

Создание и подключение облачных S3-хранилищ к PT Sandbox

Оглавление

Введение.....	3
Yandex.Cloud Object Storage.....	3
VK Cloud Storage	6
Cloud.ru Evolution S3.....	8
Диагностика подключения к S3-хранилищу	12
Ссылки на актуальную справочную информацию	13

Введение

S3 - Simple Storage Service — это решение, предназначенное для хранения и управления большими объемами данных. Оно обеспечивает высокую доступность, масштабируемость и безопасность, позволяя пользователям загружать, скачивать и организовывать файлы через веб-интерфейс или API. Принцип работы прост: создаётся бакет — это «контейнер» для хранения файлов (объектов), каждый с уникальным именем. В бакеты загружаются файлы любого типа, доступ к которым настраивается с помощью списков управления доступом (S3 ACL). S3 используется для различных задач, включая резервное копирование, архивирование данных и хранение статического контента для веб-приложений.

В PT Sandbox 5.24 появился функционал, позволяющий проверять S3 источники **только в неблокирующем режиме (режиме мониторинга)** и сигнализировать о нахождении файлов с вредоносным содержанием. Данная инструкция содержит описание действий по созданию бакетов в облаках Yandex.Cloud, VK Cloud и Cloud.ru Evolution и настройке задач для сканирования в песочнице. Также представлены шаги для диагностики проблем с подключением с использованием утилит curl и AWS CLI.

Yandex.Cloud Object Storage

Для создания бакета и настройки прав доступа на стороне облачного провайдера требуется открыть панель управления Yandex.Cloud и перейти в сервис Object Storage, в котором требуется нажать кнопку "Создать бакет" в правом верхнем углу. На отобразившейся странице требуется задать имя и прочие параметры, необходимые для работы:

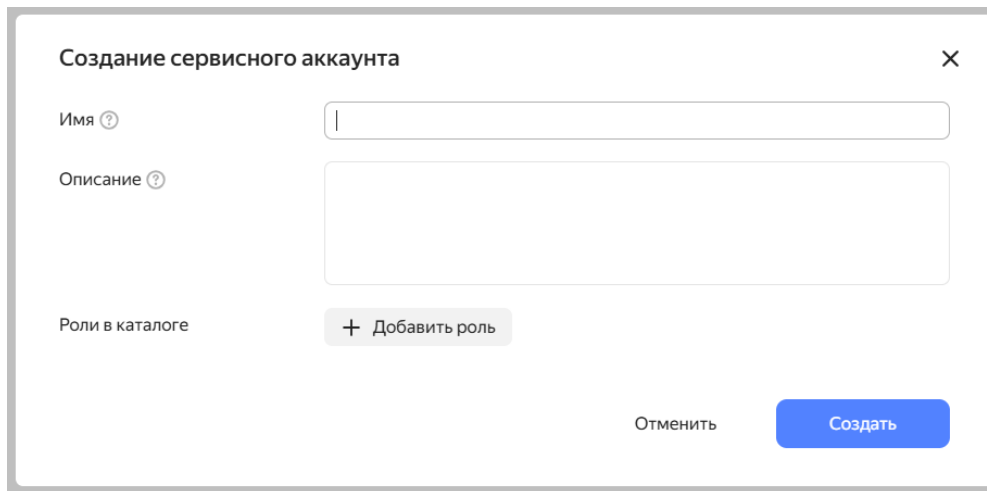
The screenshot shows the 'Новый бакет' (New Bucket) configuration page in the Yandex.Cloud Object Storage console. The breadcrumb navigation at the top reads: 'cloud-sec DE default Object Storage / Бакеты / Новый бакет'. The page is divided into several sections:

