КИБЕРПРОТЕКТ

КИБЕР Бэкап

Версия 19.0



Руководство пользователя

Редакция: 06.11.2026

© ООО «Киберпротект», 2026

ООО «Киберпротект» является правообладателем данного документа.

Все права защищены.

Распространение измененных версий данного руководства, а также переработанных материалов, входящих в данное руководство, запрещено без явного разрешения владельца авторских прав.

ДОКУМЕНТ ПРЕДОСТАВЛЯЕТСЯ «КАК ЕСТЬ». ДОКУМЕНТ НЕ ПРЕДПОЛАГАЕТ ОБЯЗАТЕЛЬСТВ И/ИЛИ ГАРАНТИЙ ПРАВООБЛАДАТЕЛЯ ОТНОСИТЕЛЬНО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, НАСКОЛЬКО ТАКОЕ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ДОПУСКАЕТСЯ ЗАКОНОМ, ВКЛЮЧАЯ, СРЕДИ ПРОЧЕГО, ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ, УДОВЛЕТВОРИТЕЛЬНОГО КАЧЕСТВА, ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ.

Оглавление

Издания и лицензии Кибер Бэкап **1**

Пробная версия 2

Активация лицензии 2

Обновление идентификатора инсталляции 3

Деактивация лицензии 4

Лицензирование Кибер Бэкап 18.6 и предыдущих версий 5

Установка **6**

Компоненты 6

Сервер управления 6

Агенты 6

Узел хранения 10

Другие компоненты 10

Требования к программному обеспечению 11

Поддерживаемые веб-браузеры 12

Поддерживаемые операционные системы 12

Поддерживаемые платформы виртуализации 17

Поддерживаемые почтовые сервисы 21

Поддерживаемые СУБД 22

Поддерживаемые версии приложений Microsoft 24

Поддерживаемые приложения 24

Необходимые пакеты для ОС Linux 25

Совместимость с ОС Astra Linux SE 32

Совместимость с программами шифрования 34

Поддерживаемые интеграции со службами каталогов 36

Системные требования 36

Рекомендуемые конфигурации оборудования для сервера управления 38

Сервер управления на машине с ОС Linux или Windows, использующий СУБД SQLite 38

Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL . . 43

Сервер управления на машине с ОС Windows, использующий СУБД Microsoft SQL Server 49

Поддержка файловых систем 52

Настройки прокси-сервера 55

Развертывание Кибер Бэкап 58

Установка сервера управления . . . 59
Установка в ОС Windows . . . 59
Установка в Linux . . . 64
Настройка отказоустойчивого кластера . . . 70
Архитектура . . . 70
Развертывание и настройка . . . 72
Добавление машин через веб-интерфейс . . . 87
Добавление машины с ОС Windows . . . 88
Добавление машины с ОС Linux . . . 92
Добавление vCenter или хоста ESXi . . . 93
Установка агентов . . . 97
Установка агентов в ОС Windows вручную . . . 97
Установка агентов в ОС Linux вручную . . . 100
Установка агентов для ОС Linux из RPM-репозитория . . . 103
Ручная установка агента для VMware (виртуальное устройство) из шаблона OVF 112
Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация) . . . 117
Развертывание резервного копирования для Кибер Инфраструктуры . . . 122
Ручная установка агента для SpaceVM . . . 129
Ручная установка агента для ECP VeiL . . . 133
Установка агента для OpenStack . . . 137
Ручная установка агента для VK Cloud . . . 150
Установка агента для Basis DynamiX Enterprise . . . 157
Установка агента для OpenNebula . . . 166
Установка агента для Proxmox . . . 182
Установка агента для VMmanager . . . 187
Автоматическая установка или автоматическое удаление . . . 195
Автоматическая установка или автоматическое удаление в Windows . . . 195
Автоматическая установка или автоматическое удаление в Linux . . . 202
Развертывание агентов с использованием групповой политики . . . 207
Регистрация агента вручную . . . 209
Установка и настройка узла хранения . . . 212
Установка узла хранения . . . 212
Добавление управляемого хранилища . . . 216
Защита хранилища паролем . . . 218
Дедупликация . . . 218
Проверка наличия обновлений программного обеспечения . . . 222
Управление лицензиями . . . 222
Автоматическое обнаружение машин . . . 223

Автоматическое и ручное обнаружение . . . 226
Выбор компонентов для установки . . . 230
Управление обнаруженными машинами . . . 231
Устранение неисправностей при автоматическом обнаружении . . . 232
Обновление виртуальных устройств . . . 233
Обновление агентов . . . 234
Модернизация с предыдущих версий продукта . . . 237
Удаление продукта . . . 243
Веб-консоль Кибер Бэкап . . . 246
Настройка веб-браузера для выполнения встроенной проверки подлинности Windows . . . 248
Добавление консоли к списку веб-узлов локальной интрасети . . . 249
Добавление консоли к списку доверенных веб-узлов . . . 250
Настройки сертификата SSL . . . 253
Использование самозаверяющих сертификатов . . . 253
Использование сертификата, выданного доверенным центром сертификации . . . 255
Режимы отображения списка устройств . . . 256
План защиты и модули . . . 261
Создание плана защиты . . . 261
Разрешение конфликтов плана . . . 263
Операции с планами защиты . . . 265
Активная защита (Active Protection) . . . 280
Технические требования и ограничения службы Active Protection . . . 281
Активная защита (Active Protection) для Windows . . . 281
Активная защита (Active Protection) для Linux . . . 286
Группы устройств . . . 289
Операции со статическими группами . . . 290
Операции с динамическими группами . . . 295
Применение плана защиты к группе . . . 304
Переименование группы . . . 305
Удаление группы . . . 306
Резервное копирование . . . 307
Агент . . . 309
Типы резервных копий . . . 310
Формат TIBX . . . 310
Модуль резервного копирования: памятка . . . 311
Выбор данных для резервного копирования . . . 318
Выбор всей машины . . . 318

Выбор файлов и папок . . . 319
Выбор дисков и томов . . . 321
Что содержится в резервных копиях томов или дисков . . . 323
Выбор конфигурации ESXi . . . 324
Выбор места сохранения . . . 325
О разделе Зона безопасности . . . 331
О продуктах Кибер Инфраструктура и Кибер Хранилище . . . 334
Поддержка хранилищ, работающих в режиме ”Только для добавления” . . . 336
Расписание . . . 338
Планирование по событиям . . . 341
По событию в журнале событий Windows . . . 342
Условия запуска . . . 344
Пользователь неактивен . . . 345
Хост хранилища резервных копий доступен . . . 345
Пользователи завершили сеанс . . . 346
В интервале времени . . . 347
Сэкономить заряд батареи . . . 347
Не запускать при работе на лимитном подключении . . . 348
Не запускать при подключении к следующим сетям Wi-Fi . . . 349
Проверить IP-адрес устройства . . . 350
Правила хранения . . . 351
Защита паролем . . . 353
Преобразование в виртуальную машину . . . 353
Преобразование в виртуальную машину в плане защиты . . . 355
Как работает обычное преобразование в виртуальную машину . . . 357
Репликация . . . 358
Замечания по использованию узла хранения . . . 361
Запуск резервного копирования вручную . . . 362
Одновременное резервное копирование . . . 366
Ограничение общего количества планов для файлового и дискового резервного копирования . . . 369
Ограничение общего количества виртуальных машин . . . 369
Ограничение общего количества планов для почтовых ящиков и баз данных PostgreSQL 372
Резервное копирование виртуальных машин без использования локальной сети (LAN-free backup) 372
Резервное копирование без использования локальной сети (LAN-free backup) для oVirt . 373
Резервное копирование без использования локальной сети (LAN-free backup) для VMware 380
Резервное копирование без использования локальной сети посредством виртуального устройства для VMware . . . 380

Резервное копирование без использования локальной сети посредством Windows-агента для VMware . . . 388
Параметры резервного копирования . . . 392
Оповещения . . . 399
Консолидация резервных копий . . . 400
Имя файла резервной копии . . . 401
Формат резервной копии . . . 406
Проверка резервных копий . . . 408
Функция Changed Block Tracking (CBT) . . . 409
Способ резервного копирования кластера . . . 410
Уровень сжатия . . . 412
Многопоточность . . . 413
Уведомления по электронной почте . . . 414
Уведомления в MAX . . . 415
Обработка ошибок . . . 421
Быстрое инкрементное/дифференциальное резервное копирование . . . 423
Фильтры файлов . . . 423
Моментальные снимки резервных копий на уровне файлов . . . 425
Сокращение журнала Microsoft SQL Server . . . 426
Создание моментальных снимков LVM . . . 427
Точки подключения . . . 427
Многотомные моментальные снимки . . . 428
Производительность и окно резервного копирования . . . 429
Команды до и после процедуры . . . 433
Команда до резервного копирования . . . 433
Команда после резервного копирования . . . 435
Команды до и после захвата данных . . . 435
Команда до захвата данных . . . 436
Команда после захвата данных . . . 437
Моментальные снимки оборудования SAN . . . 438
Планирование . . . 439
Посекторное резервное копирование . . . 440
Деление . . . 440
Управление лентами . . . 441
Действие при сбое плана . . . 448
Условия запуска задания . . . 448
Служба теневого копирования томов (VSS) . . . 449
Служба теневого копирования томов (VSS) для виртуальных машин . . . 450

Еженедельное резервное копирование . . . 451
Журнал событий Windows . . . 451
Восстановление . . . 452
Восстановление: памятка . . . 452
Создание загрузочных носителей . . . 453
Восстановление машины . . . 454
Физическая машина . . . 454
Восстановление физической машины в виртуальную . . . 456
Виртуальная машина . . . 458
Восстановление дисков с помощью загрузочного носителя . . . 461
Использование компонента Универсальное восстановление (Universal Restore) . . . 462
Компонент Универсальное восстановление (Universal Restore) в Windows . . . 462
Компонент Универсальное восстановление (Universal Restore) в Linux . . . 464
Восстановление файлов . . . 465
Восстановление файлов с помощью веб-интерфейса . . . 465
Восстановление файлов с помощью загрузочного носителя . . . 468
Извлечение файлов из локальных резервных копий . . . 469
Требования . . . 469
Восстановление конфигурации ESXi . . . 469
Параметры восстановления . . . 471
Проверка резервных копий . . . 472
Режим загрузки . . . 473
Дата и время для файлов . . . 474
Обработка ошибок . . . 474
Исключения файлов . . . 476
Безопасность на уровне файлов . . . 476
Flashback . . . 476
Восстановление полного пути . . . 477
Точки подключения . . . 477
Производительность . . . 477
Команды до и после процедуры . . . 478
Команда, выполняемая перед восстановлением . . . 478
Команда после восстановления . . . 479
Управление лентами . . . 480
Изменение идентификатора безопасности . . . 480
Управление питанием BM . . . 480
Журнал событий Windows . . . 481
Включить после восстановления . . . 481

Операции с резервными копиями **482**
Подключение томов из резервной копии 482
Экспорт резервных копий 484
Удаление резервных копий 485
Обработка данных вне хоста (off-host) 486
Репликация резервных копий 487
Проверка резервных копий 489
Очистка от устаревших резервных копий 493
Преобразование резервных копий в виртуальные машины 494
Вкладка ”Планы” **497**
Вкладка ”Хранилища резервных копий” **499**
Загрузочный носитель **501**
Мастер создания загрузочных носителей 503
Загрузочные носители на основе Linux 503
Параметры ядра 508
Сценарии на загрузочных носителях 510
Сервер управления 517
Сетевые настройки 518
Сетевой порт 519
Драйверы для компонента Универсальное восстановление (Universal Restore) . . 519
Загрузочный носитель на основе WinPE 520
Подготовка WinPE 4.0 и более поздние версии 521
Добавление подключаемого модуля Киберпротект к WinPE 522
Подключение к машине, загружаемой с носителя 525
Регистрация носителя на сервере управления 526
Операции с загрузочным носителем 528
Резервное копирование 530
Восстановление 531
Управление дисками 532
Поддержка файловых систем 533
Основные меры предосторожности 533
Выбор операционной системы для управления дисками 533
Операции с дисками 534
Операции с томами 540
Ожидающие операции 547
Настройка устройств iSCSI 547
Диспетчер восстановления при загрузке (Startup Recovery Manager) 549

