиту сети организации.

Вы можете установить Kaspersky Security на следующих серверах:

- на терминальных серверах;
- на серверах печати;
- на серверах приложений;
- на контроллерах доменов;
- на серверах, защищающих сетевые хранилища;
- на файловых серверах – они более других подвержены заражению, так как обмениваются файлами с рабочими станциями пользователей.

Вы можете управлять Kaspersky Security следующими способами:

- через Консоль Kaspersky Security, установленную на одном сервере с Kaspersky Security или на другом компьютере;
- с помощью команд командной строки;
- через Консоль администрирования Kaspersky Security Center.

Вы можете использовать программу Kaspersky Security Center для централизованного управления защитой многих серверов, на каждом из которых установлен Kaspersky Security.

Системные и аппаратные требования Kaspersky Security

На странице Kaspersky Security 10 для Windows Server (http://www.kaspersky.com/business-security/windows-server-security) вы можете найти актуальную информацию о системных и аппаратных требованиях, которым должны удовлетворять защищаемые сервера или сетевые хранилища для успешной установки и использования программы.

Компоненты Kaspersky Security

В состав программы входят следующие компоненты:

- Постоянная защита.

  Kaspersky Security проверяет объекты при обращении к ним.

- Контроль сервера.

  Kaspersky Security отслеживает все обращения к сетевым файловым ресурсам, позволяет контролировать запуск программ и блокирует доступ к серверу для удаленных компьютеров, если с их стороны выявлена вредоносная активность или активность шифрования.

- Защита RPC-подключаемых сетевых хранилищ и Защита ICAP-подключаемых сетевых хранилищ.

  Kaspersky Security, установленный на сервере под управлением операционной системы Microsoft Windows, защищает сетевые хранилища от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.

- Проверка по требованию.

  Kaspersky Security однократно проверяет указанную область на наличие вирусов и других угроз компьютерной безопасности. Kaspersky Security проверяет файлы, оперативную память сервера, а также объекты автозапуска.

О защите ICAP-подключаемых сетевых хранилищ

Kaspersky Security, установленный на сервере под управлением операционной системы Microsoft Windows, защищает ICAP-подключаемые сетевые хранилища (например, EMC™ Isilon™) от вирусов и других угроз компьютерной безопасности, проникающих посредством файлового обмена.

Kaspersky Security не имеет прямого доступа к файлам, размещенным в ICAP-подключаемом сетевом хранилище (далее также *сетевом хранилище*). При попытке чтения, создания или изменения файла, сетевое хранилище формирует ICAP-запрос к Kaspersky Security и передает файл внутри этого запроса. Программа выполняет антивирусную проверку файла в соответствии с параметрами, заданными в задаче Защита ICAP-подключаемых сетевых хранилищ. При обнаружении угрозы Kaspersky Security выполняет над файлом действия, заданные в параметрах задачи, и передает результат проверки сетевому хранилищу. Если в параметрах задачи задано действие Лечить, и файл удалось вылечить, Kaspersky Security возвращает сетевому хранилищу вылеченный файл в ответе на запрос.

В Kaspersky Security вы можете настроить действия, которые программа выполняет над зараженными и возможно зараженными файлами.

При использовании KSN в задаче Защита ICAP-подключаемых сетевых хранилищ Kaspersky Security не может удалять или блокировать файлы, которые используются ICAP-подключаемым сетевым хранилищем, так как на момент получения недоверенного заключения от служб KSN программа не имеет прямого доступа к сетевым каталогам хранилища. Информация о получении недоверенного заключения фиксируется в журнале выполнения задачи Использование KSN.

Вы можете защитить одно сетевое хранилище с помощью одного сервера с установленным Kaspersky Security. Для улучшения быстродействия сетевого хранилища и сервера с установленным Kaspersky Security вы можете использовать несколько серверов с установленным Kaspersky Security для защиты одного сетевого хранилища. В этом случае сетевое хранилище распределяет нагрузку между присоединенными серверами с установленным Kaspersky Security.