- Новый бакет**: Contains a text input for 'Имя*' (Name) and a button 'Добавить метку' (Add tag).
- Основные настройки**: Contains several configuration options:
 - 'Макс. размер' (Max size): A text input with '50' and a dropdown menu with 'ГБ' (GB).
 - 'Доступ на чтение объектов' (Object read access): Radio buttons for 'Ограниченный' (Limited) and 'Публичный' (Public).
 - 'Доступ к списку объектов' (Object list access): Radio buttons for 'Ограниченный' (Limited) and 'Публичный' (Public).
 - 'Доступ на чтение настроек' (Configuration read access): Radio buttons for 'Ограниченный' (Limited) and 'Публичный' (Public).
 - 'Класс хранилища' (Storage class): Radio buttons for 'Стандартное' (Standard), 'Холодное' (Cold), and 'Ледяное' (Ice).
- Шифрование**: Contains a 'Ключ KMS' (KMS key) section with a 'Создать ключ' (Create key) button and a warning icon with the text 'В каталоге ещё нет ключей.' (There are no keys in the catalog yet).

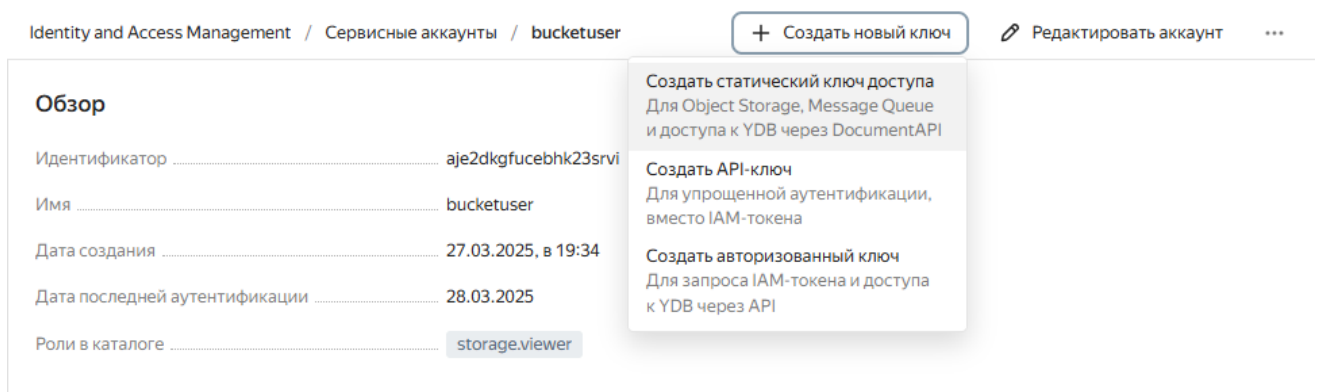
At the bottom of the form is a large blue button labeled 'Создать бакет' (Create bucket).

Далее требуется создать Сервисный аккаунт для предоставления доступа к бакету по паре Access key и Secret access key. Для этого перейдите в раздел Identity and Access Management, выберите

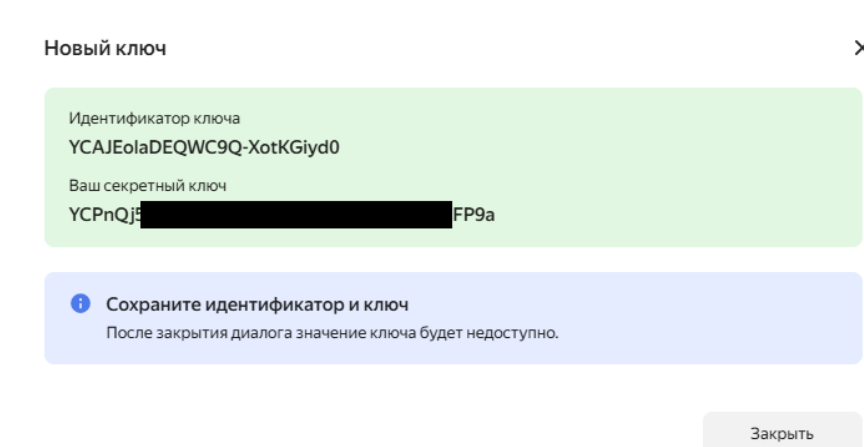
раздел Сервисные аккаунты и нажмите кнопку "Создать сервисный аккаунт" в правом верхнем углу. В появившемся диалоговом окне задайте имя, описание, а также задайте требуемую роль для сервисного аккаунта (минимально необходимая - storage.viewer, подробнее о ролях Вы можете ознакомиться в документации - <https://yandex.cloud/docs/storage/security/#storage-viewer>):