PXE-сервер Киберпротект . . . 551
Установка PXE-сервера . . . 551
Настройка машины на загрузку с PXE . . . 552
Работа в подсетях . . . 553
Защита приложений, сервисов, баз данных . . . 554
Защита приложений Microsoft . . . 554
Предварительные требования . . . 556
Резервное копирование баз данных Microsoft SQL Server и Microsoft Exchange Server . . . 558
Выбор баз данных Microsoft SQL Server . . . 558
Выбор данных Microsoft Exchange Server . . . 559
Защита группы Always On Availability Groups (AAG) . . . 561
Защита групп обеспечения доступности базы данных (DAG) . . . 563
Резервное копирование с поддержкой приложений . . . 566
Требуемые права пользователя . . . 567
Резервная копия почтового ящика . . . 567
Выбор почтовых ящиков сервера Exchange . . . 569
Требуемые права пользователя . . . 569
Восстановление баз данных Microsoft SQL Server . . . 569
Восстановление системных баз данных . . . 573
Подключение баз данных Microsoft SQL Server . . . 573
Восстановление баз данных Microsoft Exchange Server . . . 574
Подключение баз данных Microsoft Exchange Server . . . 577
Восстановление почтовых ящиков Exchange и элементов почтового ящика . . . 577
Восстановление почтовых ящиков . . . 579
Восстановление элементов почтовых ящиков . . . 581
Копирование библиотек Microsoft Exchange Server . . . 585
Изменение учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server . . . 585
Защита CommuniGate Pro . . . 586
Предварительные требования для защиты CommuniGate Pro . . . 587
Установка CommuniGate Pro . . . 593
Резервное копирование CommuniGate Pro . . . 597
Создание плана защиты для CommuniGate Pro . . . 597
Настройка плана защиты для CommuniGate Pro . . . 602
Резервное копирование данных CommuniGate Pro . . . 603
Резервное копирование больших объемов данных CommuniGate Pro . . . 606
Резервные копии CommuniGate Pro . . . 610
Восстановление CommuniGate Pro . . . 612

Удаление CommuniGate Pro . . . 618
Защита VK WorkMail и VK WorkDisk . . . 619
Установка VK WorkMail . . . 620
Резервное копирование VK WorkMail и VK WorkDisk . . . 627
Резервное копирование данных пользователей VK WorkMail . . . 627
Резервное копирование данных пользователей VK WorkDisk . . . 631
Резервное копирование больших объемов данных . . . 632
Резервное копирование серверов VK WorkMail и VK WorkDisk . . . 635
Особенности резервного копирования VK WorkMail и VK WorkDisk на ленты . . . 639
Восстановление VK WorkMail и VK WorkDisk . . . 640
Восстановление данных пользователей VK WorkMail . . . 640
Восстановление данных пользователей VK WorkDisk . . . 644
Просмотр писем VK WorkMail . . . 645
Скачивание файлов из архива VK WorkDisk . . . 646
Восстановление серверов VK WorkMail и VK WorkDisk . . . 647
Обновление токена VK WorkMail . . . 648
Защита Mailion . . . 649
Установка Mailion . . . 650
Резервное копирование данных Mailion . . . 655
Восстановление данных Mailion . . . 657
Защита RuPost . . . 660
Установка RuPost . . . 661
Резервное копирование данных RuPost . . . 664
Восстановление данных RuPost . . . 669
Защита Oracle Database . . . 673
Защита Oracle Database предыдущих версий . . . 674
Установка . . . 678
Резервное копирование базы данных Oracle . . . 682
Резервное копирование сервера . . . 685
Восстановление всего сервера . . . 685
Восстановление баз данных Oracle с использованием Oracle Explorer . . . 685
Восстановление данных Oracle с помощью сценариев . . . 687
Защита баз данных PostgreSQL . . . 690
Предварительная настройка PostgreSQL . . . 693
Установка и настройка агента для PostgreSQL . . . 696
Методы резервного копирования PostgreSQL . . . 699
Резервное копирование с использованием библиотеки libpgprobackup . . . 699
Резервное копирование с использованием функции создания сводок WAL . . . 701

Резервное копирование PostgreSQL . . . 702
Восстановление баз данных PostgreSQL . . . 705
Восстановление экземпляра PostgreSQL в виде файлов . . . 706
Подключение экземпляра PostgreSQL из архива . . . 707
Гранулярное восстановление баз данных PostgreSQL . . . 708
Ограничения . . . 711
Известные проблемы и их решения . . . 711
Защита данных MySQL и MariaDB . . . 713
Настройка резервного копирования с поддержкой приложений . . . 714
Восстановление данных из резервной копии с поддержкой приложений . . . 716
Восстановление всего сервера . . . 716
Восстановление экземпляров . . . 717
Восстановление баз данных . . . 717
Восстановление таблиц . . . 719
Защита баз данных РЕД База Данных . . . 720
Предварительная настройка базы данных . . . 721
Резервное копирование РЕД База Данных . . . 722
Восстановление базы данных . . . 724
Защита баз данных MongoDB . . . 724
Настройка резервного копирования баз данных MongoDB . . . 725
Восстановление данных MongoDB . . . 730
Защита Kubernetes . . . 731
Установка агента для Kubernetes . . . 732
Подготовка кластера Kubernetes . . . 733
Создание служебной учетной записи для агента Kubernetes . . . 734
Подготовка файла kubeconfig . . . 741
Добавление кластера Kubernetes . . . 743
Резервное копирование Kubernetes . . . 744
Восстановление Kubernetes . . . 752
Резервное копирование постоянных томов в хранилище Кибер Бэкап . . . 759
Защита SAP HANA . . . 763
Резервное копирование физических серверов . . . 764
Резервное копирование виртуальных серверов . . . 768
Восстановление всего сервера . . . 769
Восстановление базы данных с помощью SAP HANA Studio . . . 769
Восстановление из последней резервной копии . . . 769
Восстановление из определенной резервной копии . . . 775

Специальные операции с виртуальными машинами 779
Запуск виртуальной машины из резервной копии (мгновенное восстановление) 779
Запуск машины 780
Удаление машины 782
Финализация машины 782
Работа в VMware vSphere 783
Репликация виртуальных машин 783
Создание плана репликации 785
Тестирование реплики 786
Переход к реплике 787
Параметры репликации 789
Параметры возврата из реплики 789
Сохранение первоначальной реплики 790
Использование локально присоединенного хранилища 791
Привязка виртуальной машины 792
Поддержка миграции VM 795
Управление средами виртуализации 796
Просмотр статуса резервного копирования в клиенте vSphere 797
Агент для VMware: необходимые привилегии 798
Предельное количество виртуальных машин для резервного копирования 812
Одновременное восстановление 813
Использование моментальных снимков оборудования SAN 813
Настройка хранилища данных YADRO TATLIN.UNIFIED 815
Требования для хранилища данных NetApp SAN 820
Настройка Huawei OceanStor (Dorado) 822
Настройка машины с агентом для VMware (Windows) 829
Регистрация хранилища данных SAN на сервере управления 833
Настройка машины с агентом для oVirt 835
Резервное копирование кластеризованных машин Hyper-V 839
Миграция машины 840
Миграция Linux-машины с логическими томами (LVM) 842
Увеличение объёма ОЗУ виртуального устройства 843
Резервное копирование облачных виртуальных машин без доступа к гипервизору 844
Мониторинг, отчёты и аудит 845
Панель мониторинга ”Обзор” 845
Виджет ”Резервные копии” 846
Виджет ”Статус защиты” 846
Виджет ”Нет последних резервных копий” 847

Панель мониторинга ”Оповещения” . . . 848
Панель мониторинга ”Действия” . . . 850
Отчёты . . . 852
Журнал аудита . . . 862
Регистрируемые события . . . 866
Настройка внешнего мониторинга средствами Grafana . . . 875
Настройка Prometheus в качестве источника данных . . . 877
Настройка Grafana Loki в качестве источника данных . . . 882
Настройка системы мониторинга Grafana . . . 885
Внешний мониторинг средствами Zabbix . . . 888
Ленточные устройства . . . 893
Типы и свойства лент . . . 893
Поддержка резервного копирования на ленту . . . 896
Совместимость с RSM и программным обеспечением других поставщиков . . . 896
Поддерживаемое оборудование . . . 896
База данных управления лентами . . . 897
Параметры записи на ленты . . . 898
Связанные с лентой параметры резервного копирования . . . 900
Параллельные операции . . . 900
Ограничения . . . 901
Начало работы с ленточным устройством . . . 902
Резервное копирование машины на локально подключенное ленточное устройство . . . 902
Резервное копирование на ленточное устройство, подключенное к узлу хранения . . . 903
Восстановление с ленточного устройства из операционной системы . . . 905
Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства . . . 906
Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения . . . 908
Управление лентами . . . 909
Обнаружение ленточных устройств . . . 909
Пулы лент . . . 909
Операции с пулами . . . 910
Создание пула . . . 910
Изменение пула . . . 911
Удаление пула . . . 912
Операции с лентами . . . 912
Перемещение в другой слот . . . 912
Перемещение в другой пул . . . 913

Инвентаризация . . . 918
Повторное сканирование . . . 921
Переименование . . . 922
Стирание . . . 923
Извлечение . . . 924
Удаление . . . 924
Указание набора лент . . . 925
Ручная очистка ленточных приводов . . . 926

Настройки системы . . . 927

Уведомления по электронной почте . . . 927
Сервер электронной почты . . . 929
Настройка уведомлений в MAX . . . 930
Безопасность . . . 934
Обновления . . . 935
Параметры резервного копирования по умолчанию . . . 935
Настройка PAM-модуля . . . 936
Управление журналом аудита . . . 937
Отправка записей журнала аудита на Syslog-сервер . . . 937

Управление учетными записями пользователей и отделами организации . . . 940

Отделы и административные учетные записи . . . 940
Добавление административных учетных записей . . . 944
Создание отделов . . . 949

Диагностика неполадок . . . 950

Издания и лицензии Кибер Бэкап

Для Кибер Бэкап 19 доступны следующие типы лицензий:

- Кибер Бэкап для рабочей станции,
- Кибер Бэкап для физического сервера,
- Кибер Бэкап для платформы виртуализации,
- Кибер Бэкап для почтового ящика,
- Кибер Бэкап для СУБД PostgreSQL,
- Кибер Бэкап универсальная лицензия.

Кроме того, доступны следующие редакции:

- **Стандартная** редакция подходит для резервного копирования данных в ИТ-инфраструктурах небольшого размера, в которых резервные копии отправляются в целевые хранилища напрямую без использования узла хранения, не требуется глобальная дедупликация, не требуется дифференциация ролей администратора, не используются ленточные носители.
- **Расширенная** редакция предназначена для крупных ИТ-инфраструктур, где требуется защита физических серверов, рабочих станций, виртуальных машин и приложений. Включает централизованное управление, глобальную дедупликацию данных, поддержку ленточных носителей, позволяет создавать организационные единицы и добавлять администраторов для них, а также содержит другие расширенные функции.

Лицензии на рабочие станции, физические серверы и платформы виртуализации доступны в двух редакциях: **Стандартная** и **Расширенная**.

Лицензии на почтовые ящики, СУБД PostgreSQL и универсальная лицензия доступны только в одной редакции: **Расширенная**.

Для использования Кибер Бэкап в кластере хостов виртуализации VMware ESXi или MS Hyper-V необходимо для каждого хоста в кластере иметь лицензии одного типа (**Для платформы виртуализации** или **Универсальная лицензия**) и одной редакции (**Стандартная** или **Расширенная**). Смешивание лицензий разных типов или редакций не допускается. Подробнее см. в статье базы знаний Особенности лицензирования резервного копирования виртуальных машин.

Все лицензии являются бессрочными. Приобретаемые лицензии распространяются на основную версию продукта, а также на все прошлые и будущие минорные обновления основной версии. Более подробную информацию о лицензиях см. в статье Лицензирование.

Пробная версия

Перед покупкой лицензии можно воспользоваться пробной версией. Она позволит оценить все возможности продукта без ограничений в течение 30 дней.

Активация лицензии

Активация лицензии — это операция, необходимая для получения доступа к лицензируемым функциям Кибер Бэкап. Активация происходит с помощью идентификатора инсталляции, который генерируется Кибер Бэкап и устанавливает криптографическую связь между лицензионным ключом, облачным сервисом лицензирования и конкретным оборудованием сервера управления на стороне пользователя.

> **Важно**
>
> Активировать лицензии необходимо только после завершения настройки локального сервера управления и его сетевого окружения.

Существенные изменения конфигурации сервера управления могут привести к изменению идентификатора инсталляции. Это приведет к сбою проверки лицензии и может потребовать повторной активации всех лицензий (см. раздел *Обновление идентификатора инсталляции*).

Лицензию можно повторно активировать на новой инсталляции после её деактивации на старой (см. раздел *Деактивация лицензии*).

Чтобы активировать лицензию, выполните следующие действия:

1. В веб-консоли Кибер Бэкап:
    1. Перейдите в раздел **Настройки** → **Лицензии** и сгенерируйте идентификатор инсталляции в виде файла или строки:
        - Для получения идентификатора инсталляции в виде файла нажмите **Скачать**.
        - Для копирования идентификатора инсталляции в виде строки в буфер обмена нажмите **Идентификатор инсталляции**.
    2. Нажмите **Перейти в личный кабинет**.
2. В личном кабинете:
    1. Выберите **Инсталляции** и нажмите **Добавить инсталляцию**.
    2. В открывшемся окне **Добавление инсталляции** выполните одно из следующих действий:
        - Нажмите **Загрузить файл**, выберите файл идентификатора инсталляции и нажмите

Открыть.