Задача Защита ICAP-подключаемых сетевых хранилищ создана по умолчанию и является системной задачей Kaspersky Security. Вы не можете удалить или переименовать эту задачу. Вы не можете создать пользовательские задачи защиты ICAP-подключаемых сетевых хранилищ. Вы можете настраивать задачу Защита ICAP-подключаемых сетевых хранилищ.

Вы можете запускать задачи защиты сетевых хранилищ, если активный ключ поддерживает функцию защиты сетевых хранилищ. Если вы запустите задачу защиты сетевых хранилищ, но активный ключ не поддерживает функцию защиты сетевых хранилищ, то задача завершится с ошибкой. В этом случае Kaspersky Security не защищает сетевые хранилища.

Компонент Защита ICAP-подключаемых сетевых хранилищ доступен в составе решения программы Kaspersky Security для систем хранения данных.

Подробная информация о решениях для защиты организации, в состав которых входит Kaspersky Security для Windows Server, содержится на веб-сайте «Лаборатории Касперского» и в *Руководстве администратора Kaspersky Security 10 для Windows Server.*

Рекомендации по защите сетевых хранилищ

Оптимальная защита ICAP-подключаемого сетевого хранилища во время использования Kaspersky Security обеспечивается при выполнении следующих условий:

- задача Защита ICAP-подключаемых сетевых хранилищ выполняется с параметрами, настроенными по умолчанию;
- задача Защита ICAP-подключаемых сетевых хранилищ запускается регулярно в соответствии с заданными параметрами расписания.

> Чтобы исключить вероятность остановки задачи после перезагрузки сервера, убедитесь, что запуск задачи по расписанию применяется. По умолчанию применение расписания в задаче Защита ICAP-подключаемых сетевых хранилищ отключено.

Для расчета минимального количества серверов Kaspersky Security, требующихся для защиты ICAP-подключаемых сетевых хранилищ, вы можете использовать следующую формулу:

$$N_{min} = \frac{O_{max}}{C_{max}} \times \frac{K}{R_{max}} + 1$$

, где используются переменные:

- *N min* - минимальное количество требующихся KS-серверов;
- *O max* - пиковая пропускная способность KS-сервера;
- *C max* - количество операций по протоколу CIFS (20);
- *K* - процент команд, которые приводят к сканированию файлов (10 %);
- *R max* - максимальное количество операций по протоколу CIFS (40).

Для расчета оптимального количества серверов Kaspersky Security, требующихся для защиты ICAP-подключаемых сетевых хранилищ, рекомендуется использовать следующую формулу:

$$[N_{min}, N_{min} \times 2]$$

См. также

Производительность Kaspersky Security

В этом разделе содержится информация об экспериментах по измерению производительности Kaspersky Security и защищаемых сетевых хранилищ, подключаемых по протоколу ICAP, при разных нагрузках на серверах Kaspersky Security и конфигурациях этих серверов и защищаемых сетевых хранилищ.

В этом разделе

Конфигурации участников экспериментов

Сетевое хранилище

EMC Isilon под управлением операционной системой OneFS™ v7.1.0.3 B_7_1_0_91(RELEASE).

Программное и аппаратное обеспечение установлено на все узлы без дополнительных пакетов и обновлений.

Аппаратное обеспечение кластера

Таблица 2. Аппаратное обеспечение кластера

Узел	Модель	Конфигурация	Серийный номер
1	Isilon X200-2U-Single-12Gb-2x10GE SPF+-12Tb	400-0034-03	SX-200-231228-0065
2	Isilon X200-2U-Single-12Gb-2x10GE SPF+-12Tb	400-0034-03	SX-200-231228-0068
3	Isilon X200-2U-Single-12Gb-2x10GE SPF+-12Tb	400-0034-03	SX-200-231228-0067
4	Isilon X200-2U-Single-12Gb-2x10GE SPF+-12Tb	400-0034-03	SX-200-231228-0066

Программное обеспечение кластера

Таблица 3. Программное обеспечение кластера

Устройство	Тип	Прошивка	Узлы
IsilonFPV1	FrontPnl	UI.01.29	1-4
IsilonIB	Network	4.8.930+205-0002-05_A	1-4
LSI	DiskCtrl	16.00.01.00	1-4
LSIExp0	DiskExp	0910+0210	1-4

Средство виртуализации

Среда под управлением Hyper-V® Server:

- Производитель: IBM®.
- Модель системы: IBM System x3550 M4 Server -[7914L2G].