После создания в сервисном аккаунте нажмите кнопку "Создать новый ключ" и выберите "Создать статический ключ доступа":



В появившемся окне введите описание ключа и нажмите "Создать". Далее отобразится пара ключей, необходимых для доступа к бакету:



Будьте внимательны! Секретный ключ отображается только 1 раз, и при его потере потребуются пересоздать ключевую пару.

На стороне PT Sandbox:

Требуется перейти во вкладку Источники, выбрать создание нового источника и указать имя источника и его тип "Общая папка" со следующими настройками:

Доменное имя или IP-адрес узла с папкой - S3 - storage.yandexcloud.net : 443

Использовать SSL - чекбокс установлен

Проверять подлинность SSL-сертификата - чекбокс установлен

Регион - ru-central1

Логин - полученный при создании ключевой пары access key

Пароль - полученный при создании ключевой пары secret key

Путь к папке - имя Вашего бакета.

Параметры доступа к общей папке

PT Sandbox проверяет файлы в общей папке. Настройте для PT Sandbox доступ на чтение файлов в этой папке.

Доменное имя или IP-адрес узла с папкой

:

Если используется стандартный порт, оставьте поле порта пустым

☒ Использовать SSL

☒ Проверять подлинность SSL-сертификата

Регион

Логин

Пароль

Путь к папке

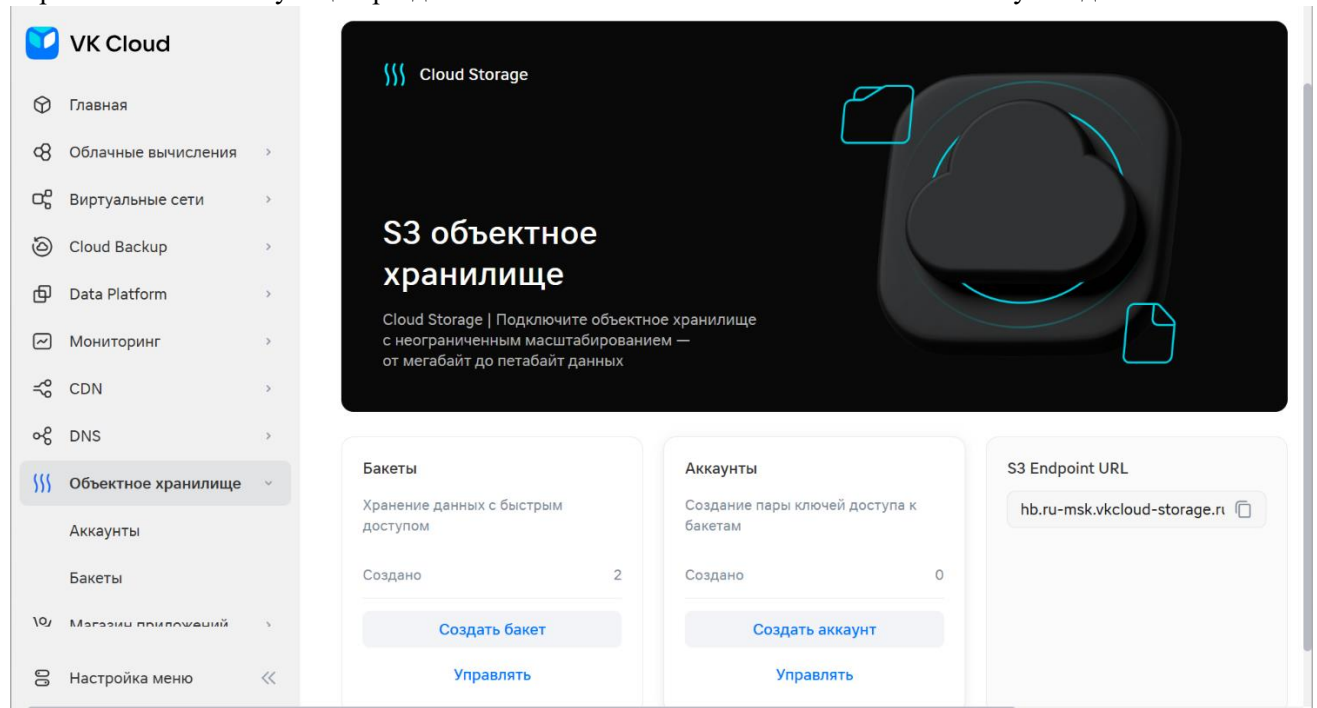
Используйте косую черту (/) в качестве разделителя каталогов в пути к общей папке

