КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.07

Защита больших массивов ресурсов

Редакция: 01.09.2026

Оглавление

Введение

В данном руководстве описан способ защиты очень большого количества ресурсов путём создания динамических групп, распределения ресурсов по этим группам и применения к группам планов защиты.

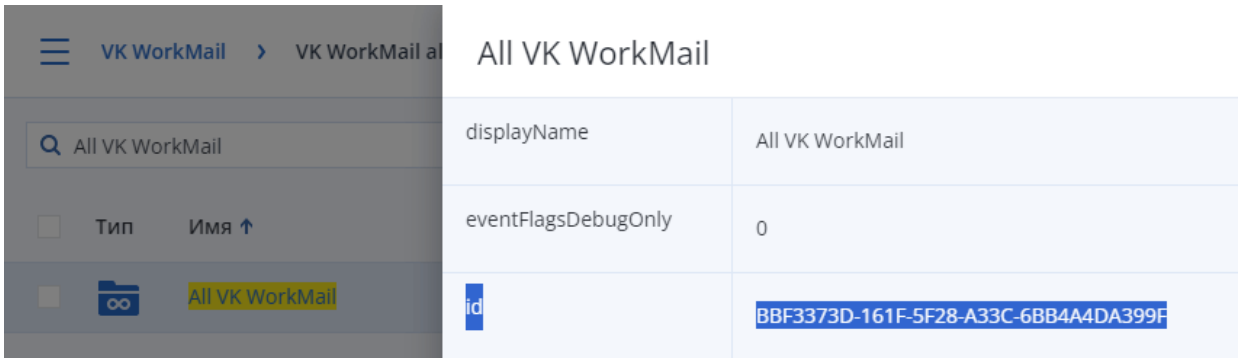
Все действия выполняются с помощью Python-скрипта `workloads-sharding.py`. Для его работы необходимы библиотека `requests`, а также учётная запись в Кибер Бэкапе Облачном. Запустить скрипт можно на любой машине с доступом к сервисам управления Кибер Бэкапа Облачного.

Распределение ресурсов по динамическим группам и их защита

1. Зарегистрируйте агентов для нужного типа устройств, настройте параметры поиска устройств и дождитесь, пока устройства появятся в веб-консоли.

   Найденные устройства будут помещены в автоматически созданную группу. Например, почтовые ящики VK WorkMail окажутся в группе домена VK WorkMail.

2. Определите идентификатор автоматически созданной группы устройств. На странице **Устройства** → **<Тип устройств>** щёлкните по значку группы устройств. В меню **Действия** щёлкните **Сведения** → **Все свойства**. Идентификатор будет приведён в поле **id**. Его понадобится указать в качестве аргумента в параметре скрипта `--master-group-id` (см. шаг 6).