- В поле **ID инсталляции** вставьте идентификатор инсталляции в виде строки из буфера обмена.

3. Нажмите **Добавить**.
4. Перейдите в раздел **Лицензии**, выберите соответствующий тип лицензии и нажмите **Просмотреть все**, затем **Активировать лицензии**.
5. В окне **Активация лицензий** выберите существующую инсталляцию или добавьте новую, как указано ранее. Нажмите **Продолжить**.
6. В следующем окне укажите количество лицензий, которые необходимо привязать к данной инсталляции. Если не нужно разделять лицензии между несколькими инсталляциями, можно указать все доступные лицензии.

   При необходимости можно указать комментарий и подтвердить скачивание лицензий сразу после активации. Скачанные лицензии понадобятся на дальнейших шагах.

   > **Важно**
   >
   > Все активированные лицензии будут доступны только для выбранной инсталляции до тех пор, пока не будут деактивированы.

3. В веб-консоли Кибер Бэкап:
   1. Перейдите в раздел **Настройки** → **Лицензии**.
   2. Выберите **Добавить** → **Лицензионный файл**.
   3. В открывшемся диалоге выберите файлы активированных лицензий, скачанные из личного кабинета.

В дальнейшем для управления лицензиями в веб-консоли Кибер Бэкап выберите **Настройки** → **Лицензии**.

Кроме того, можно управлять лицензиями для каждой отдельной машины. Для этого в веб-консоли Кибер Бэкап в разделе **Устройства** выберите нужную машину и нажмите **Сведения**, далее щелкните **Изменить** в пункте **Лицензия**.

Обновление идентификатора инсталляции

Идентификатор инсталляции зависит от нескольких неизменяемых аппаратных и программных параметров сервера управления. При изменении этих параметров идентификатор инсталляции может измениться.

Операции, влияющие на изменение идентификатора инсталляции:

- Если сервер управления установлен на физической машине:
  - замена оборудования, смена MAC/IP-адресов, обновление ОС;
  - полная переустановка Кибер Бэкап на ту же машину (с деинсталляцией);
  - восстановление дисков/разделов, в т. ч. системного диска, на новую машину;
  - восстановление из резервной копии физической машины в виртуальную.
- Если сервер управления установлен на виртуальной машине:
  - замена оборудования, смена MAC/IP-адресов, обновление ОС;
  - полная переустановка Кибер Бэкап на ту же машину (с деинсталляцией);
  - клонирование или перенос виртуальной машины;
  - восстановление виртуальной машины в новую.

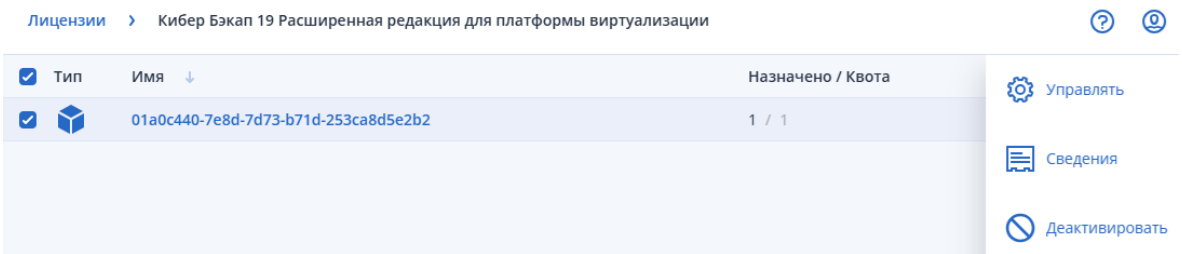
В случае появления ошибки необходимо выявить причину изменений системы и восстановить её оригинальное состояние. Если сделать это невозможно (например, было заменено вышедшее из строя оборудование), необходимо обратиться в службу технической поддержки для повторной активации лицензии с новым идентификатором.

Деактивация лицензии

Деактивация лицензии может понадобиться для её переноса на другой сервер управления, подготовки к обновлению лицензии или при выводе оборудования из эксплуатации.

Чтобы деактивировать лицензию, выполните следующие действия:

1. В веб-консоли Кибер Бэкап:
   1. Перейдите в раздел **Настройки** → **Лицензии**.
   2. В разделе **Активные** в строке с нужной активной лицензией нажмите **Управлять**.
   3. На следующем экране выберите необходимые лицензии и нажмите **Деактивировать**.



2. В окне **Деактивация лицензий** подтвердите деактивацию.

В результате Кибер Бэкап автоматически сгенерирует файл деактивации.

Повторно скачать файл деактивации можно в сведениях о деактивированной лицензии на вкладке **История**.

> **Важно**
>
> Без передачи файла деактивации в личный кабинет лицензии остаются закрепленными за инсталляцией, и их нельзя использовать в других операциях.

3. В личном кабинете пользователя Кибер Бэкап:
    1. Перейдите в раздел **Лицензии**.
    2. Нажмите **Деактивировать лицензии**.
    3. В окне **Деактивация лицензий** нажмите **Выбрать**, укажите файл деактивации и нажмите **Продолжить**.

В результате статус лицензии изменится на **Доступна для активации**. Деактивированную лицензию можно использовать для лицензирования на другом сервере управления.

Лицензирование Кибер Бэкап 18.6 и предыдущих версий

Виды и типы лицензий одинаковы для всех версий Кибер Бэкап (см. раздел *Издания и лицензии Кибер Бэкап*). Более подробную информацию о лицензиях см. в статье Лицензирование.

Лицензирование Кибер Бэкап 18.6 и предыдущих версий происходит с помощью лицензионных ключей.

Порядок активации лицензионного ключа

1. В веб-консоли Кибер Бэкап перейдите в раздел **Настройки** → **Лицензии**.
2. В разделе **У вас уже есть лицензия** нажмите **Добавить**.
3. В выпадающем списке выберите **Лицензионные ключи. Для Кибер Бэкап 18.6 и предыдущих версий**.
4. В окне **Добавить лицензионные ключи** вставьте лицензионный ключ и нажмите **Добавить**.

В дальнейшем для управления лицензиями в веб-консоли Кибер Бэкап выберите **Настройки** → **Лицензии**.

Кроме того, можно управлять лицензиями для каждой отдельной машины. Для этого в веб-консоли Кибер Бэкап в разделе **Устройства** выберите нужную машину и нажмите **Сведения**, далее щелкните **Изменить** в пункте **Лицензия**.

Установка

Компоненты

Кибер Бэкап состоит из сервера управления, агентов, а также различных вспомогательных компонентов. Все компоненты должны быть установлены в одной сети.

Сервер управления

Сервер управления является центральным компонентом. Он отвечает за обмен данными с агентами Кибер Бэкап, управляет планами защиты и предоставляет пользователям веб-интерфейс.

ПО сервера управления должно быть установлено на аппаратную платформу, оснащённую одной из поддерживаемых операционных систем (ОС) *Windows* или *Linux*. Установка сервера управления на машине с ОС Windows позволяет удалённо развёртывать агенты на других компьютерах. Информация о возможных конфигурациях аппаратной платформы приведена в разделе *Рекомендуемые конфигурации оборудования для сервера управления*.

Агенты

Агенты — это приложения, которые устанавливаются на рабочие нагрузки и выполняют резервное копирование данных, их восстановление и другие операции.

Перед выполнением любой операции защиты агенты обращаются к серверу управления для проверки предварительных требований. Подключение к серверу управления необходимо для развёртывания новых планов защиты. Если план защиты уже развёрнут, агент продолжает выполнять операции защиты на протяжении 30 дней после утраты связи с сервером управления.

Выберите агент в зависимости от того, для какого именно объекта нужно создать резервную копию. В таблице ниже приведены основные сведения, которые помогут принять решение.

Обратите внимание: вместе с агентами для Exchange, SQL, Active Directory и Oracle автоматически устанавливается агент для Windows. Например, установив агент для SQL, вы также сможете создавать резервные копии всей машины.

Часть агентов предоставляется в виде виртуального устройства, и для их развёртывания требуется лишь среда виртуализации.

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Физические машины		
Диски, тома и файлы на физических машинах под управлением ОС Windows	Агент для Windows	На защищаемую машину с *ОС Windows*.
Диски, тома и файлы на физических машинах под управлением ОС Linux	Агент для Linux	На защищаемую машину с *ОС Linux*.
Приложения		
Базы данных PostgreSQL, PostgreSQL для 1С, Postgres Pro Standard, Postgres Pro Enterprise, Patroni, Platform V Pangolin, Proxima DB, Jatoba, JaDog (Jatoba), Tantor, Arenadata Prosperity	Агент для PostgreSQL, а также агент для Windows или агент для Linux	На машину с сервером PostgreSQL или на имеющий к нему сетевой доступ компьютер с *ОС Windows* или *ОС Linux*.
РЕД База Данных	Агент для Windows или агент для Linux	На машину с СУБД РЕД База Данных и *ОС Windows* или *ОС Linux*.
Базы данных MySQL/MariaDB	Агент для MySQL/MariaDB и агент для Linux	На машину с сервером MySQL/MariaDB и *ОС Linux*.
Базы данных MongoDB	Агент для Windows или агент для Linux	На машину с сервером MongoDB и *ОС Windows* или *ОС Linux*.
Базы данных SQL Server	Агент для SQL	На машину с Microsoft SQL Server и *ОС Windows*.
Машины под управлением Oracle Database	Агент для Oracle	На машину с запущенной Oracle Database и *ОС Windows* или *ОС Linux*.
Базы данных SAP HANA[1]	Агент для Linux	На машину с SAP HANA и *ОС Linux*.
Пространства имён и постоянные тома Kubernetes	Агент для Kubernetes	На машину с *ОС Linux*, у которой есть сетевой доступ к кластеру Kubernetes.
Данные CommuniGate Pro	Агент для CommuniGate Pro, а также агент для Windows или агент для Linux	На машину с CommuniGate Pro или на другую машину, имеющую сетевой доступ к CommuniGate Pro, оснащённую *ОС Windows* или *ОС Linux*.
Данные VK WorkMail и VK WorkDisk	Агент для VK WorkMail, а также агент для Windows или агент для Linux	На машину с *ОС Windows* или *ОС Linux*, у которой есть сетевой доступ к VK WorkMail.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Данные RuPost	Агент для RuPost и агент для Linux	На машину с *ОС Linux*, у которой есть сетевой доступ к RuPost.
Данные Mailion	Агент для Mailion, а также агент для ОС Windows или агент для Linux	На машину с Mailion или на другую машину, имеющую сетевой доступ к Mailion, оснащённую *ОС Windows* или *ОС Linux*.
Базы данных и почтовые ящики Exchange	Агент для Exchange	На машину с ролью почтового ящика Microsoft Exchange Server[2], оснащённую *ОС Windows*. Если требуется резервное копирование только почтового ящика, агент может быть установлен на любой машине с ОС Windows, которая имеет сетевой доступ к машине, на которой включена роль клиентского доступа Microsoft Exchange Server.
Машины с Microsoft SharePoint	Агент для SQL и агент для Windows	На машину с *ОС Windows* и сервером баз данных, сервером веб-интерфейса и сервером приложений.
Машины с доменными службами Active Directory	Агент для Active Directory	На машину контроллера домена с *ОС Windows*.
Виртуальные машины		
Виртуальные машины VMware ESXi	Агент для VMware (Windows)	На машину с *ОС Windows* с сетевым доступом к vCenter Server и хранилищу виртуальных машин.[3] Предоставляется в виде приложения Windows для работы в среде ОС Windows. Используйте этот агент в случаях, когда необходимо настроить *резервное копирование без использования локальной сети (LAN-free backup)*, когда доступен свободный сервер на базе ОС Windows либо требуется развертывание на этой ОС, или когда требуется восстановление данных из резервных копий с *поддержкой приложений в виде файлов*. Во всех прочих сценариях рекомендуется задействовать агенты на базе виртуального устройства.
	Агент для VMware (виртуальное устройство)	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Виртуальные машины oVirt, ROSA Virtualization, zVirt, Red Hat Virtualization, РЕД Виртуализация, HOSTVM	Агент для oVirt (локальный)	На машину с *ОС Linux*. Используйте этот агент для резервного копирования с использованием аппаратных моментальных снимков (подробнее см. в разделе *Настройка хранилища данных YADRO TATLIN.UNIFIED*). В прочих сценариях рекомендуется задействовать агенты на базе виртуального устройства.
	Агент для oVirt (виртуальное устройство)	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины SpaceVM	Агент для SpaceVM	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины ECP VeiL	Агент для ECP VeiL	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины Кибер Инфраструктуры	Агент для Кибер Инфраструктуры	В среду виртуализации в виде виртуального устройства.
Виртуальные машины OpenStack, РУСТЭК, VK Cloud	Агент для OpenStack	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины Basis DynamiX Enterprise	Агент для Basis DynamiX Enterprise	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины OpenNebula, ПК СВ ”Брест”, ПО ”Альт Виртуализация”, Система группового управления ”Горизонт-ВС”	Агент для OpenNebula	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины Proxmox VE	Агент для Proxmox VE	В среду виртуализации в виде виртуального устройства с предустановленной поддерживаемой ОС.
Виртуальные машины VMmanager	Агент для VMmanager	В среду виртуализации в виде виртуального устройства.
Виртуальные машины Hyper-V	Агент для Hyper-V	На хост Hyper-V с *ОС Windows*.
Виртуальные машины Red Hat Virtualization (RHV/RHEV)	Агент для Windows или агент для Linux[4]	На машину, резервная копия которой будет создана.[5]

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Виртуальные машины на основе ядра (KVM)	Агент для Windows или агент для Linux[4]	На машину, резервная копия которой будет создана.[5]
Виртуальные машины Oracle	Агент для Windows или агент для Linux[4]	На машину, резервная копия которой будет создана.[5]

Узел хранения

Узел хранения — это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объём корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается управлением хранилищами корпоративных резервных копий (см. *Добавление управляемого хранилища*).