Также предлагается задать Параметры проверки, и при необходимости активировать пользовательские правила, поведенческий анализ и прочие опции.

После сохранения и включения источника во вкладке Задания должны появиться файлы из бакета, отправленные на анализ в соответствии с настройками источника.

VK Cloud Storage

Для создания бакета и настройки прав доступа на стороне облачного провайдера требуется перейти в соответствующий раздел личного кабинета VK Cloud и нажать кнопку Создать бакет:



На отобразившейся странице требуется задать имя бакета и определить тип хранилища:

VK Cloud > Cloud Storage > Бакеты > Создание бакета

Создание бакета

Название бакета ⓘ

sand

S3 Bucket URL

https://sand.hb.ru-msk.vkcloud-storage.ru

Класс хранения по умолчанию ⓘ



Hotbox

Быстрая раздача большого количества файлов для высоконагруженных сайтов и приложений



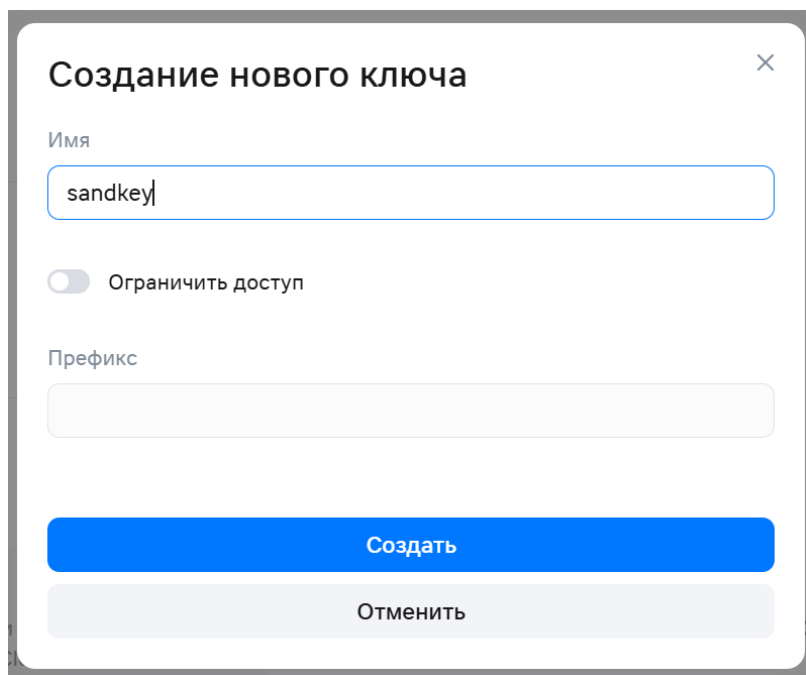
Icebox

Холодное хранение бэкапов, логов, медиаконтента, архивов и других редкоиспользуемых данных

