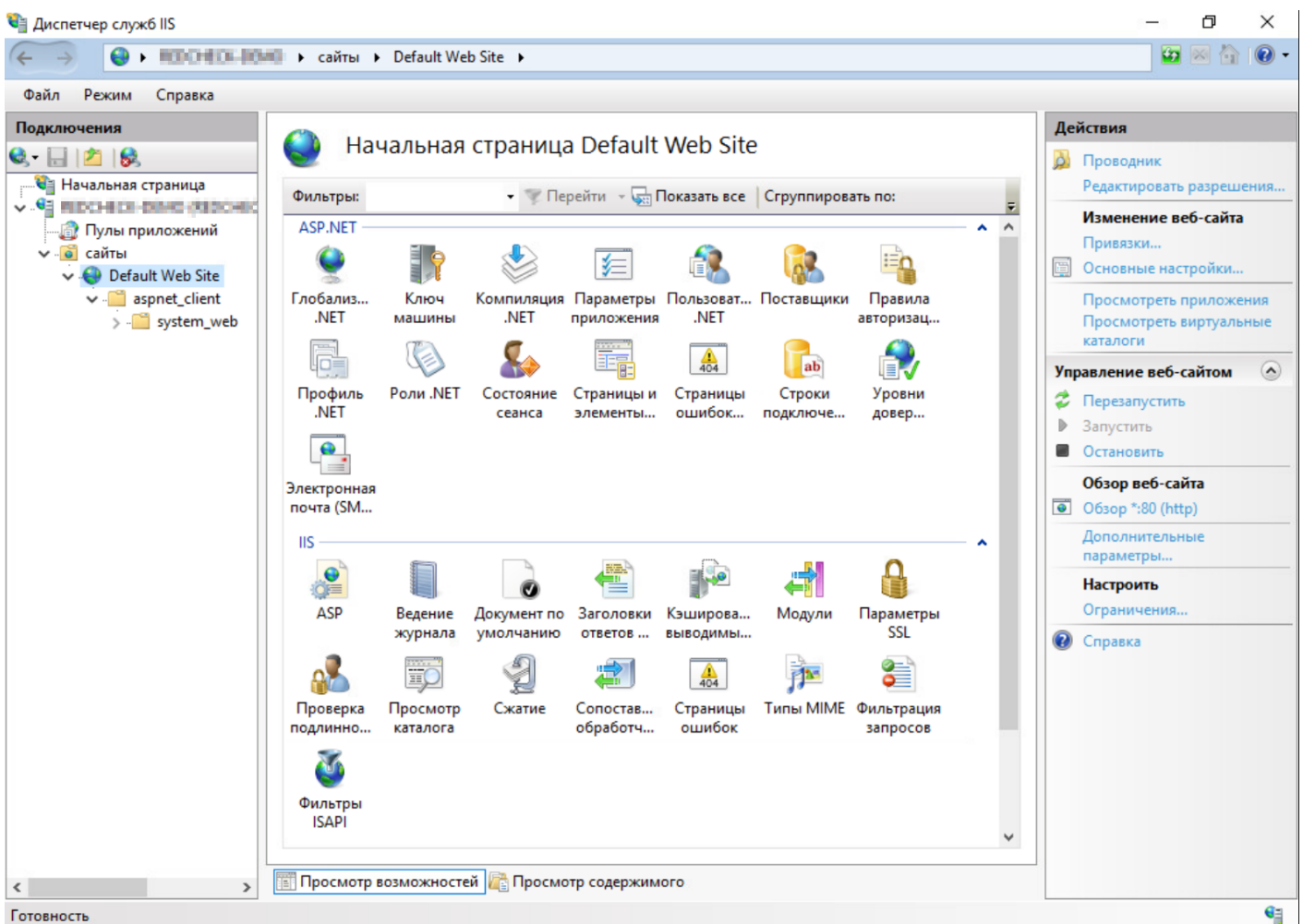


IIS

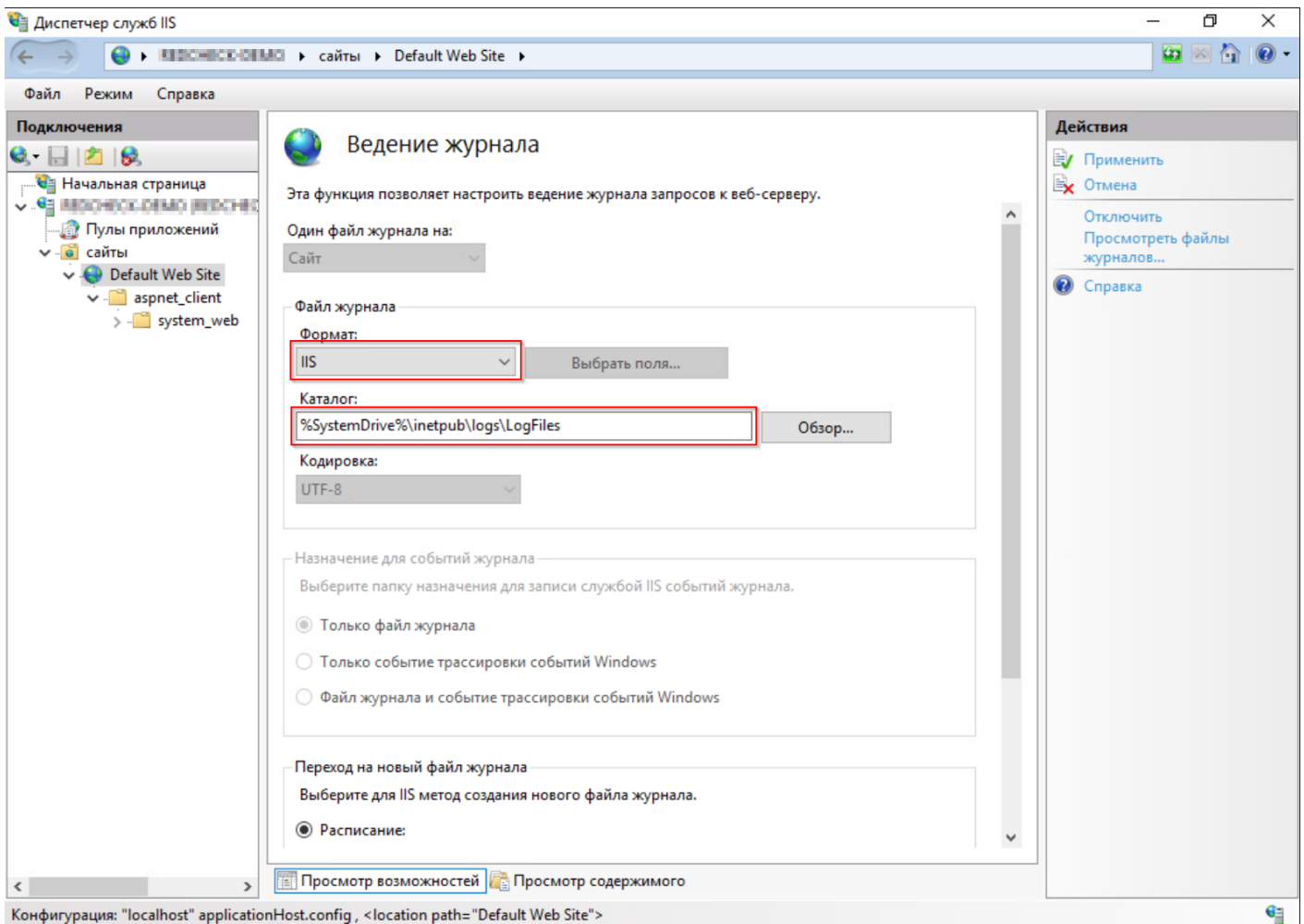
Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Настройка IIS сервера