- Тип системы: 64-разрядная операционная система.
- Объем оперативной памяти: 32741 МБ.
- Процессор: однопроцессорная конфигурация, Intel® 64 семейства 6 модели 45 Stepping 7 GenuineIntel ~ 2700 Mhz.
- Операционная система: Microsoft Windows Server 2012 R2 Standard.
- Сетевые карты:
  - Intel Ethernet Server Adapter I340-T4.
  - Intel I350 Gigabit Network Connection.
  - IBM USB Remote NDIS Network Device.
  - Hyper-V Virtual Ethernet Adapter, vEthernet (Intel I350 Gigabit Network Connection #3 - Virtual Switch).

Виртуальные машины

Сервер Kaspersky Security:

- Производитель: Microsoft Corporation.
- Модель системы: виртуальная машина.
- Тип системы: 64-разрядная операционная система.
- Объем оперативной памяти: 8192 МБ.
- Операционная система: Microsoft Windows Server 2008 R2 Standard.
- Процессор: однопроцессорная конфигурация; Intel64 Family 6 Model 45 Stepping 7 GenuineIntel ~2700 Mhz
- Сетевая карта: Microsoft Virtual Machine Bus Network Adapter.

Клиентские компьютеры:

- Производитель: Microsoft Corporation.
- Модель системы: виртуальная машина.
- Тип системы: 64-разрядная операционная система.
- Объем оперативной памяти: 4096 МБ.
- Операционная система: Microsoft Windows Server 2008 R2 Standard.
- Процессор: однопроцессорная конфигурация; Intel64 Family 6 Model 45 Stepping 7 GenuineIntel ~ 2700 Mhz.
- Сетевая карта: Microsoft Virtual Machine Bus Network Adapter.

Информация о проведенных экспериментах

Для получения данных о производительности Kaspersky Security было проведено два эксперимента с использованием серверов с установленным Kaspersky Security (далее также «KS-серверы»). При проведении экспериментов имитируется доступ пользователей в папки, находящиеся в сетевом хранилище, и измеряется нагрузка на KS-серверы.

Условия для проведения экспериментов:

- Используется хранилище Isilon, защищенное KS-сервером (Эксперимент 1) или двумя KS-серверами (Эксперимент 2).
- В сетевом хранилище создаются папки (профили пользователя), содержащие 1350 файлов разного размера, по 150 копий каждого: 1 КБ, 10 КБ, 100 КБ, 500КБ, 1 МБ, 3 МБ, 5 МБ, 7 МБ, 10 МБ. Количество копий этой папки в сетевом хранилище соответствует количеству пользователей, обращающихся к этому хранилищу.
- Каждой копии папки соответствует скрипт, запускаемый с клиентских компьютеров. Скрипт имитирует работу пользователя с профилем, т.е. последовательное открытие и закрытие каждого файла.
- С помощью компонента Счетчик производительности измеряется нагрузка на KS-сервер. Раз в четыре секунды снимаются показатели количества потребляемой KS-сервером оперативной памяти и процент загрузки процессоров KS-сервера. Данные о нагрузке на KS-сервер регистрируются в программе Системный монитор Microsoft Windows.

Проведенные эксперименты:

- Эксперимент 1 (см. раздел «Эксперимент 1. Измерение нагрузки на один KS-сервер при разном количестве одновременных обращений к файлам хранилища» на стр. 18): вычисляется нагрузка на один KS-сервер при разном количестве одновременных обращений пользователей к файлам хранилища. Цель эксперимента - сравнить данные нагрузки на KS-сервер при увеличении количества пользователей, одновременно обращающихся к сетевому хранилищу.