ПО узла хранения должно быть установлено на аппаратную платформу, оснащённую одной из поддерживаемых ОС *Windows* или *Linux*. Требования к аппаратной платформе узла хранения приведены в разделе *Системные требования*.

Другие компоненты

Компонент	Функция	Куда его следует установить?
Компоненты для удалённой установки	Сохраняет пакеты установки агента в локальную папку.	На машину с *ОС Windows* и сервером управления.
Мастер создания загрузочных носителей	Создаёт загрузочный носитель.	На машину с *ОС Windows* или *ОС Linux*.

(продолжается на следующей странице)

[1] Также поддерживается защита СУБД SAP HANA, которая установлена в виртуальную машину VMware ESXi. Подробные сведения см. в разделе *Резервное копирование виртуальных серверов*.

[2] В ходе установки агент для Exchange проверяет достаточность свободного пространства на машине, где он запущен. При выполнении фрагментарного восстановления временно необходимо свободное пространство в объеме, равном 15 процентам от объема самой большой базы данных Exchange.

[3] Если ваш ESXi использует SAN-хранилище, установите агент на машине, подключенной к тому же SAN-хранилищу. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Подробные инструкции см. в разделе *Резервное копирование без использования локальной сети посредством Windows-агента для VMware*.

[4] Для выполнения операций защиты установите агент для операционной системы, которая используется в гостевой системе (агент для Windows или агент для Linux).

[5] Лицензия Кибер Бэкап Стандартная для платформы виртуализации не подходит для лицензирования данных ВМ. Необходимо использовать либо лицензию Кибер Бэкап Расширенная для платформы виртуализации для лицензирования хоста виртуализации, либо лицензии Кибер Бэкап для рабочей станции или физического сервера для лицензирования каждой ВМ как физической машины.

(продолжение с предыдущей страницы)

Компонент	Функция	Куда его следует установить?
Программа командной строки	Предоставляет интерфейс командной строки.	На машину с *ОС Windows* или *ОС Linux*.
Мониторинг Защиты Данных	Позволяет пользователям отслеживать выполнение запущенных задач в области уведомлений ОС Windows.	На машину с *ОС Windows*.
PXE-сервер	Активирует загрузку машин на загрузочный носитель по сети.	На машину с *ОС Windows*.

Требования к программному обеспечению

В этом разделе приведены требования к программному обеспечению, необходимому для установки и работы Кибер Бэкап и его компонентов:

- к операционным системам и средам (см. раздел *Поддерживаемые операционные системы и среды*), в том числе:
  - к наличию дополнительных пакетов для работы в среде ОС Linux (см. раздел *Необходимые пакеты для ОС Linux*);
  - к настройкам для поддержки ОС Astra Linux SE (см. раздел *Совместимость с ОС Astra Linux SE*);
- к веб-браузерам для работы с интерфейсом пользователя (см. раздел *Поддерживаемые веб-браузеры*).

Также в разделе приведены сведения о программном обеспечении, которое поддерживается в качестве защищаемых рабочих нагрузок:

- об операционных системах (см. раздел *Поддерживаемые операционные системы*);
- о платформах виртуализации (см. раздел *Поддерживаемые платформы виртуализации*);
- о почтовых сервисах (см. раздел *Поддерживаемые почтовые сервисы*);
- о СУБД (см. раздел *Поддерживаемые СУБД*);
- о приложениях Microsoft (см. раздел *Поддерживаемые версии приложений Microsoft*).

Кроме этого, в разделе указаны требования к поддерживаемым программам шифрования (см. раздел *Совместимость с программами шифрования*) и службам каталогов (см. раздел *Поддерживаемые интеграции со службами каталогов*).

Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Яндекс Браузер 26 или более поздней версии
- Google Chrome 146 или более поздней версии
- Opera 127 или более поздней версии
- Mozilla Firefox 148 или более поздней версии
- Microsoft Edge 146 или более поздней версии

В других веб-браузерах интерфейс пользователя может отображаться неправильно или могут быть недоступны некоторые функции.

Поддерживаемые операционные системы

В таблице приведена информация об операционных системах (ОС), совместимость которых с текущей версией Кибер Бэкап протестирована или заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап. Поддерживаются только 64-битные версии ОС.

- **Да** — совместимость подтверждена в ходе тестирования с данной версией Кибер Бэкап.
- **Экспертно** — совместимость заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.
- **Нет** — совместимость не подтверждена в ходе тестирования с данной версией Кибер Бэкап.

ОС	Версия, выпуск	Версия ядра (для ОС Linux)[с. 17, 4]	Агент	Сервер управления	Узел хранения
AlmaLinux	9.7	5.14.0-611.27.1.el9_7	Да	Да	Да
AlmaLinux	9.3	5.14.0-362.24.2.el9_3	Да	Экспертно	Экспертно
AlmaLinux	8.x[1]		Экспертно	Экспертно	Экспертно
Альт Сервер	10.0	5.10.145-std-def-alt1	Да	Да	Да
Альт Сервер	9.2	5.4.224-std-def-alt1	Да	Да	Да
Альт Сервер	11.0	6.12.34-6.12-alt1	Да	Да	Да
Альт СП	10.2 Сервер	6.1.134-un-def-alt0.c10f.2	Да	Да	Да
Альт СП	10.2.1 Сервер	6.1.136-un-def-alt0.c10f.2	Да	Да	Да
Альт СП	8 Сервер	5.10.150-std-def-alt0.c9f.2	Да	Да	Да
Альт Рабочая станция	10.1	5.10.154-std-def-alt1	Да	Да	Да
Альт Рабочая станция	11.1 beta	6.12.34-6.12-alt1	Да	Да	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

ОС	Версия, выпуск	Версия ядра (для ОС Linux)[4]	Агент	Сервер управления	Узел хранения
Альт Рабочая станция К	10.3	6.1.79-un-def-alt1	Да	Да	Да
АльтерОС	9.5 Сервер	6.6.58-1.el9.alteros	Да	Да	Да
АльтерОС	7.5 Сервер	5.16.2-1.el7.alteros	Да	Да	Да
Astra Linux Special Edition	1.8.1	6.1.90-1-generic	Да	Да	Экспертно
Astra Linux Special Edition	1.8.2	6.1.124-1-generic	Да	Да	Экспертно
Astra Linux Special Edition	1.8.3	6.1.141-1-generic	Да	Да	Экспертно
Astra Linux Special Edition	1.8.5	6.12.60-1-generic	Да	Да	Экспертно
Astra Linux Special Edition	1.8.6	6.12.77-1-generic	Да	Да	Экспертно
Astra Linux Special Edition (с включённым КСЗИ)	1.8.1	6.6.28-1-generic	Да	Да	Да
Astra Linux Special Edition	1.7.0	5.4.0-54-generic	Да	Да	Да
Astra Linux Special Edition	1.7.1	5.10.0-1045-generic	Да	Да	Да
Astra Linux Special Edition	1.7.10	6.1.161-1-generic	Да	Да	Экспертно
Astra Linux Special Edition	1.7.3	5.15.0-33-generic	Да	Да	Да
Astra Linux Special Edition	1.7.4	5.15.0-70-generic	Да	Да	Да
Astra Linux Special Edition	1.7.5	6.1.50-1-generic	Да	Да	Да
Astra Linux Special Edition	1.7.6	6.1.90-1-generic	Да	Экспертно	Экспертно
Astra Linux Special Edition	1.7.9	5.15.0-158-generic	Да	Да	Экспертно

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

ОС	Версия, выпуск	Версия ядра (для ОС Linux)[4]	Агент	Сервер управления	Узел хранения
Astra Linux Special Edition (с включённым КСЗИ)	1.7.3	5.15.0-33-generic	Да	Да	Да
Astra Linux Common Edition	2.12.43	5.10.0-1038.40-generic	Да	Да	Да
Astra Linux Common Edition	2.12.45	5.15.0-33-generic	Да	Да	Да
Astra Linux Common Edition	2.12.46	5.15.0-70-generic	Да	Да	Да
Astra Linux Special Edition	1.6 ”Смоленск”	4.15.3-1-generic	Да	Да	Да
Astra Linux Special Edition (с включённым КСЗИ)	1.6 ”Смоленск”	4.15.3-1-generic	Да	Да	Да
CentOS Linux	8.5.2111	4.18.0-348.7.1.el8_5	Да	Да	Да
CentOS Linux	7.9.2009	3.10.0-1160.80.1.el7	Да	Нет	Да
CentOS	Stream 9	5.14.0-572.el9	Да	Да	Да
CentOS	Stream 10	6.12.0-63.el10	Да	Да	Да
Debian GNU/Linux	12	6.1.0-22	Да	Да	Да
Debian GNU/Linux	12	6.1.0-47	Да	Да	Экспертно
Debian GNU/Linux	11	5.10.0-20, 5.10.0-36	Да	Да	Да
Debian GNU/Linux	10	4.19.0-19, 4.19.0-24	Да	Да	Да
Debian GNU/Linux	13	6.12.48+deb13	Да	Да	Да
Microsoft Windows	10 Pro, 11 Pro, 11 Enterprise		Да	Да	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

ОС	Версия, выпуск	Версия ядра (для ОС Linux)[4]	Агент	Сервер управления	Узел хранения
Microsoft Windows Server	2016 Standard[3], 2019 Standard[с. 17, 3], 2022 Standard[с. 17, 3], 2025 Standard[с. 17, 3], 2019 Datacenter[с. 17, 3], 2022 Datacenter[с. 17, 3]		Да	Да	Да
Мос.ОС Серверная	15.5	5.14.21-151500.55.59-default	Да	Да	Да
МСВСфера Сервер	9.1	5.14.0-162.6.1.el9_1	Да	Да	Да
openSUSE	12.3	3.7.10-1.32-desktop	Да	Нет	Да
openSUSE Leap	15.2	5.3.18-lp152.106-default	Да	Да	Да
Oracle Linux	9.5	5.15.0-306.177.4.1.el9uek	Да	Да	Да
Oracle Linux	8.x		Экспертно	Экспертно	Экспертно
Основа	2.10.1	6.6.27-0	Да	Да	Да
Основа	2.7	5.15.0-2.7	Да	Да	Да
Основа	3.0.3	6.12.29-1	Да	Да	Да
Red Hat Enterprise Linux	10.0	6.12.0-55.41.1.el10_0	Да	Да	Да
Red Hat Enterprise Linux	8.10[с. 17, 1]		Экспертно	Экспертно	Экспертно
Red Hat Enterprise Linux	7.x[с. 17, 1]		Экспертно	Нет	Экспертно
РЕД ОС	8.0 Стандартная (конфигурация ”Сервер минимальный”)	6.12.21-1.red80	Да	Да	Да
РЕД ОС	8.0 Стандартная (конфигурация ”Сервер минимальный”)	6.6.51-1.red80, 6.6.6-1.red80	Да	Да	Экспертно

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

ОС	Версия, выпуск	Версия ядра (для ОС Linux)[4]	Агент	Сервер управления	Узел хранения
РЕД ОС	8.0.2 Стандартная (конфигурация ”Сервер минимальный”)	6.12.90-1.red80	Да	Да	Экспертно
РЕД ОС	7.3.1 Стандартная (конфигурация ”Сервер минимальный”)	5.15.35-5.el7.3	Да	Да	Да
РЕД ОС	7.3.5 Стандартная (конфигурация ”Сервер минимальный”)	6.1.128-2.el7.3	Да	Да	Да
РЕД ОС	7.2		Экспертно	Экспертно	Экспертно
РОСА ”ХРОМ”	12F.1 Рабочая станция	6.1.58-generic-5rosa2021.15	Да	Экспертно	Экспертно
РОСА ”ХРОМ”	12.3 Сервер	5.10.150-generic-1rosa2021.1	Да	Да	Да
РОСА ”ХРОМ”	12.4 Сервер	5.17.11-generic-2rosa2021.1	Да	Да	Да
РОСА ”ХРОМ”	12.5.1 Сервер	6.6.27-generic-3rosa2021.1	Да	Да	Да
РОСА ”ХРОМ”	12F.1 Сервер	6.1.58-generic-5rosa2021.15	Да	Да	Да
РОСА ”КОБАЛЬТ”	7.9 Сервер	3.10.0-1160.76.1.el7	Да	Да	Да
РОСА ”ФРЕШ”	12.3 Сервер	5.15.79-generic-1rosa2021.1	Да	Да	Да
РОСА ”ФРЕШ”	12.5 Сервер	6.12.25	Да	Да	Да
Platform V SberLinux OS	9.3	5.14.0-362.24.1.sl9_3.1	Да	Да	Да
SUSE Linux Enterprise Server	15 SP5[2]	5.14.21-150500.55.68-default	Да	Да	Да
SUSE Linux Enterprise Server	15[с. 17, 2]		Экспертно	Экспертно	Экспертно
SUSE Linux Enterprise Server	12[с. 17, 2]		Экспертно	Нет	Экспертно