1. Откройте диспетчер служб IIS и перейдите в настройки требуемого сайта



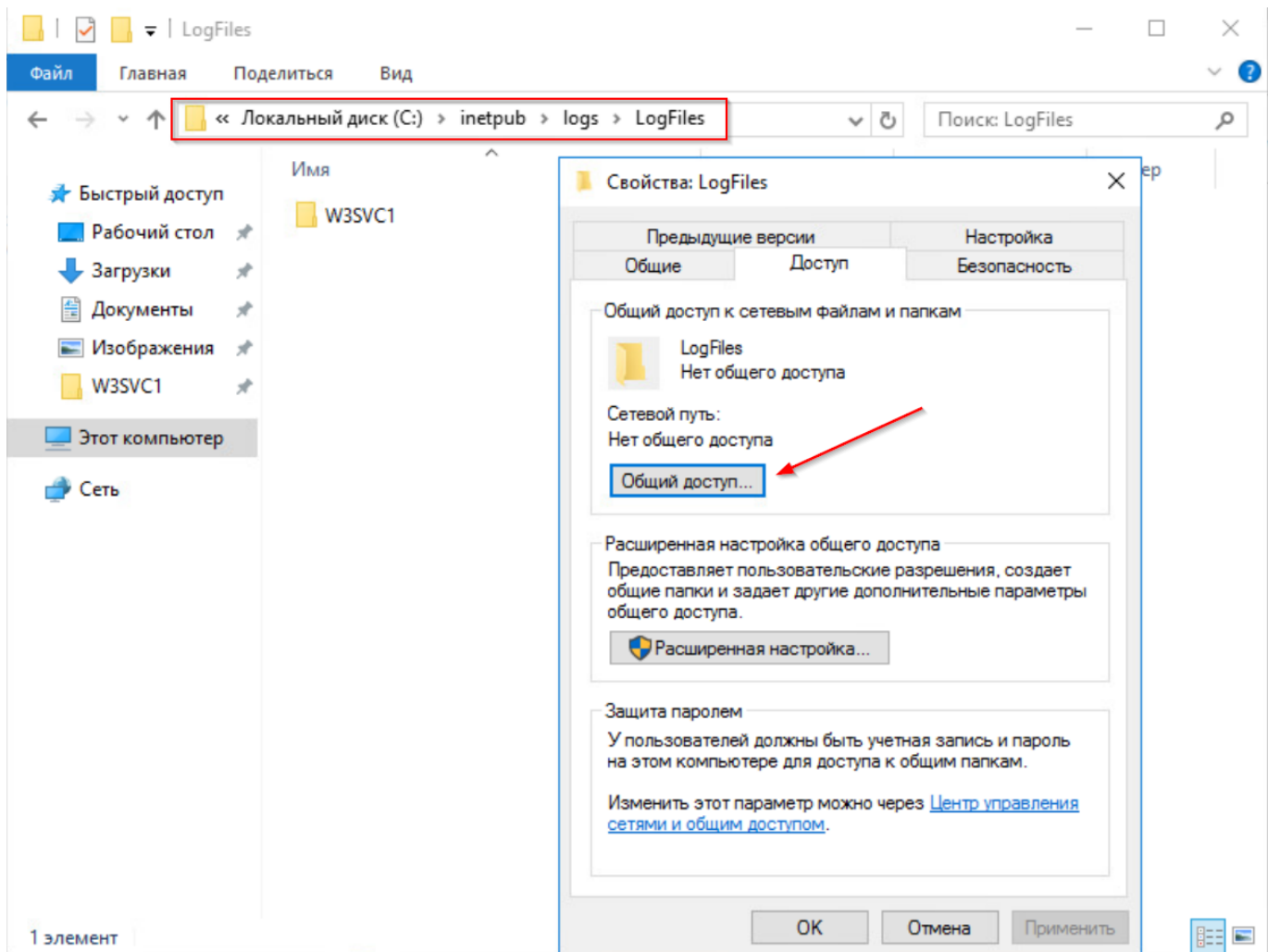
2. В разделе IIS выберите "Ведение журнала". Задайте формат журнала "IIS" и укажите папку для хранения логов. После выполнения настроек в окне "Действия" нажмите применить.