- Эксперимент 2 (см. раздел «Эксперимент 2. Измерение нагрузки на один и два KS-сервера при фиксированном количестве одновременных обращений к файлам хранилища» на стр. 20): вычисляется нагрузка на KS-серверы при использовании одного или двух KS-серверов при обращении к ним фиксированного числа пользователей. Цель эксперимента - сравнить данные распределения нагрузки при использовании одного и двух KS-серверов для защиты сетевого хранилища при фиксированном количестве пользователей, одновременно обращающихся к этому хранилищу.

Эксперимент 1. Измерение нагрузки на один KS-сервер при разном количестве одновременных обращений к файлам хранилища

Цель Эксперимента 1 - сравнить данные нагрузки на KS-сервер при увеличении количества пользователей, одновременно обращающихся к сетевому хранилищу.

Описание эксперимента

Для проведения эксперимента настроен один KS-сервер, защищающий сетевое хранилище Isilon. Имитируется доступ пользователей к данным сетевого хранилища. Количество пользователей последовательно увеличивается:

- 0 пользователей (отсутствуют обращения к хранилищу Isilon);
- 24 пользователя (имитируется доступ к хранилищу Isilon одновременно 24 пользователей, каждый пользователь обращается в свой профиль);
- 50 пользователей (имитируется доступ к хранилищу Isilon одновременно 50 пользователей, каждый пользователь обращается в свой профиль);
- 76 пользователей (имитируется доступ к хранилищу Isilon одновременно 76 пользователей, каждый пользователь обращается в свой профиль);
- 100 пользователей (имитируется доступ к хранилищу Isilon одновременно 100 пользователей, каждый пользователь обращается в свой профиль).

Таблица 4. Вычисление нагрузки на один KS-сервер при разном количестве одновременных обращений к хранилищу

Активность обращения к хранилищу Isilon					
Количество пользователей, обращающихся к хранилищу	**0**	**24**	**50**	**76**	**100**
Продолжительность активности обращения (ч)	0:00:00	2:20:00	4:46:00	7:21:00	9:24:00
Нагрузка на KS-сервер					
Время работы Счетчика производительности (ч)	3:00:00	2:30:00	5:00:00	8:00:00	10:00:00
Общая загрузка центрального процессора (%)	1	36	35	35	35
Увеличение загрузки центрального процессора (по сравнению с отсутствием обращений) (%)	0	35	34	34	34
Общее потребление оперативной памяти (МБ)	889	917	963	977	988
Увеличение потребления оперативной памяти (по сравнению с отсутствием обращений) (МБ)	0	28	74	88	99

Выводы

- Нагрузка на центральный процессор при увеличении количества пользователей не меняется.
- Увеличивается количество используемой оперативной памяти при увеличении количества пользователей.

Критичным параметром для производительности работы среды является производительность подсистем хранилища, так как общее время обработки обращений KS-сервером увеличивается с ростом количества пользователей.

Эксперимент 2. Измерение нагрузки на один и два KS-сервера при фиксированном количестве одновременных обращений к файлам хранилища

Цель эксперимента - сравнить данные распределения нагрузки при использовании одного и двух KS-серверов для защиты сетевого хранилища при фиксированном количестве пользователей, одновременно обращающихся к этому хранилищу.

Описание эксперимента

Для проведения эксперимента настроены один или два KS-сервера, которые защищают одно хранилище Isilon. Имитируется доступ фиксированного количества пользователей (25) к данным сетевого хранилища.

Измерения нагрузки на KS-серверы проведены при следующих условиях:

- Нет активности обращения к сетевому хранилищу.
- Настроен и включен один KS-сервер, имитируется доступ к сетевому хранилищу одновременно 25 пользователей.
- Настроено два KS-сервера, один KS-сервер включен, другой KS-сервер выключен, имитируется доступ к сетевому хранилищу одновременно 25 пользователей.
- Настроено два KS-сервера, оба KS-сервера включены, имитируется доступ к сетевому хранилищу одновременно 25 пользователей.

Результаты, полученные в ходе вычисления нагрузки на KS-серверы, описаны в таблице ниже.