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

ОС	Версия, выпуск	Версия ядра (для ОС Linux)[4]	Агент	Сервер управления	Узел хранения
Ubuntu	22.10	5.19.0-26-generic	Да	Да	Да
Ubuntu	23.04	6.2.0-20-generic	Да	Да	Да
Ubuntu	25.04	6.14.0-32-generic	Да	Да	Да
Ubuntu	18.04.6 LTS	4.15.0-213-generic	Да	Да	Да
Ubuntu	20.04.5 LTS	5.15.0-60-generic	Да	Да	Да
Ubuntu	22.04.2 LTS	5.15.0-25-generic	Да	Да	Да
Ubuntu	24.04.3 LTS	6.14.0-29-generic	Да	Да	Да
Ubuntu	24.04.3 LTS	6.8.0-90-generic	Да	Экспертно	Экспертно
Ubuntu	26.04 LTS	7.0.0-28-generic	Да	Да	Да

Поддерживаемые платформы виртуализации

Кибер Бэкап позволяет выполнять резервное копирование платформ виртуализации как на уровне гипервизора (без использования агента), так и изнутри гостевой операционной системы (ОС); подробнее об этом см. в разделе *Резервное копирование*.

В таблице приведена информация о платформах виртуализации, совместимость которых с текущей версией Кибер Бэкап протестирована или заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.

- **Да** — совместимость подтверждена в ходе тестирования с данной версией Кибер Бэкап.
- **Экспертно** — совместимость заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.
- **Нет** — совместимость не подтверждена в ходе тестирования с данной версией Кибер Бэкап.

Агенты для указанных в таблице платформ виртуализации поставляются в виде виртуальных устройств с предустановленной поддерживаемой ОС, кроме:

- Microsoft Hyper-V — агент поддерживает только *ОС Windows*.
- VMware ESXi — один из агентов для VMware предоставляется в виде Windows-приложения для работы в среде *ОС Windows*.
- oVirt — один из агентов для oVirt, предназначенный для *резервного копирования с*

[4] Агенты поддерживают работу с ОС с версиями ядра от 3.2 до 7.0 и glibc версии 2.17 и новее. Сервер управления поддерживает работу с ОС с версиями ядра от 3.2 до 7.0 и glibc версии 2.25 и новее. Узел хранения поддерживает работу с ОС с версиями ядра от 3.2 до 7.0 и glibc версии 2.17 и новее.

[1] Кроме конфигураций со Stratis.

[3] Все выпуски, кроме Nano Server.

[2] Поддерживается в файловых системах, за исключением Btrfs.

использованием аппаратных моментальных снимков, поддерживает только *ОС Linux*.

О том, какой агент необходим для защиты данных и куда он должен быть установлен, см. в разделе *Компоненты*.

Платформа виртуализации	Версия, выпуск	Совместимость
Кибер Инфраструктура	6.0	Экспертно
Кибер Инфраструктура	6.5, 6.7.0, 6.7.3	Да
HOSTVM	4	Экспертно
ROSA Virtualization	2.0, 2.1, 3.0[1], 4.0[с. 19, 1]	Экспертно
РУСТЭК	2.6	Экспертно
VK Cloud	4.0	Экспертно
VK Cloud	4.3	Нет
VMware ESXi	6.7U3, 7.0, 8.0U3	Да
VMware ESXi	8.0, 8.0U1, 8.0U2	Экспертно
Microsoft Hyper-V	Windows 10 с Hyper-V, Microsoft Hyper-V Server 2016, Windows Server 2022 с Hyper-V[2][3]	Экспертно
Microsoft Hyper-V	Windows Server 2016 с Hyper-V[с. 19, 3], Windows Server 2019 с Hyper-V[с. 19, 3]	Да
OpenStack	Zed, Caracal, Dalmatian	Экспертно
OpenStack	Ussuri	Да
Proxmox Virtual Environment	7.2, 7.3, 7.4, 8.4.0, 9.0.3	Экспертно
SpaceVM	с 6.0.5—6.5.8	Экспертно
SpaceVM	7.0.3	Да
ECP VeiL	с 4.7—5.1.10	Экспертно
ECP VeiL	5.1.9	Да
oVirt	4.2, 4.3, 4.5	Экспертно
oVirt	4.4	Да
РЕД Виртуализация	7.2, 7.3.2, 8.0	Экспертно
РЕД Виртуализация	7.3	Да
zVirt	3.0, 3.1, 3.2, 3.3, 4.0, 4.2, 4.3, Max, 4.4, 5.0	Экспертно
zVirt	4.1, 4.5	Да
Basis DynamiX Enterprise	3.8.8—4.1, 4.3	Экспертно
Basis DynamiX Enterprise	4.4	Да
ПК СВ ”Брест”	На основе OpenNebula 6.0.0.2	Экспертно
Альт Виртуализация	10 (на основе OpenNebula 6.2.0.1), 10.2 (PVE 7.4)	Да
Альт Виртуализация	10.4, 11 (PVE 7.4 и PVE 8.4)	Экспертно

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Платформа виртуализации	Версия, выпуск	Совместимость
Система группового управления ”Горизонт-ВС”	1.8.3	Да
OpenNebula	6.0.0.2	Да
VMmanager	6 (2026.09.1-7 Regular)	Да

Ограничения

Создание моментальных снимков дисков при резервном копировании без агента

При резервном копировании без агента моментальные снимки дисков ВМ создаются через API-интерфейс платформы виртуализации. Система хранения данных, на которой размещены диски ВМ, должна поддерживать создание моментальных снимков средствами платформы виртуализации.

Отказоустойчивые машины

Агент для VMware выполняет резервное копирование отказоустойчивой машины, только если в VMware vSphere включена отказоустойчивость. При выполнении обновления с более ранней версии vSphere достаточно отключить и снова включить отказоустойчивость для каждой машины. При использовании более ранней версии vSphere установите агент в гостевой операционной системе.

Независимые диски и RDM-диски

Агент для VMware не создает резервные копии RDM-дисков в режиме физической совместимости или независимых дисков. При выполнении резервного копирования агент пропускает эти диски и добавляет предупреждения в журнал. Чтобы не получать эти предупреждения, следует исключить из плана защиты независимые диски и RDM-диски в режиме физической совместимости. Если необходимо выполнить резервное копирование этих дисков или данных на этих дисках, установите агент в гостевой операционной системе.

Диски прямого доступа

Агенты для Hyper-V не выполняют резервного копирования дисков прямого доступа. Во время резервного копирования агент пропускает эти диски и добавляет предупреждения в журнал. Чтобы не получать эти предупреждения, следует исключить из плана защиты диски прямого доступа. Если необходимо выполнить резервное копирование этих дисков или данных на этих дисках, установите агент в гостевой операционной системе.

Кластеризация гостевых систем Hyper-V

Агент для Hyper-V не поддерживает резервное копирование виртуальных машин Hyper-V, которые

[1] Не поддерживается восстановление ВМ с ОС на основе CentOS в новую ВМ на платформу VMware.

[2] Резервное копирование с поддержкой приложений не поддерживается.

[3] Все варианты установки, кроме Nano Server.

являются узлами отказоустойчивого кластера Windows Server. Моментальный снимок VSS на уровне хоста может даже временно отключить внешний диск кворума от кластера. Если необходимо выполнить резервное копирование этих машин, установите агенты в гостевых операционных системах.

Подключение iSCSI в гостевой ОС

Агент для VMware и агент для Hyper-V не выполняют резервное копирование томов логического устройства, подключенных инициатором iSCSI, который работает в этой гостевой операционной системе. Поскольку у гипервизоров ESXi и Hyper-V нет никакой информации о таких томах, эти тома не включаются в моментальные снимки на уровне гипервизора, а их резервное копирование пропускается без предупреждений. Чтобы создать резервную копию этих томов или данных на этих томах, установите агент в гостевой операционной системе.

Машины Linux с логическими томами (LVM)

Агент для VMware и агент для Hyper-V не поддерживают указанные ниже операции для машин Linux с LVM:

- Миграция P2V и V2P. Используйте агент для Linux или загрузочный носитель, чтобы создать резервную копию, и загрузочный носитель для восстановления.
- Запуск виртуальной машины из резервной копии, созданной агентом для Linux или загрузочным носителем.
- Преобразование резервной копии, созданной агентом для Linux или загрузочным носителем, в виртуальную машину.

Зашифрованные виртуальные машины

- Резервное копирование зашифрованных виртуальных машин выполняется в незашифрованном состоянии.
- Восстановленные виртуальные машины всегда являются незашифрованными.
- При резервном копировании виртуальных машин рекомендуем также шифровать виртуальную машину, на которой запущен агент для VMware. В противном случае операции с зашифрованными машинами могут выполняться медленнее, чем ожидается. Примените **политику шифрования ВМ** к машине агента, используя веб-клиент vSphere.
- Резервное копирование зашифрованных виртуальных машин будет выполнено по локальной сети, даже если настроен режим транспорта сети SAN для агента. Агент выполнит возврат из реплики, используя транспорт NBD, поскольку VMware не поддерживает транспорт сети SAN для резервного копирования зашифрованных виртуальных дисков.

Безопасная загрузка

Безопасная загрузка отключается после восстановления виртуальной машины как новой виртуальной машины. По окончании восстановления можно вручную включить этот параметр.

Резервное копирование конфигурации ESXi

Не поддерживается для VMware vSphere 7.0 и новее.

Виртуальные диски типа Direct LUN виртуальных машин oVirt и аналогичных систем виртуализации

При резервном копировании виртуальных машин систем виртуализации oVirt, ROSA Virtualization, zVirt, Red Hat Virtualization, РЕД Виртуализация и HOSTVM виртуальные диски типа Direct LUN не включаются в резервные копии.

Сортировка дисков виртуальных машин oVirt и аналогичных систем виртуализации

При резервном копировании только выбранных дисков виртуальных машин систем виртуализации oVirt, ROSA Virtualization, zVirt и РЕД Виртуализация необходимо включить сортировку дисков ВМ на виртуальном устройстве с агентом. Для этого в файле `/etc/Acronis/VirtualWare.config` установите значение `1` параметру `DiskSortingEnabled`. Например:

```
<key name=”oVirt”>
...
<value name=”DiskSortingEnabled” type=”Tdword”>1</value>
...
</key>
```

Резервное копирование виртуальной машины с диском TPM State для Proxmox Virtual Environment (Альт Виртуализация Proxmox)

Резервное копирование виртуальной машины с диском TPM State не поддерживается, если машина включена. Перед запуском резервного копирования виртуальную машину необходимо выключить.

Поддерживаемые почтовые сервисы

Кибер Бэкап позволяет выполнять резервное копирование почтовых сервисов (подробнее об этом см. в разделе *Защита приложений, сервисов, баз данных*).

В таблице приведена информация о почтовых сервисах, совместимость которых с текущей версией Кибер Бэкап протестирована или заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.

- **Да** — совместимость подтверждена в ходе тестирования с данной версией Кибер Бэкап.
- **Экспертно** — совместимость заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.

- **Нет** — совместимость не подтверждена в ходе тестирования с данной версией Кибер Бэкап.

Агенты для указанных в таблице почтовых сервисов могут быть установлены на машину с *ОС Windows* или с *ОС Linux*, кроме:

- RuPost — агент поддерживает только *ОС Linux*;
- Microsoft Exchange Server — агент поддерживает только *ОС Windows*.

О том, какой агент необходим для защиты данных и куда он должен быть установлен, см. в разделе *Компоненты*.

Почтовый сервис	Версия, выпуск	Совместимость
CommuniGate Pro	6.3.14, 6.3.19, 6.4.0, 6.5, 6.5.2hotfix1	Да
VK WorkMail	25.4, 26.1, 26.3	Да
Mailion	2.3	Да
Microsoft Exchange Server	2013[1]—2016[2]	Экспертно
Microsoft Exchange Server	SE 15.2, 2019[2]	Да
Microsoft Exchange Server DAG	SE 15.02.2562.017	Да
RuPost	4.2.3 Enterprise	Да

Поддерживаемые СУБД

Кибер Бэкап позволяет выполнять резервное копирование систем управления базами данных (СУБД), подробнее об этом см. в разделе *Защита приложений, сервисов, баз данных*.