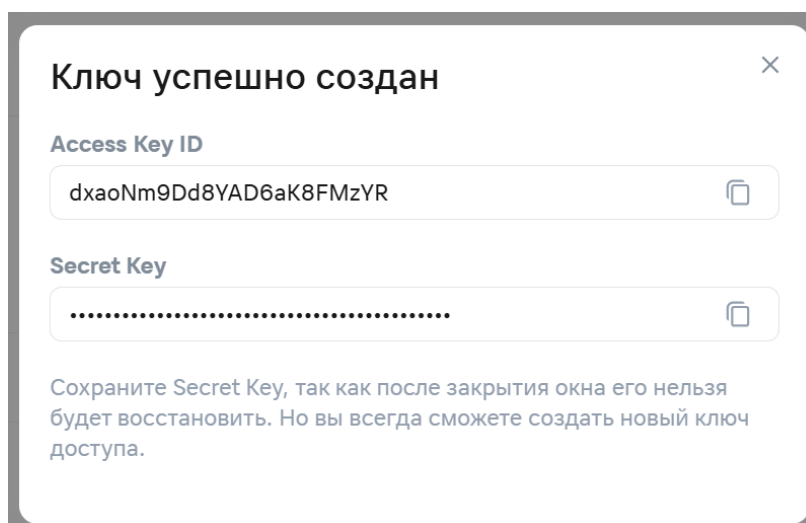
☐ Включить Object lock ⓘ

Включение блокировок не устанавливает блокировки на уже загруженные объекты, а только позволяет устанавливать их.

После создания бакета требуется создать ключи для доступа. Для этого откройте вкладку Ключи в бакете и нажмите Добавить ключ:



После создания отобразится диалоговое окно, содержащее ключевую информацию:



Будьте внимательны! Секретный ключ отображается только 1 раз, и при его потере потребуется пересоздать ключевую пару.

Настройки на стороне PT Sandbox:

Требуется перейти во вкладку Источники, выбрать создание нового источника и указать имя источника и его тип "Общая папка" со следующими настройками:

Доменное имя или IP-адрес узла с папкой - S3 - hb.ru-msk.vkcloud-storage.ru : 443

Использовать SSL - чекбокс установлен

Проверять подлинность SSL-сертификата - чекбокс установлен

Регион - ru-msk

Логин - полученный при создании ключевой пары access key

Пароль - полученный при создании ключевой пары secret key

Путь к папке - имя Вашего бакета.

Параметры доступа к общей папке

PT Sandbox проверяет файлы в общей папке. Настройте для PT Sandbox доступ на чтение файлов в этой папке.

Доменное имя или IP-адрес узла с папкой

S3

hb.ru-msk.vkcloud-storage.ru

 :

443

Если используется стандартный порт, оставьте поле порта пустым

- ☒ Использовать SSL
- ☒ Проверять подлинность SSL-сертификата

Регион

ru-msk

Логин

dxaoNm9Dd8YAD6aK8FMzVR

Пароль

Изменить

Путь к папке

sand/

Используйте косую черту (/) в качестве разделителя каталогов в пути к общей папке

Также предлагается задать Параметры проверки, и при необходимости активировать пользовательские правила, поведенческий анализ и прочие опции.

После сохранения и включения источника во вкладке Задания должны появиться файлы из бакета, отправленные на анализ в соответствии с настройками источника.

Cloud.ru Evolution S3

Для создания бакета и настройки прав доступа на стороне облачного провайдера требуется перейти в соответствующий раздел личного кабинета Cloud.ru и выбрать Создать бакет:

Создание бакета

Общие параметры

Название ?

bucket-2958d9

×

Глобальное название ?

Доменное имя ?

Полное доменное имя: не задано

Настройки

Класс хранения по умолчанию ?