Таблица 5. Результаты вычисления нагрузки на KS-серверы

Активность обращения к хранилищу Isilon				
Количество пользователей, обращающихся к хранилищу	**0**	**25**	**25**	**25**
Продолжительность активности обращения (ч)	0:00:00	2:20:00	2:20:00	2:20:00
Нагрузка на KS-сервер				
Использование KS-серверов	Не используется	Один KS-сервер	Один из двух KS-серверов	Два из двух KS-серверов
Время работы Счетчика производительности (ч)	3:00:00	2:30:00	2:30:00	2:30:00
Общая загрузка центрального процессора (%)	1	36	20	21
Увеличение загрузки центрального процессора (по сравнению с отсутствием обращений) (%)	0	35	19	20
Общее потребление оперативной памяти (МБ)	889	918	1003	977
Увеличение потребления оперативной памяти (по сравнению с отсутствием обращений) (МБ)	0	29	114	108

Выводы

При увеличении количества KS-серверов:

- нагрузка на центральный процессор уменьшается.
- незначительно увеличивается коэффициент умножения оперативной памяти.

Критичным параметром для производительности работы среды является производительность подсистем хранилища, так как общее время обработки обращений KS-сервером не зависит от изменения количества KS-серверов, защищающих это хранилище.

Масштабирование Kaspersky Security

В этом разделе содержатся рекомендации по защите сетевых хранилищ с помощью Kaspersky Security, а также инструкции по расчету минимального и оптимального количества серверов Kaspersky Security, требующихся для защиты ICAP-подключаемых сетевых хранилищ.

В этом разделе

Расчет количества требующихся KS-серверов

Следующие расчеты позволяют определить минимальное и оптимальное количество KS-серверов, требующихся для защиты ICAP-подключаемых сетевых хранилищ организации:

- расчет значения пиковой пропускной способности KS-сервера;
- расчет дополнительного коэффициента умножения.

Расчет значения пиковой пропускной способности KS-сервера

Значение пиковой пропускной способности равно отношению произведения максимального количества операций по протоколу CIFS (20 операций / сек.) и количества файлов, к которым обращается один пользователь, к продолжительности операции.

► *Чтобы рассчитать значение пиковой пропускной способности KS-сервера, выполните следующие действия:*

1. Найдите произведение количества операций по протоколу CIFS (20) и количества файлов, к которым обращается один пользователь (1350).

   Полученное значение равно 27000.

2. Найдите отношение полученного значения к продолжительности операции (350).

   Полученное значение равно 77.

Пиковая пропускная способность KS-сервера для одного пользователя равна 77 операций / сек.

Вычисленные значения пиковой пропускной способности для разного количества пользователей приведены в таблице ниже.

Таблица 6. Расчет пиковой пропускной способности для разного количества пользователей

Параметр	Значение параметра				
Количество файлов хранилища Isilon, к которым обращаются пользователи	1350	32400	67500	101250	135000
Продолжительность операции сканирования (сек.)	350	8400	17760	26460	34920
Пиковая пропускная способность (операций / сек.)	77	77	76	76,5	77
Количество пользователей, запросивших доступ к хранилищу	1	24	50	75	100
Пиковая пропускная способность для данного количества пользователей (операций / сек.)	77	1851	3800	5739	7731

Расчет дополнительного коэффициента умножения

Для расчета оптимального количества KS-серверов требуется дополнительный коэффициент умножения, необходимый для учета тех команд, которые приводят к сканированию файлов. Коэффициент умножения равен отношению процента таких команд (2 команды из 20 - 10%) к максимальному количеству операций по протоколу CIFS (20 операций / сек.).

► *Чтобы рассчитать дополнительный коэффициент умножения, выполните следующие действия:*

1. Найдите произведение количества операций по протоколу CIFS и 2, чтобы при дальнейших расчетах учесть все возможные типы операций (открытие и закрытие) с файлами.

   Полученное значение является максимальным количеством операций по протоколу CIFS и равно 40.

2. Найдите отношение процентного количества команд, приводящих к сканированию файлов, к максимальному количеству операций по протоколу CIFS.

   Полученное значение равно 0,0025.