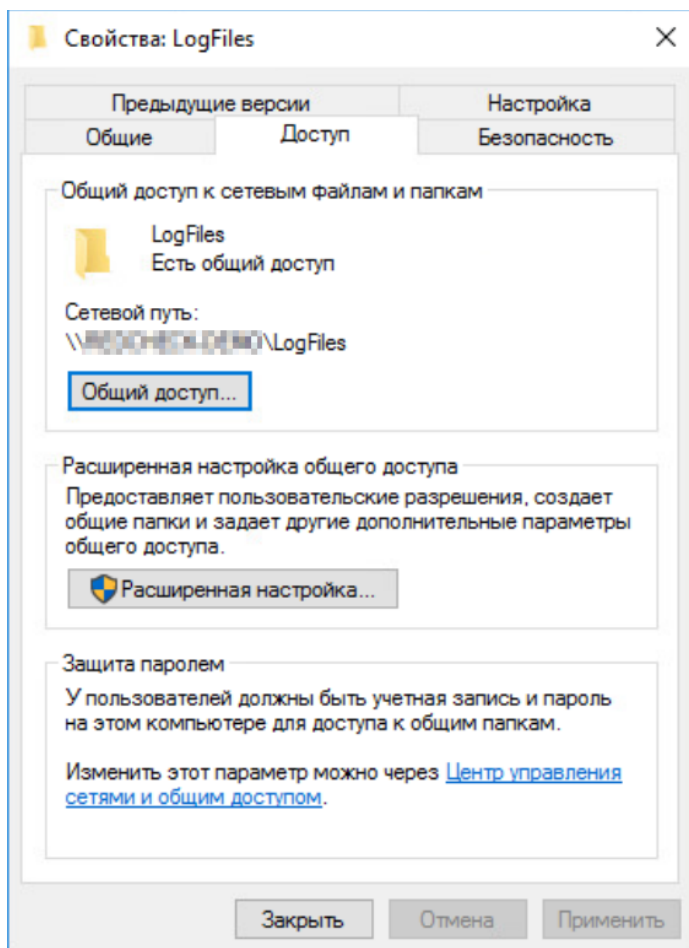


Формат логов должен быть именно **IIS** для возможности использования коробочного нормализатора

Подробнее про данный формат логов: <https://learn.microsoft.com/en-us/windows/win32/http/iis-logging>

3. По умолчанию лог IIS будет записан в папку `C:\inetpub\logs\LogFiles`. Для данной папки необходимо включить общий доступ на чтение.





Монтирование папки в KUMA

Для чтения файла логов коллектором KUMA необходимо примонтировать папку содержащую логи IIS сервера на сервер коллектора KUMA.

1. Для начала необходимо установить утилиту **cifs**, если она еще не установлена.

```
yum install -y cifs-utils
```

2. Далее необходимо создать файл с учетными данными пользователя для доступа к общей папке **/root/.iis-secret** со следующим содержимым:

```
username=<имя пользователя с правами на чтение папки>
password=<пароль пользователя>
domain=<домен, в случае доменного пользователя>
```

3. Далее нужно создать папку на сервере коллектора KUMA, куда будет примонтирована папка с логами DNS сервера.

```
mkdir /mnt/iis
```

4. Далее в конец файла `/etc/fstab` необходимо добавить строку

```
\\<путь к общей папке сервера> <путь монтирования> cifs credentials=<файл с учетными данными>,cache=none 0 0
```

Пример:

```
\\iis.demo.lab\dhcp /mnt/iis cifs credentials=/root/.iis-secret,cache=none 0 0
```

5. Далее необходимо примонтировать общую папку командой:

```
mount -a
```

Для проверки успешности монтирования можно выполнить следующую команду:

```
ls /mnt/iis
```

6. Убедитесь, что у пользователя kuma есть права на чтение файлов логов из данной директории, а также возможность просматривать директории по пути к логам.

Альтернативно, можно назначить пользователя kuma владельцем примонтированной папки:

```
chown -R kuma:kuma /mnt/iis
```

Создание коллектора KUMA

Для создания коллектора KUMA необходимо в веб-консоли KUMA перейти на вкладку **Ресурсы - Коллекторы** и нажать на кнопку **Добавить коллектор**. Также можно на вкладке **Ресурсы** выбрать пункт **Подключить источник**. В обоих случаях откроется мастер подключения источников событий.

На первом шаге мастера необходимо выбрать **Тенант**, которому будет принадлежать коллектор и также задать **Имя коллектора**.