В таблице приведена информация о СУБД, совместимость которых с текущей версией Кибер Бэкап протестирована или заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.

- **Да** — совместимость подтверждена в ходе тестирования с данной версией Кибер Бэкап.
- **Экспертно** — совместимость заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.
- **Нет** — совместимость не подтверждена в ходе тестирования с данной версией Кибер Бэкап.

Агенты для указанных в таблице СУБД могут быть установлены на машину с *ОС Windows* или с *ОС Linux*, кроме:

- MySQL и MariaDB — агент поддерживает только *ОС Linux*;
- Microsoft SQL Server и SAP HANA — агент поддерживает только *ОС Windows*.

[1] Все выпуски, накопительный пакет обновления 1 (CU1) или более поздней версии.
[2] Все выпуски.

О том, какой агент необходим для защиты данных и куда он должен быть установлен, см. в разделе *Компоненты*.

СУБД	Версия, выпуск	Совместимость
MariaDB	10.1, 10.3, 10.11	Да
MySQL	8.0.36, 8.0.45	Да
Microsoft SQL Server	2012—2017	Экспертно
Microsoft SQL Server	2019	Да
Microsoft SQL Server AAG	2019	Да
PostgreSQL	11, 12, 14, 15, 16, 17, 18	Да
PostgreSQL	13	Экспертно
PostgreSQL для 1С		Экспертно
Postgres Pro Standard	11	Экспертно
Postgres Pro Standard	12, 13, 14, 15, 16, 17, 18	Да
Postgres Pro Enterprise	11, 12, 13, 16	Экспертно
Postgres Pro Enterprise	14, 15, 17, 18	Да
Patroni	3.3.2, 4.0.4	Да
Oracle Database	11.2[4], 12.2[4]	Да[5]
Oracle Database	19[4]	Экспертно
Jatoba	5, 6, 18	Да
JaDog	4.0, 4.3	Да
Proxima DB	2.0, 3.0	Да
Platform V Pangolin SE	6.1.7[1]	Экспертно
Tantor	14—17	Экспертно
Arenadata Prosperity	4.0	Экспертно
РЕД База Данных	3.0—5.1	Экспертно
MongoDB	6.0[2]	Экспертно
SAP HANA	2.0 SPS 03[3]	Экспертно

[4] Все выпуски.

[5] Поддержка резервного копирования осуществляется с помощью команд, выполняемых до и после резервного копирования, в связке с ПО RMAN (подробнее см. в разделе *Защита Oracle Database*).

[1] Требуются дополнительные настройки на машине с агентом, подробнее см. статью базы знаний.

[2] Поддержка через *команды до и после процедуры*.

[3] Установка в RHEL 7.6 на физической или виртуальной машине VMware ESXi. Поскольку SAP HANA не поддерживает восстановление контейнеров баз данных с несколькими арендаторами с использованием моментальных снимков хранилища, данное решение поддерживает контейнеры SAP HANA с базой данных только одного арендатора.

Поддерживаемые версии приложений Microsoft

Поддерживаемые версии Microsoft Active Directory

Поддерживается резервное копирование контроллеров домена Active Directory, развёрнутых на серверах Microsoft Windows Server (перечень версий см. в разделе *Поддерживаемые операционные системы*).

Поддерживаемые версии Microsoft Exchange Server

Поддерживаемые версии Microsoft Exchange Server приведены в разделе *Поддерживаемые почтовые сервисы*.

Поддерживаемые версии Microsoft SharePoint

Кибер Бэкап поддерживает резервное копирование баз данных SQL Server, используемых локально установленными продуктами SharePoint следующих версий:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2 (необходима ферма восстановления SharePoint для прикрепления баз данных)

Защита данных SharePoint в Microsoft 365 не поддерживается.

Резервные копии или базы данных, из которых извлекаются данные, должны происходить из той же версии SharePoint, что и версия, где установлен SharePoint Explorer.

Поддерживаемые версии Microsoft SQL Server

Поддерживаемые версии Microsoft SQL Server приведены в разделе *Поддерживаемые СУБД*.

Поддерживаемые приложения

Кибер Бэкап позволяет выполнять резервное копирование Kubernetes (подробнее см. в разделе *Защита Kubernetes*).

В таблице приведена информация о приложениях, совместимость которых с текущей версией Кибер Бэкап протестирована или заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.

- **Да** — совместимость подтверждена в ходе тестирования с данной версией Кибер Бэкап.

- **Экспертно** — совместимость заявлена экспертно на основе тестирования с предыдущими версиями Кибер Бэкап.
- **Нет** — совместимость не подтверждена в ходе тестирования с данной версией Кибер Бэкап.

Агент для Kubernetes может быть установлен на машину с *ОС Linux* (подробнее см. в разделе *Компоненты*).

СУБД	Версия, выпуск	Совместимость
Kubernetes	1.24.17, 1.32.12	Да
Deckhouse	1.68.13 EE	Экспертно

Необходимые пакеты для ОС Linux

Чтобы добавить необходимые модули к ядру Linux, программе установки требуются перечисленные ниже пакеты Linux:

- Пакет с заголовками или исходными кодами ядра. Версия пакета должна соответствовать версии ядра.
- Набор компиляторов GNU Compiler Collection (GCC). Версия GCC должна быть той же, с которой было скомпилировано ядро.
- Инструмент Make.
- Интерпретатор Perl.
- Инструмент mokutil. Необходим для определения режима загрузки ОС (UEFI с Secure Boot, UEFI без Secure Boot, BIOS).
- Библиотеки `libelf-dev`, `libelf-devel` или `elfutils-libelf-devel` с установленным параметром CONFIG_UNWINDER_ORC=y. Библиотеки необходимы для сборки ядер не ниже 4.15. Для некоторых дистрибутивов их необходимо установить отдельно от заголовков ядра.

Для корректного формирования и выгрузки отчётов в ОС ALT Linux также требуется набор шрифтов, включая следующие пакеты:

- `fonts-ttf-ms`;
- `fonts-ttf-liberation`;
- `fonts-ttf-dejavu`;
- `fonts-ttf-PTAstra`;
- `fonts-ttf-paratype-pt-*`.

Примечание

Названия вышеуказанных пакетов зависят от используемого дистрибутива ОС Linux.

В ОС Red Hat Enterprise Linux и CentOS пакеты обычно устанавливаются программой установки. В других дистрибутивах вы должны сами установить пакеты, если они не установлены или это не те версии, которые требуются.

Чтобы проверить, установлены ли пакеты, выполните следующее:

1. Выполните следующую команду, чтобы узнать версию ядра и необходимую версию GCC:

   ```
   $ cat /proc/version
   ```

   Эта команда возвращает примерно такие строки: `Linux version 2.6.35.6` и `gcc version 4.5.1`

2. Выполните следующие команды, чтобы узнать, установлен ли инструмент Make и компилятор GCC:

   ```
   $ make -v
   $ gcc -v
   ```

   Для `gcc` убедитесь, что команда возвращает ту же версию, что и в параметре `версия gcc` в шаге 1. Для инструмента `make` просто проверьте, что команда выполняется.

3. Проверьте, установлена ли соответствующая версия пакетов для создания модулей ядра.

   - В Red Hat Enterprise Linux и CentOS выполните следующую команду:

     ```
     $ yum list installed | grep kernel-devel
     ```

   - В Ubuntu выполните следующие команды:

     ```
     $ dpkg --get-selections | grep linux-headers
     $ dpkg --get-selections | grep linux-image
     ```

   В каждом из этих случаев убедитесь в том, что версии такие же, как в параметре `Linux version` в шаге 1.

4. Чтобы выяснить, установлен ли интерпретатор Perl, выполните следующую команду:

   ```
   $ perl --version
   ```

   Если на экране отображаются сведения о версии Perl, это означает, что интерпретатор установлен.

5. Проверьте, установлен ли инструмент mokutil.

   - В Red Hat Enterprise Linux и CentOS выполните следующую команду:

     ```
     $ yum list installed | grep mokutil
     ```

   - В Ubuntu выполните следующую команду:

     ```
     $ dpkg --get-selections | grep mokutil
     ```

6. В Red Hat Enterprise Linux и CentOS выполните следующую команду, чтобы проверить, установлена ли библиотека `elfutils-libelf-devel`:

   ```
   $ yum list installed | grep elfutils-libelf-devel
   ```

   Если на экране отображаются сведения о версии библиотеки, это означает, что библиотека установлена.

Установка пакетов из репозитория

Далее указано, как установить необходимые пакеты в различных дистрибутивах Linux.

Red Hat Enterprise Linux

kernel-devel, gcc, make, elfutils-libelf-devel

Программа установки загрузит и установит эти пакеты автоматически по вашей подписке на Red Hat.

perl, mokutil

Выполните следующие команды:

```
$ yum install perl
$ yum install mokutil
```

CentOS

kernel-devel, gcc, make, elfutils-libelf-devel

Программа установки загрузит и установит эти пакеты автоматически.

perl, mokutil

Выполните следующие команды:

```
$ yum install perl
$ yum install mokutil
```

Ubuntu, Debian

linux-headers, linux-image, rpm, gcc, make, perl, mokutil

Выполните следующие команды:

```
$ sudo apt-get update
$ sudo apt-get install linux-headers-$(uname -r)
$ sudo apt-get install linux-image-$(uname -r)
$ sudo apt-get install rpm
$ sudo apt-get install gcc-<версия>
$ sudo apt-get install make
$ sudo apt-get install perl
$ sudo apt-get install mokutil
```

SUSE Linux, OpenSUSE

kernel-source, gcc, make, perl, mokutil

Выполните следующие команды:

```
$ sudo zypper install kernel-source
$ sudo zypper install gcc
$ sudo zypper install make
$ sudo zypper install perl
$ sudo zypper install mokutil
```

Для OpenSUSE 12.3:

```
$ cd /usr/src/linux
$ sudo make oldconfig && make modules_prepare && make prepare
```

Astra Linux

rpm, gcc, make, linux-headers, mokutil, zstd, libnss3

Выполните следующие команды:

```
$ sudo apt install rpm
$ sudo apt install gcc
$ sudo apt install make
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
$ sudo apt-get install linux-headers-`uname -r`
$ sudo apt-get install mokutil
$ sudo apt-get install zstd
$ sudo apt-get install libnss3
```

Дополнительно для ядер версии 5.10 и новее: flex, bison

Выполните следующие команды:

```
$ sudo apt install flex
$ sudo apt install bison
```

Если используется Astra SE, пакеты необходимо установить с диска разработчика для текущей версии Astra.

ALT Linux

kernel-source, kernel-headers-modules, gcc, make, kmod-sign, mokutil, fonts-ttf-ms, fonts-ttf-liberation, fonts-ttf-dejavu, fonts-ttf-PTAstra, fonts-ttf-paratype-pt-*

Выполните следующие команды:

```
$ su -
# apt-get install kernel-source-<x.x> (где <x.x> – версия ядра)
# apt-get install kernel-headers-modules-std-def
# apt-get install gcc
# apt-get install make
# apt-get install kmod-sign
# apt-get install mokutil
# apt-get install fonts-ttf-ms
# apt-get install fonts-ttf-liberation
# apt-get install fonts-ttf-dejavu
# apt-get install fonts-ttf-PTAstra
# apt-get install fonts-ttf-paratype-pt-*
```

Если версия пакетов в репозитории новее версии текущего ядра, необходимо также обновить ядро:

```
$ su -
# apt-get update
# apt-get dist-upgrade
# update-kernel
```

После этого перезагрузите систему.

РЕД ОС

kernel-lt-devel, kernel-lt-headers, mokutil

Выполните следующие команды:

```
$ sudo yum install kernel-lt-devel
$ sudo yum install kernel-lt-headers
$ sudo yum install gcc
$ sudo yum install make
$ sudo yum install mokutil
```

Также рекомендуется полностью обновить систему:

```
$ sudo yum update
```

И затем перезагрузить её.

> **Примечание**
>
> Для разных операционных систем на основе Linux названия указанных пакетов могут отличаться.

Для других дистрибутивов Linux обратитесь к документации по дистрибутиву, чтобы выяснить точные имена необходимых пакетов и способы их установки.

Установка пакетов вручную

Возможно, необходимо будет установить пакеты вручную, если:

- У машины нет активной подписки на Red Hat или подключения к Интернету.
- Программе установки не удается найти версию `kernel-devel` или `gcc`, соответствующую версии ядра. Если доступная версия `kernel-devel` новее версии ядра, необходимо обновить ядро или установить соответствующую версию `kernel-devel` вручную.
- Необходимые пакеты имеются в локальной сети, и вы не хотите тратить время на автоматический поиск и загрузку.

Загрузите пакеты из своей локальной сети или с веб-сайта надежного третьего поставщика и установите, как описано ниже.