Дополнительный коэффициент умножения равен 0,0025.

Определение минимального количества требующихся KS-серверов

Минимальное количество требующихся серверов обеспечивает защиту сетевых хранилищ в условиях стабильной работы и гарантированного отсутствия сбоев в работе всех серверов сети.

Значение минимального количества требующихся KS-серверов равно отношению значения пиковой пропускной способности к количеству операций по протоколу CIFS, умноженному на дополнительный коэффициент.

► *Чтобы рассчитать минимальное количество необходимых KS-серверов, выполните следующие действия:*

1. Найдите отношение пиковой пропускной способности (см. таблицу Расчет пиковой пропускной способности для разного количества пользователей) к максимальному количеству операций по протоколу CIFS.

2. Полученное значение умножьте на дополнительный коэффициент умножения (0,0025).

3. Если необходимо, округлите полученное значение до целого числа.

Минимальное количество требующихся KS-серверов равно 1.

Определение оптимального количества требующихся KS-серверов

Оптимальное количество требующихся серверов обеспечивает защиту сетевых хранилищ в критических условиях работы, например, при выходе из строя всех серверов сети.

При расчете оптимального количества KS-серверов рекомендуется линейно увеличивать на 1 минимальное количество серверов или, для максимальной отказоустойчивости, дублировать каждый KS-сервер.

Выводы

При учете фактора отказоустойчивости оптимальное количество необходимых KS-серверов, требующихся для защиты сетевых хранилищ равно N+1; максимальное количество требующихся KS-серверов равно N*2, где N - минимальное количество требующихся KS-серверов без учета отказоустойчивости.

Примеры расчетов количества требующихся KS-серверов

Следующие значения позволяют рассчитать количество требующихся KS-серверов в условиях последовательного увеличения одновременных обращений пользователей к хранилищу Isilon:

- Динамический понижающий коэффициент. Позволяет учесть неравномерность нагрузки на KS-сервер при увеличении количества сканируемых файлов. Значение динамического понижающего коэффициента равно времени отклика хранилища Isilon при увеличении количества обращений и равно 8,6 мс.

  > Значение динамического понижающего коэффициента в настоящем эксперименте заимствуется из общедоступных источников http://www.spec.org/sfs2008/results/res2011q2/sfs2008-20110527-00194.html.

- Относительный динамический понижающий коэффициент для соответствующих значений пиковой пропускной способности. Относительный динамический понижающий коэффициент равен отношению текущего времени отклика для каждого значения пиковой пропускной способности к 8,6 мс.

Вычисленные значения количества требующихся KS-серверов с учетом динамического понижающего коэффициента приведены в таблице ниже.

Таблица 7. Расчетов количества требующихся KS-серверов

Параметр	Значение параметра						
Количество файлов хранилища Isilon, к которым обращаются пользователи	1350	32400	67500	101250	135000	1350000	2700000
Продолжительность операции сканирования (сек.)	350	8400	17760	26460	34920	Нет данных	Нет данных
Пиковая пропускная способность (операций / сек.)	77,14285714	77,14285714	76,01351351	76,53061224	77,31958763	76,82988553	76,82988553
Количество пользователей, запросивших доступ к хранилищу	1	24	50	75	100	1000	2000
Пиковая пропускная способность для данного количества пользователей (операций / сек.)	77,14285714	1851,428571	3800,675676	5739,795918	7731,958763	76829,88553	153659,7711
Количество операций по протоколу CIFS	20	20	20	20	20	20	20
Максимальное количество операций по протоколу CIFS	40	40	40	40	40	40	40
Процент количества команд, приводящих к сканированию файлов	0,1	0,1	0,1	0,1	0,1	0,1	0,1

Параметр	Значение параметра						
Минимальное количество требующихся KS-серверов	0,009642857	0,231428571	0,475084459	0,71747449	0,966494845	9,603735692	19,20747138
Минимальное количество требующихся KS-серверов (после округления)	1	1	1	1	1	9	19
Оптимальное количество требующихся KS-серверов	2	2	2	2	2	3	5
Максимальное количество требующихся KS-серверов	2	2	2	2	2	4	8

АО «Лаборатория Касперского»

«Лаборатория Касперского» – известный в мире производитель систем компьютерной защиты от различных видов угроз, включая защиту от вирусов и других вредоносных программ, нежелательной почты (спама), сетевых и хакерских атак.