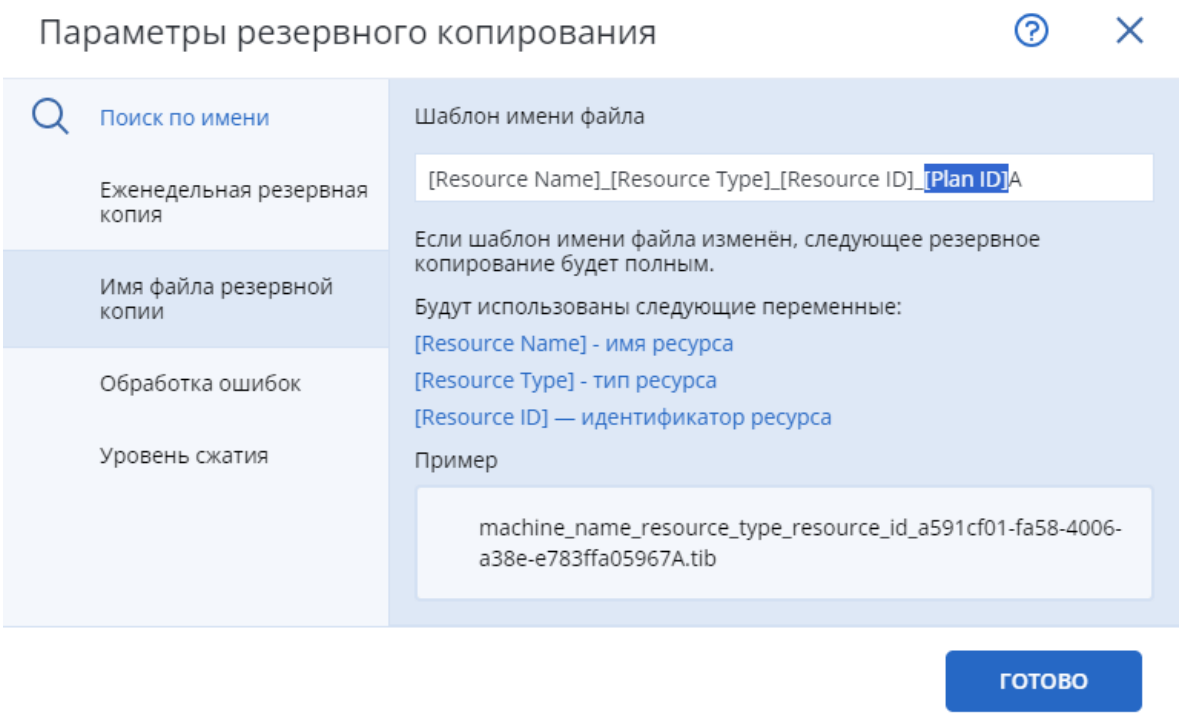
   

3. Создайте нужное число планов защиты в разделе **Планы** → **Защита**.

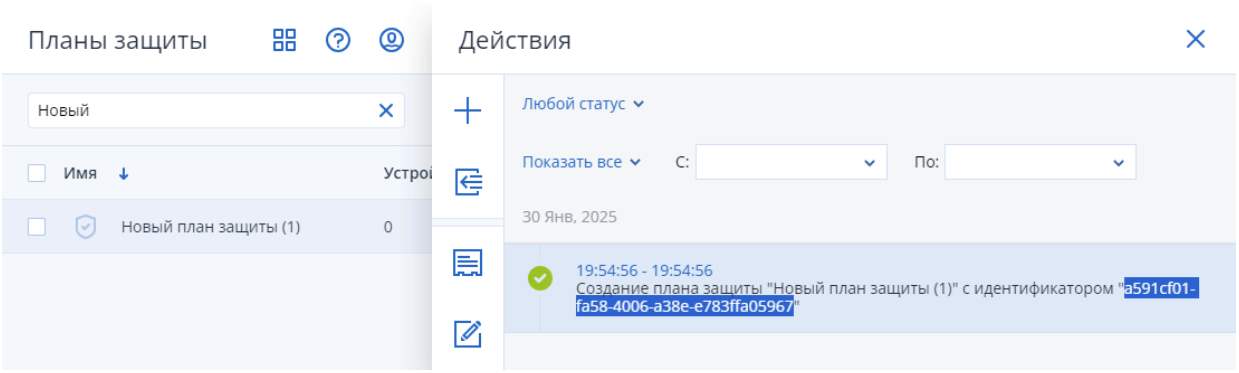
   В частности, для защиты ресурсов VK может понадобиться план для данных VK WorkMail и план для данных VK WorkDisk.

   Каждый план нужно создать следующим образом:

   - Не добавляя в него устройства.
   - В разделе **Параметры резервного копирования** на вкладке **Имя файла резервной копии** в поле **Шаблон имени файла** нужно заменить ”[Plan ID]” на уникальную константу, например, сгенерированный UUID.



4. Определите идентификатор каждого созданного плана. Для этого на панели **Действия** плана щёлкните **Действия**. Идентификатор будет приведён в действии ”Создание плана защиты...”.

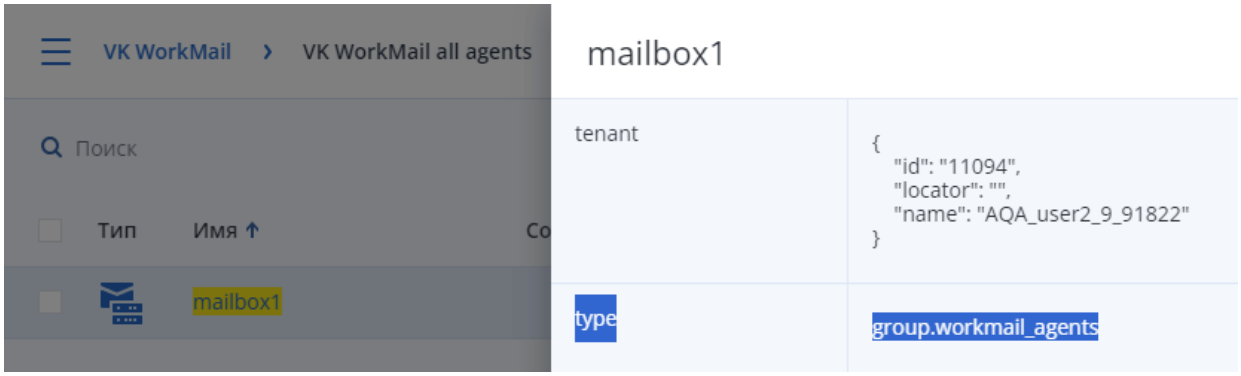


   Идентификаторы планов нужно будет указать через запятую в качестве аргумента параметра скрипта `--master-policy-ids` (см. шаг 6). Каждый из планов будет применен к указанной группе.