- В Red Hat Enterprise Linux и CentOS выполните следующую команду как привилегированный пользователь:

```
$ rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

- В Ubuntu выполните следующую команду:

```
$ sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

Пример установки пакетов вручную

Для установки необходимых пакетов выполните следующие шаги.

1. Узнайте версии ядра и GCC. Например:

```
$ cat /proc/version
Linux version 2.6.35.6-45.fc14.i686
gcc version 4.5.1
```

2. Получите пакеты `kernel-devel` и `gcc`, которые соответствуют этой версии ядра:

```
kernel-devel-2.6.35.6-45.fc14.i686.rpm
gcc-4.5.1-4.fc14.i686.rpm
```

3. Получите пакет `make`:

```
make-3.82-3.fc14.i686
```

4. Установите пакеты, выполнив следующую команду как привилегированный пользователь:

```
$ rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
$ rpm -ivh gcc-4.5.1.fc14.i686.rpm
$ rpm -ivh make-3.82-3.fc14.i686
```

   Все эти пакеты можно указать в одной команде `rpm`. Установка этих пакетов может потребовать установки дополнительных пакетов для разрешения зависимостей.

Дополнительные пакеты для ОС Linux

Для резервного копирования в сетевые папки на машине с установленным агентом для Linux необходимо иметь установленные дополнительные пакеты Linux. Например, для CentOS 7 должны быть установлены следующие пакеты (в зависимости от места сохранения резервных копий):

Место сохранения	Необходимый компонент Linux
SMB NTLM	cifs-utils
SMB with Kerberos	cifs-utils keyutils
NFS	nfs-utils

Совместимость с ОС Astra Linux SE

В этом разделе собраны сведения об особенностях использования продукта Кибер Бэкап на машинах с ОС Astra Linux Special Edition, в которой включены мандатное управлением доступом (МРД) и мандатный контроль целостности (МКЦ). Эти механизмы обеспечивают защиту конфиденциальности информации и целостности ОС и ее приложений. Подробные сведения о работе МРД и МКЦ см. в документации Astra Linux.

Установка компонентов Кибер Бэкап

- Если включено только МРД, установку необходимо выполнять с привилегиями администратора от имени пользователя из группы `astra-admin`, используя минимальный уровень конфиденциальности и пустой набор категорий конфиденциальности.
- Если включен только МКЦ, установку необходимо выполнять с привилегиями администратора от имени пользователя из группы `astra-admin`, используя максимальный уровень целостности.
- Если включены как МРД, так и МКЦ, установку необходимо выполнять с привилегиями администратора от имени пользователя из группы `astra-admin`, используя минимальный уровень конфиденциальности, пустой набор категорий конфиденциальности и максимальный уровень целостности.

Пример установки при включенных МРД и МКЦ:

```
myuser@astra-smol1-7-3:~$ id
uid=1000(myuser) gid=1000(myuser) groups=...(astra-admin)...
myuser@astra-smol1-7-3:~$ pdp-id
Уровень конф.=0(Уровень_0), Уровень целостности:63(Высокий), Категории=0x0(Нет)
Роли=()
myuser@astra-smol1-7-3:~$ chmod +x CyberBackup_18_64-bit.x86_64
myuser@astra-smol1-7-3:~$ sudo update-initramfs -u -k all
myuser@astra-smol1-7-3:~$ sudo reboot
myuser@astra-smol1-7-3:~$ sudo ./CyberBackup_18_64-bit.x86_64
...
```

Резервное копирование дисков и томов

Резервное копирование выполняется обычным образом, так как оно осуществляется на уровне блочных устройств.

Резервное копирование файлов и папок

Резервное копирование выполняется обычным образом, так как агент защиты запущен с привилегиями администратора и обладает полным доступом ко всем файловым системам.

Восстановление дисков и томов

Восстановление выполняется обычным образом, так как оно осуществляется на уровне блочных устройств.

Восстановление файлов и папок

При восстановлении Кибер Бэкап пытается назначить изначальные мандатные метки восстановленным файлам и папкам, однако какие мандатные метки получат восстановленные объекты в итоге, зависит от правил, действующих в ОС с включенными МРД и МКЦ.

> **Предупреждение**
>
> При восстановлении файлов и папок с мандатными метками на файловую систему, не поддерживающую МРД и МКЦ, мандатные метки не восстанавливаются.

Для сохранения изначальных мандатных меток файлов и папок при восстановлении из резервной копии необходимо назначать PARSEC-привилегию `PARSEC_CAP_UNSAFE_SETXATTR` агенту защиты на время восстановления.

Чтобы назначить эту привилегию агенту, выполните следующие действия на целевой машине:

1. Измените файл `/etc/systemd/system/acronis_mms.service` так, как показано ниже:

   ```
   ...
   [Service]
   CapabilitiesParsec=PARSEC_CAP_UNSAFE_SETXATTR
   ...
   ```

2. Выполните следующие команды:

   ```
   systemctl daemon-reload
   systemctl restart acronis_mms.service
   ```

3. Запишите `1` в файл `/parsecfs/unsecure_setxattr`, чтобы привилегия `PARSEC_CAP_UNSAFE_SETXATTR` вступила в силу, например:

```
echo 1 | sudo tee /parsecfs/unsecure_setxattr
```

> **Примечание**
>
> После перезагрузки машины в файл `/parsecfs/unsecure_setxattr` записывается `0`.

Репликация резервных копий

При репликации резервных копий их tibx-файлам назначаются мандатные метки по правилам, действующим в ОС с включенными МРД и МКЦ.

Узел хранения

Узел хранения устанавливается как компонент Кибер Бэкап и работает обычным образом.

Пользователи организации и ее отделов

Учетные данные пользователей, созданных на машине с сервером управления, используются для аутентификации пользователей организации и ее отделов в веб-панели Кибер Бэкап. Кибер Бэкап не учитывает, какие уровни конфиденциальности, категории конфиденциальности, уровни целостности и PARSEC-привилегии назначены этим пользователям на уровне ОС.

Совместимость с программами шифрования

Нет ограничений на резервное копирование и восстановление данных, зашифрованных программой шифрования на уровне файлов.

Программы шифрования на уровне дисков шифруют данные в реальном времени. Поэтому данные, содержащиеся в резервной копии, не шифруются. Программы шифрования на уровне дисков часто меняют области системы: загрузочные записи, таблицы разделов или таблицы файловой системы. Эти факторы влияют на резервное копирование и восстановление на уровне дисков, а также на возможность загрузки восстановленной системы и доступа ее к Зоне безопасности.

Можно создать резервную копию данных, зашифрованных при помощи указанных ниже программ шифрования на уровне файлов:

- Шифрование дисков Microsoft BitLocker,
- McAfee Endpoint Encryption,
- PGP Whole Disk Encryption.

Для надежного восстановления на уровне дисков следуйте общим правилам и рекомендациям по конкретному продукту.

Типичные правила установки

Рекомендуется установить программу шифрования перед установкой агентов защиты.

Способ использования Зоны безопасности

Зона безопасности не должна быть зашифрована на уровне дисков. Это единственный способ использования Зоны безопасности:

1. Установите программу шифрования, а затем установите агент.
2. Создайте Зону безопасности.
3. Исключите Зону безопасности при шифровании диска или его томов.

Общее правило резервного копирования

Позволяет выполнить резервное копирование на уровне дисков операционной системы. Не пытайтесь выполнить резервное копирование с использованием загрузочного носителя.

Процедуры восстановления для конкретных программ

Шифрование дисков Microsoft BitLocker

Как восстановить систему, зашифрованную функцией BitLocker:

1. Загрузите машину с загрузочного носителя.
2. Восстановите систему. Восстановленные данные будут незашифрованы.
3. Перезагрузите восстановленную систему.
4. Включите функцию BitLocker.

Если необходимо восстановить только один раздел диска, выполните восстановление из операционной системы. При восстановлении с использованием загрузочного носителя восстановленный раздел может не распознаваться системой Windows.

McAfee Endpoint Encryption и PGP Whole Disk Encryption

Можно восстановить шифрованный системный раздел, используя только загрузочный носитель.

Если восстановленную систему не удастся загрузить, восстановите основную загрузочную запись.

Поддерживаемые интеграции со службами каталогов

Кибер Бэкап позволяет добавлять пользователей и группы пользователей из следующих служб каталогов:

- Active Directory,
- Samba DC,
- FreeIPA,
- ALD Pro,
- РЕД АДМ.

Добавленные пользователи могут использовать свои учётные записи в службах каталогов для входа в веб-консоль Кибер Бэкап. Кроме того, им можно назначать привилегии для работы в Кибер Бэкап.

Процедура добавления учётных записей описана в разделе *Добавление административных учетных записей*.

Системные требования

В таблице ниже представлены требования к дисковому пространству и памяти для типичных сценариев установки компонентов продукта Кибер Бэкап. Установка выполняется с настройками по умолчанию.

Устанавливаемые компоненты	**Для установки необходимо место на диске**	**Минимальный используемый объем памяти**
Сервер управления	См. раздел *Рекомендуемые конфигурации оборудования для сервера управления*.	
Узел хранения и агент для ОС Windows Примечания: • поддерживается только 64-разрядная платформа; • для использования функции дедупликации требуется минимум 8 ГБ ОЗУ (дополнительные сведения см. в разделе *Рекомендации по дедупликации*).	2,5 ГБ	513 МБ
Агент для ОС Windows	1,4 ГБ	412 МБ

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Устанавливаемые компоненты	Для установки необходимо место на диске	Минимальный используемый объем памяти
Агент для ОС Windows и один из следующих агентов: • агент для Microsoft SQL Server; • агент для Microsoft Exchange.	1,5 ГБ	430 МБ
Агент для ОС Windows и один из следующих агентов: • агент для VMware (ОС Windows); • агент для Hyper-V.	2,4 ГБ	540 МБ
Агент для ОС Linux	1,1 ГБ	530 МБ
Агент для oVirt (виртуальное устройство zVirt/ROSA Virtualization/РЕД Виртуализация)	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для oVirt (для ОС Linux при использовании аппаратных снимков уровня СХД)		
Агент для SpaceVM	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для ECP VeiL	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для OpenStack	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для Basis DynamiX Enterprise	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для VMmanager	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для OpenNebula	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	
Агент для VMware	Предоставляется в качестве виртуального устройства, в котором учтены минимальные системные требования.	

Во время резервного копирования агент обычно занимает около 350 МБ памяти (значение получено при резервном копировании тома размером 500 ГБ). Максимальное потребление памяти может достигать 2 ГБ в зависимости от объема и типа обрабатываемых данных.

Для восстановления экземпляра базы данных PostgreSQL требуется не менее 4 ГБ памяти.

Для резервного копирования больших архивов (600 ГБ или больше) требуется 1 ГБ ОЗУ на каждый терабайт архива.

Для загрузочного носителя или восстановления диска с перезагрузкой требуется не менее 1 ГБ памяти.

Объем компонентов Кибер Бэкап с учетом файлов журналов может достигать 2 ГБ.

Производительность сервера управления зависит от сценария его установки. По умолчанию сервер управления устанавливается с локальной СУБД SQLite, что накладывает ограничения на его производительность и возможности. Для повышения производительности рекомендуется использовать СУБД PostgreSQL или Microsoft SQL Server, установленную на отдельную машину. СУБД PostgreSQL можно использовать для сервера управления на машине с ОС Linux, а СУБД Microsoft SQL Server — для сервера управления на машине с ОС Windows. Подробнее о сценариях установки см. в разделе *Рекомендуемые конфигурации оборудования для сервера управления*.

Рекомендуемые конфигурации оборудования для сервера управления

В этом разделе описаны рекомендуемые конфигурации оборудования для различных сценариев установки сервера управления.

Сервер управления на машине с ОС Linux или Windows, использующий СУБД SQLite

Требования к оборудованию

Для работы сервера управления и размещения его баз данных необходимы следующие ресурсы:

- как минимум 6 ядер ЦП (для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер),
- 16 ГБ ОЗУ,
- не менее 200 ГБ дискового пространства на SSD-диске.

Важно

Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от типа, версии и редакции используемой ОС.

Рекомендуемая конфигурация продукта Кибер Бэкап

В продукте Кибер Бэкап, развернутом на оборудовании с описанными выше характеристиками, рекомендуется:

- Использовать не более 6 000 лицензий (для повышения производительности рекомендуется

использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства).

Для установок Кибер Бэкап с большим количеством контролируемых ресурсов рекомендуется добавлять лицензии до регистрации агентов и добавления устройств.

- Добавлять не более 6 000 устройств (физических и виртуальных машин, почтовых ящиков, баз данных и других ресурсов, отображаемых в веб-консоли Кибер Бэкап в разделе **Устройства**).
- Добавлять не более 50 виртуальных устройств (virtual appliance).
- Включать в общий план не более 100 устройств (общий план включает в себя отдельные устройства), для большего количества устройств используйте групповые планы.
- Включать в групповой план не более 500 устройств (групповой план включает в себя группы устройств).
- Создавать не более 500 общих и групповых планов.
- Выполнять не более 500 одновременных операций резервного копирования и восстановления.
- Создавать не более 500 отделов.
- Использовать не более 10 уровней в иерархии отделов.
- Создавать в отделе не более 300 подотделов одного уровня.