Стандартный

▼

Для хранения данных во всех зонах доступности, выберите «Стандартный», «Холодный» или «Ледяной» класс хранения

Максимальный размер



Размер бакета будет ограничен заданным значением

100

×

ГБ

▼

Логирование ?



Отмена

Создать

При необходимости - скорректировать имя, размер выделяемого пространства, класс хранения и иные параметры. После создания потребуется записать ID тенанта, регион и Endpoint URL, перейдя во вкладку Object Storage API в созданном бакете:

Новый Проект

Эволюция / Object Storage / bucket-aa7543

83,15 Р

?

9+

AM

Назад к «Object Storage»

Файловый менеджер

Мультикомпонентная загрузка

О бакете

Настройка хостинга сайта

Настройка Bucket Policy

Object Storage API

Мониторинг

bucket-aa7543

Для работы с API

Endpoint ?

https://s3.cloud.ru/bucket-aa7543

ID тенанта

f7e52644-47ea-4b95-9b19-ec3106a5b616

Регион ?

ru-central-1

Название сервиса ?

s3

Для получения ключей доступа требуется перейти в раздел Пользователи, выбрать Сервисные аккаунты в панели слева и нажать кнопку "Создать сервисный аккаунт":

Пользователи	Сервисные аккаунты				
Локальные пользователи	1				
Федеративные пользователи	0				
Приглашённые пользователи	0				
Сервисные аккаунты	5				

Название	Статус	Роль на проект	Создан	Описание	
Logging-sa	Активен	Администратор проекта	24.04.2025	auto-generated servi...	***
s3-service-acc	Активен	Пользователь проекта	31.03.2025	s3 service account	***
Secret_Management-sa	Активен	Администратор проекта	29.03.2025	auto-generated servi...	***
Evolution_Managed_...	Активен	Администратор проекта	29.03.2025	auto-generated servi...	***
Evolution_Container_...	Активен	Администратор проекта	29.03.2025	auto-generated servi...	***

На отобразившейся странице требуется ввести название сервисного аккаунта, его описание и выбрать требуемые роли и доступы. Для предоставления наименьших привилегий возможно указать роль viewer для определённых бакетов:

Платформа Evolution

Evolution Object Storage

Роли ?

Не выбрано

Установить отдельные роли на бакеты ?

Роли на бакет

Бакет

bucket-aa7543

Роли

s3e.viewer

Для получения ключей доступа после создания сервисного аккаунта требуется выбрать из списка пользователей требуемый сервисный аккаунт и выбрать раздел Ключи доступа и нажать кнопку Создать ключ:

Назад к сервисным аккаунтам

s3-service-acc

Ключи доступа

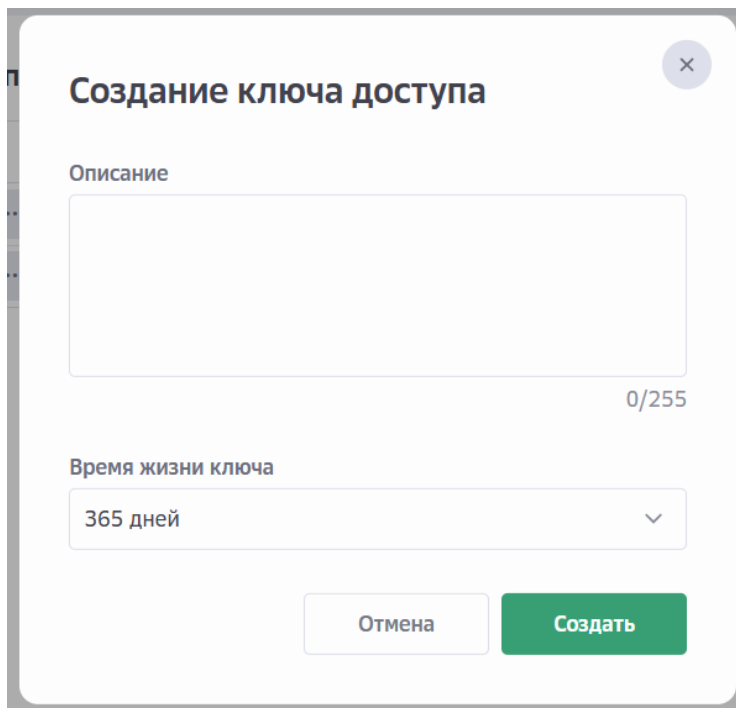
API-ключи

Создайте первый ключ доступа

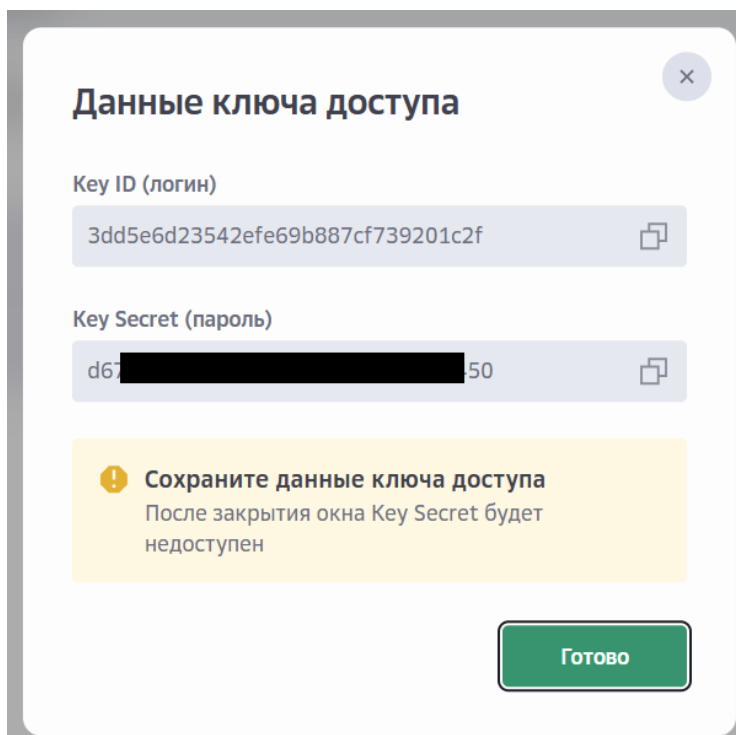
Секретный ключ доступа необходим для аутентификации сервисного аккаунта в API Cloud.ru

Подробнее в документации.

В диалоговом окне потребуется задать описание и время жизни ключа:



Далее отобразится окно с 32-значными ключами:



Будьте внимательны! Секретный ключ отображается только 1 раз, и при его потере потребуется пересоздать ключевую пару.

Особенность Cloud.ru Evolution - при формировании Access Key помимо полученного для сервисного аккаунта ключа требуется указать ID тенанта для бакета в формате tenantID:access_key, т.е. итоговая строка примет вид f7e52644-47**-****-***9-ec3106a5b616:e41f345e978a079f7ea10191d193861d

Настройки на стороне PT Sandbox:

Требуется перейти во вкладку Источники, выбрать создание нового источника и указать имя источника и его тип "Общая папка" со следующими настройками:

Доменное имя или IP-адрес узла с папкой - S3 - s3.cloud.ru : 443

Использовать SSL - чекбокс установлен

Проверять подлинность SSL-сертификата - чекбокс установлен

Регион - ru-central-1

Логин - ID тенанта бакета и полученный при создании ключевой пары access key, соединённые двоеточием. Пример:

Пароль - полученный при создании ключевой пары secret key

Путь к папке - имя Вашего бакета.



Общая папка

Параметры источника

Параметры проверки

Задания 0

Параметры доступа к общей папке

PT Sandbox проверяет файлы в общей папке. Настройте для PT Sandbox доступ на чтение файлов в этой папке.