Подключение источников событий

Коллекторы используются для получения данных из источников событий, а также преобразования их в нормализованные события, понятные KUMA. С помощью коллектора можно также отсеивать ненужные события, объединять похожие события и обогащать события информацией из сторонних источников. Чтобы создать коллектор, следуйте шагам мастера. Подробнее см. [в онлайн-справке](#).

*Название коллектора	<input type="text" value="IIS file log"/>
*Тенант	<div>Main ▾</div>
Рабочие процессы	<input type="text" value="0"/>
Отладка	<div>Выключить ▾</div>
Описание	<div>Описание <div></div></div>

На втором шаге мастера необходимо выбрать тип подключения **file** и указать **маску пути** для файлов логов IIS сервера.

Транспорт

Подключите источник, от которого хотите получать события. Подробнее см. [в онлайн-справке](#).

Основные параметры	Дополнительные параметры
<hr/>	
*Коннектор	<div>Создать ▾</div> ⓘ
*Тип	<div>file ▾</div> ⓘ
URL	<div>/mnt/iis/W3SVC1/u_in.log</div> ⓘ

На третьем шаге мастера необходимо выбрать предустановленный нормализатор **[OOTB] IIS Log File Format**. В случае отсутствия указанного нормализатора, обратитесь к своему менеджеру для его получения.

Схема нормализации

Обогащение

*Нормализатор

[OOTB] IIS Log File Format

▼

🔗

☐ Сохранить нормализатор

*Название

[OOTB] IIS Log File Format

Шаги мастера с четвертого по шестой можно пропустить, либо заполнить позднее по своему усмотрению.

На седьмом шаге мастера необходимо указать точки назначения типа **Хранилище**, если требуется сохранение событий в БД и типа **Коррелятор**, если требуется корреляция событий.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Routing

Specify where processed events should be routed to. It is recommended to send events to at least two destinations: to a correlator for analysis and to a storage for retention. For details see [Online Help](#).

Storages		
[Example] Storage	storage	test-kuma.sales.lab:7230

Correlators		
[Example] Correlator	correlator	test-kuma.sales.lab:7249

Add destination ▼

На последнем шаге мастера необходимо нажать на кнопку **Сохранить и создать сервис**, после чего скопировать появившуюся команду для дальнейшей установки сервиса коллектора.

1 Connect event sources

2 Transport

3 Event parsing

4 Event filtering

5 Event aggregation

6 Event enrichment

7 Routing

8 Setup validation

Setup validation

Configuring collector is complete and service is created in KUMA. For details see [Online Help](#).

To start receiving events, you must install this service on the server, dedicated for the collector (see example of the install command below). Make sure network access and ports were properly configured. For details see [Online Help](#).

Services using this collector

Kind	Name
collector	MS DHCP Collector

Save and restart services

Save and reload services

Recommended command for collector installation

```
/opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 38e95e63-9691-4b88-a16e-c2198e093fbc --api.port 7288 --install
```

📋 Copy

В результате на вкладке **Ресурсы - Активные сервисы** появится созданный сервис коллектора.

Установка коллектора KUMA

Для установки сервиса коллектора необходимо подключиться к консоли сервера коллектора KUMA.

Для установки сервиса коллектора необходимо выполнить скопированную команду.

```
[root@test-kuma ~]# /opt/kaspersky/kuma/kuma collector --core https://test-kuma.sales.lab:7210 --id 38e95e63-9691-4b88-a16e-c2198e093fbc --api.port 7288 --install
Created symlink /etc/systemd/system/multi-user.target.wants/kuma-collector-38e95e63-9691-4b88-a16e-c2198e093fbc.service → /usr/lib/systemd/system/kuma-collector-38e95e63-9691-4b88-a16e-c2198e093fbc.service.
[root@test-kuma ~]#
```

В результате статус коллектора в веб-интерфейсе KUMA изменится на **зеленый**.

Для поиска событий IIS можно использовать следующий запрос

```
SELECT * FROM `events` WHERE DeviceProduct = 'IIS' ORDER BY Timestamp DESC LIMIT 250
```

Revision #3

Created 16 November 2023 08:03:01 by Koala

Updated 7 July 2024 08:50:24 by Koala