5. Определите тип динамических групп. Защищаемые устройства будут распределены по группам этого типа, и к ним будут применены клоны планов защиты из шага 3.

   Например, для почтового ящика VK WorkMail типом является `group.workmail_agents`. Для домена внутри почтового ящика типом является `group.workmail_domains`.

   Чтобы определить тип, на странице **Устройства** → **<Тип устройств>** щёлкните по значку группы устройств. В меню **Действия** щёлкните **Сведения** → **Все свойства**. Идентификатор будет приведён в поле **type**.



6. Запустите скрипт `workloads-sharding.py`:

```
python ./workloads-sharding.py --dc-url=<адрес_установки>
                               --login=<имя_пользователя>
                               --password=<пароль>
                               --master-group-id=<ID_группы>
                               --master-policy-ids=<ID_плана_1>,<ID_плана_2>,...
                               --target-group-type=<тип_групп>
                               [--recreate-target-groups=all]
```

В этом скрипте:

- `<адрес_установки>` — адрес установки сервисов управления Кибер Бэкапа Облачного.
- `<имя_пользователя>` — имя пользователя учётной записи Кибер Бэкапа Облачного.
- `<пароль>` — пароль учётной записи Кибер Бэкапа Облачного.
- `<ID_группы>` — идентификатор группы устройств, определённый на шаге 2.
- `<ID_плана_N>` — идентификаторы планов защиты, определённые на шаге 4.
- `<тип_групп>` — тип групп устройств, определённый на шаге 5.

Параметр `--recreate-target-groups=all` можно опустить. Аргумент `all` будет выбран по умолчанию.

Например:

```
python ./workloads-sharding.py --dc-url=”https://my.example.dc/” --login=”mylogin” --
↪password=”mypassword” --master-group-id=3E92A21B-9F36-3930-981E-2AA25ABA06B7 --master-
↪policy-ids=5537cf66-4152-4c0d-9168-d0d5652576b7,7a15462f-4af0-4414-a619-c6741413a243 --
↪target-group-type=”group.workmail_accounts” --recreate-target-groups=all
```

После запуска скрипта будет выполнено следующее:

1. Будут созданы динамические группы с именами в формате:

```
”<имя_группы_из_шага_2>-<порядковый_номер>: <условие_именования_устройств_группы>”
```

2. Защищаемые устройства будут распределены по динамическим группам примерно поровну.
3. Планы защиты, созданные на шаге 3, будут клонированы для каждой динамической группы и применены к ней.
4. Планы защиты будут развернуты для всех устройств на соответствующих агентах. Начнётся создание резервных копий по расписанию в планах.

При увеличении числа защищаемых устройств, они будут автоматически попадать в одну из динамических групп, созданных на шаге 2, согласно условиям именования устройств. Если количество устройств в группе превысит предел плана, будет создано оповещение типа **GroupThresholdExceeded**. Оно появится в веб-консоли и, если настроены уведомления по почте, будет разослано данным способом.

Если появилось оповещение **GroupThresholdExceeded**, перезапустите скрипт.

При перезапуске скрипта:

- Если повторно указать те же параметры, то ранее созданные динамические группы и клоны планов защиты будут автоматически удалены.
- Чтобы избавиться от динамических групп, в которых превышен предел количества устройств, задайте следующий параметр:

  ```
  --recreate-target-groups=over-limit
  ```

  Такие группы будут удалены, а устройства из них будут примерно поровну распределены в новые динамические группы так, чтобы предел не оказался превышен.

- Чтобы заново клонировать планы защиты, задайте следующий параметр:

  ```
  --recreate-target-groups=””
  ```

  Динамические группы при этом затронуты не будут.

Особенности и ограничения

- Если к динамической группе, созданной скриптом, вручную применить план защиты не из числа заданных в параметре `--master-policy-ids`, этот план защиты будет удалён при перезапуске скрипта.
- В именах клонов указаны идентификаторы исходных планов защиты. Если вручную изменить имя клона, он будет создан повторно при перезапуске скрипта с параметром `--recreate-target-groups=””`.
- В оповещениях и действиях будут указаны идентификаторы и имена клонов планов защиты. Они изменятся, если при перезапусках скрипта клоны будут созданы заново.