В 2008 году «Лаборатория Касперского» вошла в четверку ведущих мировых лидеров рынка программных решений для обеспечения информационной безопасности конечных пользователей (рейтинг «IDC Worldwide Endpoint Security Revenue by Vendor»). В России, по данным IDC, «Лаборатория Касперского» – самый предпочитаемый производитель систем компьютерной защиты для домашних пользователей («IDC Endpoint Tracker 2014»).

«Лаборатория Касперского» основана в России в 1997 году. Сегодня «Лаборатория Касперского» – это международная группа компаний с 34 офисами в 31 стране мира. В компании работает более 3000 квалифицированных специалистов.

ПРОДУКТЫ. Продукты «Лаборатории Касперского» защищают как домашние компьютеры, так и компьютерные сети организаций.

Линейка персональных продуктов включает программы, обеспечивающие информационную безопасность настольных компьютеров и ноутбуков, планшетных компьютеров, смартфонов и других мобильных устройств.

Компания предлагает решения и технологии для защиты и контроля рабочих станций и мобильных устройств, виртуальных машин, файловых и веб-серверов, почтовых шлюзов, сетевых экранов. Также в портфеле компании есть специализированные продукты для защиты от DDoS-атак, защиты сред под управлением АСУТП и предотвращения финансового мошенничества. Использование этих решений в сочетании с централизованными средствами управления позволяет построить и эксплуатировать эффективную автоматизированную защиту организации любого размера от компьютерных угроз. Продукты «Лаборатории Касперского» сертифицированы крупными тестовыми лабораториями, совместимы с программным обеспечением многих поставщиков программного обеспечения и оптимизированы для работы на многих аппаратных платформах.

Вирусные аналитики «Лаборатории Касперского» работают круглосуточно. Каждый день они находят сотни тысяч новых компьютерных угроз, создают средства их обнаружения и лечения и включают сигнатуры этих угроз в базы, используемые программами «Лаборатории Касперского».

ТЕХНОЛОГИИ. Многие технологии, без которых трудно представить себе современный антивирус, впервые разработаны именно «Лабораторией Касперского». Не случайно программное ядро Антивируса Касперского используют в своих продуктах многие другие разработчики программного обеспечения, среди них: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, ZyXEL. Многие из инновационных технологий компании подтверждены патентами.

ДОСТИЖЕНИЯ. За годы борьбы с компьютерными угрозами «Лаборатория Касперского» завоевала сотни наград. Например, в 2014 году по итогам испытаний и исследований, проведенных авторитетной австрийской антивирусной лабораторией AV-Comparatives, «Лаборатория Касперского» стала одним из двух лидеров по количеству полученных сертификатов Advanced+, в результате компания была удостоена сертификата Top Rated. Но главная награда «Лаборатории Касперского» – это приверженность пользователей по всему миру. Продукты и технологии компании защищают более 400 миллионов пользователей. Количество организаций, являющихся ее клиентами, превышает 270 тысяч.

Веб-сайт «Лаборатории Касперского»:	http://www.kaspersky.ru
Вирусная энциклопедия:	http://www.securelist.ru/
Вирусная лаборатория:	http://newvirus.kaspersky.ru (для проверки подозрительных файлов и веб-сайтов)
Веб-форум «Лаборатории Касперского»:	http://forum.kaspersky.com

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки программы.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

EMC, Isilon и OneFS – товарные знаки или зарегистрированные в США и/или других странах товарные знаки EMC Corporation.

Intel – товарный знак Intel Corporation, зарегистрированный в Соединенных Штатах Америки и других странах.

IBM – товарный знак International Business Machines Corporation, зарегистрированный во многих юрисдикциях по всему миру.

Hyper-V Windows, Microsoft и Windows Server – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.