Доменное имя или IP-адрес узла с папкой

S3

s3.cloud.ru

:

443

Если используется стандартный порт, оставьте поле порта пустым

☒ Использовать SSL

☒ Проверять подлинность SSL-сертификата

Регион

ru-central-1

Логин

f7e52644-47ea-4b95-9b19-ec3106a5b616:c7e...

Пароль

Изменить

Путь к папке

bucket-aa7543/

Используйте косую черту (/) в качестве разделителя каталогов в пути к общей папке

Также предлагается задать Параметры проверки, и при необходимости активировать пользовательские правила, поведенческий анализ и прочие опции.

После сохранения и включения источника во вкладке Задания должны появиться файлы из бакета, отправленные на анализ в соответствии с настройками источника.

Диагностика подключения к S3-хранилищу

В случае возникновения проблем с подключением источника предлагается проверить:

1) Сетевую доступность от PT Sandbox к endpoint S3 URL с применением утилиты curl:

```
$ curl https://checkme.hb.ru-msk.vkcloud-storage.ru/
```

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<Error><Code>AccessDenied</Code><RequestId>yns77CML2g</RequestId><Message>Access  
Denied</Message></Error>
```

Ответ сигнализирует о необходимости передачи авторизационной информации в заголовках запроса и подтверждает наличие сетевой доступности к S3 Endpoint URL по протоколу https.

2) Корректность пары ключ доступа - секретный ключ, наличия необходимых полномочий на чтение объектов в бакете и прочие вопросы доступа можно проверить с помощью любых инструментов для работы с S3. Мы рассмотрим подключение с применением AWS CLI

Для работы AWS CLI требуется установить его

(<https://docs.aws.amazon.com/cli/latest/userguide/getting-started-install.html>) и осуществить первоначальную настройку.

После его установки потребуется задать параметры Access key, Secret access key и Region в интерактивном режиме. В случае с Linux команда выглядит следующим образом:

```
$ /usr/local/bin/aws configure
```

Далее для проверки корректности доступа в Yandex Cloud и отображения содержимого бакета требуется запустить:

```
$ /usr/local/bin/aws --endpoint-url=https://storage.yandexcloud.net s3 ls --recursive s3://boxtest
```

[где boxtest - имя бакета]. И получить вывод:

```
2025-03-27 16:28:23 2932760 pt-sandbox-configuring-sources-custom-settings-ru-20250324.pdf
```

Для VK Cloud команда примет следующий вид:

```
$ /usr/local/bin/aws --endpoint-url=https://hb.ru-msk.vkcloud-storage.ru s3 ls --recursive s3://boxtest
```

[аналогично, где boxtest - имя бакета]

Для Cloud.ru Evolution требуется учитывать перечисленные выше особенности в работе с этим облаком и осуществить настройку утилиты:

```
$ /usr/local/bin/aws configure
```

```
AWS Access Key ID [*****1b71]: f7e52644-47**-****-***g-ec3106a5b616:e41f345e978a079f7ea10191d193861d
```

```
AWS Secret Access Key [*****8b9d]: 404985a9*****60def2
```

```
Default region name [us-east-1]: ru-central-1
```

```
Default output format [None]:
```

Далее можно подключиться к бакету с указанием следующей команды:

```
$ /usr/local/bin/aws --endpoint-url=https://s3.cloud.ru/ s3 ls --recursive s3://bucket-8c6bb7
```

и получить ответ вида:

```
2025-04-02 17:03:21 2932760 pt-sandbox-configuring-sources-custom-settings-ru-20250324.pdf
```

Ссылки на актуальную справочную информацию

Yandex.Cloud - <https://yandex.cloud/ru/docs/>

VK Cloud - <https://cloud.vk.com/docs>

Cloud.ru Evolution - <https://cloud.ru/docs/s3e/ug/index?source-platform=Evolution>

PT Sandbox - <https://help.ptsecurity.com/ru-RU/projects>

AWS CLI - <https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-getting-started.html>