Кроме того, общее количество записей в таблице `resources` БД службы учетных записей (Account Server) не должно превышать 60 000. Чем ближе общее количество записей к этой границе, тем ниже производительность сервера управления.

Важно

При несоблюдении этих рекомендаций производительность сервера управления может заметно снизиться.

Примечание

Реальная производительность сервера управления зависит от профиля нагрузки. Например, в случае, когда виртуальные машины размещены в кластерах, включающих в себя большое количество серверов, производительность может быть значительно меньше, чем в случае, когда серверы не объединены в кластеры или кластеры содержат небольшое количество серверов.

Дополнительная настройка

Дополнительная настройка машины с ОС Linux

Для обеспечения высокой производительности сервера управления и СУБД параметрам, ограничивающим использование ресурсов ОС, необходимо назначить достаточно большие значения. Например, на машине с ОС CentOS 7 это можно сделать следующим образом:

1. В конфигурационный файл `/etc/sysctl.conf` добавьте следующие строки:

```
fs.file-max = 6553500
kernel.pid_max = 4194303
kernel.threads-max = 4194303
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.ip_local_port_range = 32768 60999
net.core.somaxconn = 4096
net.ipv4.tcp_max_syn_backlog = 4096
net.core.netdev_max_backlog = 16384
```

2. В конфигурационный файл `/etc/security/limits.conf` добавьте следующие строки:

```
* soft nproc 65535
* hard nproc 65535
* soft nofile 65535
* hard nofile 65535
```

> **Примечание**
>
> Параметры, указанные в файлах в каталоге `/etc/security/limits.d/`, могут переопределять параметры, указанные в файле `/etc/security/limits.conf`.

3. Перезагрузите машину:

```
reboot
```

Дополнительная настройка машины с ОС Windows

- Количество портов, входящих в диапазон динамических портов для протокола TCP, должно быть в 1,5-2 раза больше общего количества агентов и виртуальных устройств, зарегистрированных в Кибер Бэкап.

Текущий диапазон динамических портов можно просмотреть с помощью команды

```
netsh int ipv4 show dynamicport tcp
```

Например:

```
netsh int ipv4 show dynamicport tcp

Protocol tcp Dynamic Port Range
---------------------------------
Start Port      : 49152
Number of Ports : 16384
```

Задать новый диапазон динамических портов можно с помощью команды

```
netsh int ipv4 set dynamicport tcp start=<start_port> num=<number_of_ports>
```

где `<start_port>` задает начальный порт, а `<number_of_ports>` — количество портов.

- Антивирусное ПО может замедлять работу сервера управления. В таком случае нужно настроить антивирус.

Дополнительная настройка продукта Кибер Бэкап на машине с ОС Linux

Для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется увеличить лимиты на количество одновременно открытых файлов для служб сервера управления и изменить уровень детализации сообщений в журналах событий с `DEBUG` на `INFO`.

Например, если сервер управления установлен на машину с ОС CentOS 7, лимит на количество одновременно открытых файлов для службы acronis_asm и уровень детализации сообщений в журналах можно изменить следующим образом:

1. Узнайте путь к скрипту запуска службы acronis_asm, просмотрев ее unit-файл:

   ```
   cat /etc/systemd/system/acronis_asm.service
   <...>
   ExecStart=/usr/sbin/acronis_asm
   <...>
   ```

2. Задайте новый лимит в скрипте запуска службы `/usr/sbin/acronis_asm`, заменив строку

   ```
   ulimit -n 1024
   ```

   на

```
ulimit -n 10240
```

и сохранив изменение.

3. Измените уровень детализации сообщений в файлах `/usr/lib/Acronis/AccountServer/account_server.json` и `/usr/lib/Acronis/BackupManager/backup_manager.yml`:

```
...
  chronica:
    level: ”INFO”
...
```

4. Перезапустите службу:

```
systemctl restart acronis_asm
```

Настройка NATS для высоконагруженных конфигураций

При развёртывании Кибер Бэкап в инфраструктуре со значительным объёмом событий по стримам NATS стандартного размера хранилища в 10 ГБ может быть недостаточно. При достижении этого лимита в журнале фиксируется ошибка:

```
[ERR] JetStream resource limits exceeded for server
```

Журнал находится в следующем файле:

В ОС Windows

`C:\ProgramData\Acronis\NatsServer\Logs\nats-server.log`

В ОС Linux

`/var/log/Acronis/NatsServer/nats-server.log`

Такое переполнение хранилища может привести к нарушению связи между сервисами и критическим сбоям в продукте (например, прекратится отправка уведомлений на электронную почту и работа счётчиков лицензий). При этом часть событий может быть утеряна, так как новые события будут отброшены на стороне сервисов-отправителей, а механизмы повторной отправки (retry) будут недоступны.

Чтобы этого избежать, увеличьте объём хранилища JetStream в конфигурационном файле NATS Server. Для этого выполните следующие действия:

1. Откройте конфигурационный файл

   В ОС Windows:

   `C:\Program Files\Acronis\NatsServer\nats.cfg`

   В ОС Linux:

   `/usr/lib/Acronis/NatsServer/nats.cfg`

2. В блоке настроек `jetstream` замените значение параметра `max_file_store`, указав вместо `10gb` требуемое значение (например, `50gb`). Значение зависит от индивидуальных условий использования Кибер Бэкап.

3. Перезапустите службу с помощью команд:

   В ОС Windows:

   ```
   net stop asm
   net start asm
   ```

   В ОС Linux:

   ```
   systemctl restart acronis_asm
   ```

Примечание

Если данная настройка проводится после возникновения ошибки, необходимо после увеличения размера хранилища NATS вручную перезапустить пропущенные из-за сбоя операции.

Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL

Требования к оборудованию

Машина для сервера управления

Для работы сервера управления необходимы следующие ресурсы:

- как минимум 6 ядер ЦП (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 12 ядер);
- как минимум 16 ГБ ОЗУ (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 32 ГБ);

- не менее 150 ГБ дискового пространства на SSD-диске (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется не менее 300 ГБ);
- подключение к сети, поддерживающее скорость передачи данных от 30 МБ/с (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 50 МБ/с).

Важно

Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Linux.

Машина для PostgreSQL

Для работы СУБД PostgreSQL и размещения баз данных сервера управления необходимы следующие ресурсы:

- как минимум 4 ядра ЦП (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер);
- как минимум 16 ГБ ОЗУ (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 32 ГБ);
- не менее 200 ГБ дискового пространства на SSD-диске (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется не менее 300 ГБ);
- подключение к сети, поддерживающее скорость передачи данных от 30 МБ/с (для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 50 МБ/с).

Важно

Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Linux.

Рекомендуемая конфигурация продукта Кибер Бэкап

В продукте Кибер Бэкап, развернутом на оборудовании с описанными выше характеристиками, рекомендуется:

- Использовать не более 8 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства).

  Для установок Кибер Бэкап с большим количеством контролируемых ресурсов рекомендуется

добавлять лицензии до регистрации агентов и добавления устройств.

- Добавлять не более 20 000 почтовых ящиков или 8 000 других устройств (физических и виртуальных машин, баз данных и других ресурсов, отображаемых в веб-консоли Кибер Бэкап в разделе **Устройства**).

  Добавить до 60 000 почтовых ящиков или до 20 000 ВМ можно при соблюдении дополнительных условий (см. разделы *Резервное копирование больших объемов данных* и *Предельное количество виртуальных машин для резервного копирования*).

- Добавлять не более 50 виртуальных устройств (virtual appliance).
- Включать в общий план не более 100 устройств (общий план включает в себя отдельные устройства), для большего количества устройств используйте групповые планы.
- Включать в групповой план не более 500 устройств (групповой план включает в себя группы устройств).
- Создавать не более 500 общих и групповых планов.
- Выполнять не более 500 одновременных операций резервного копирования и восстановления.
- Создавать не более 500 отделов.
- Использовать не более 10 уровней в иерархии отделов.
- Создавать в отделе не более 300 подотделов одного уровня.

Кроме того, общее количество записей в таблице `resources` БД службы учетных записей (Account Server) не должно превышать 100 000. Чем ближе общее количество записей к этой границе, тем ниже производительность сервера управления.

Важно

При несоблюдении этих рекомендаций производительность сервера управления может заметно снизиться.

Примечание

Реальная производительность сервера управления зависит от профиля нагрузки. Например, в случае, когда виртуальные машины размещены в кластерах, включающих в себя большое количество серверов, производительность может быть значительно меньше, чем в случае, когда серверы не объединены в кластеры или кластеры содержат небольшое количество серверов.

Дополнительная настройка

Дополнительная настройка машин для сервера управления и СУБД PostgreSQL

Для обеспечения высокой производительности сервера управления и СУБД параметрам, ограничивающим использование ресурсов ОС, необходимо назначить достаточно большие значения. Например, на машине с ОС CentOS 7 это можно сделать следующим образом:

1. В конфигурационный файл `/etc/sysctl.conf` добавьте следующие строки:

```
fs.file-max = 6553500
kernel.pid_max = 4194303
kernel.threads-max = 4194303
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.ip_local_port_range = 32768 60999
net.core.somaxconn = 4096
net.ipv4.tcp_max_syn_backlog = 4096
net.core.netdev_max_backlog = 16384
```

2. В конфигурационный файл `/etc/security/limits.conf` добавьте следующие строки:

```
* soft nproc 65535
* hard nproc 65535
* soft nofile 65535
* hard nofile 65535
```

> **Примечание**
>
> Параметры, указанные в файлах в каталоге `/etc/security/limits.d/`, могут переопределять параметры, указанные в файле `/etc/security/limits.conf`.

3. Перезагрузите машину:

```
reboot
```

Дополнительная настройка СУБД PostgreSQL

Для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется изменить ряд параметров в конфигурационном файле `postgresql.conf`:

```
<...>
max_connections = 600
shared_buffers = [4-8]GB [~20-25% от ОЗУ]
work_mem = 16MB
checkpoint_timeout = 20min
random_page_cost = 1.2
effective_cache_size = 16GB [~50% от ОЗУ]
autovacuum_vacuum_scale_factor = 0.05
autovacuum_analyze_scale_factor = 0.02
statement_timeout = 1800000
idle_session_timeout = 1800000
<...>
```

Примечание

Минимальное значение параметра `max_connections` — 200, рекомендуемое значение для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств — 600.

Подробнее о параметрах настройки СУБД см. в официальной документации PostgreSQL.

После изменения параметров необходимо перезагрузить PostgreSQL, например:

```
systemctl restart postgresql-15
```

Дополнительная настройка продукта Кибер Бэкап

Для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется увеличить лимиты на количество одновременно открытых файлов для служб сервера управления и изменить уровень детализации сообщений в журналах событий с `DEBUG` на `INFO`.

Например, если сервер управления установлен на машину с ОС CentOS 7, лимит на количество одновременно открытых файлов для службы acronis_asm и уровень детализации сообщений в журналах можно изменить следующим образом:

1. Узнайте путь к скрипту запуска службы acronis_asm, просмотрев ее unit-файл:

   ```
   cat /etc/systemd/system/acronis_asm.service
   <...>
   ExecStart=/usr/sbin/acronis_asm
   <...>
   ```

2. Задайте новый лимит в скрипте запуска службы `/usr/sbin/acronis_asm`, заменив строку

   ```
   ulimit -n 1024
   ```

   на

   ```
   ulimit -n 10240
   ```

   и сохранив изменение.

3. Измените уровень детализации сообщений в файлах `/usr/lib/Acronis/AccountServer/account_server.json` и `/usr/lib/Acronis/BackupManager/backup_manager.yml`:

   ```
   ...
     chronica:
       level: ”INFO”
   ...
   ```

4. Перезапустите службу:

   ```
   systemctl restart acronis_asm
   ```

Настройка NATS для высоконагруженных конфигураций

При развёртывании Кибер Бэкап в инфраструктуре со значительным объёмом событий по стримам NATS стандартного размера хранилища в 10 ГБ может быть недостаточно. При достижении этого лимита в журнале фиксируется ошибка:

```
[ERR] JetStream resource limits exceeded for server
```

Журнал находится в следующем файле: `/var/log/Acronis/NatsServer/nats-server.log`.

Такое переполнение хранилища может привести к нарушению связи между сервисами и критическим сбоям в продукте (например, прекратится отправка уведомлений на электронную почту и работа счётчиков лицензий). При этом часть событий может быть утеряна, так как новые события будут отброшены на стороне сервисов-отправителей, а механизмы повторной отправки (retry) будут недоступны.

Чтобы этого избежать, увеличьте объём хранилища JetStream в конфигурационном файле NATS Server. Для этого выполните следующие действия:

1. Откройте конфигурационный файл `/usr/lib/Acronis/NatsServer/nats.cfg`.

2. В блоке настроек `jetstream` замените значение параметра `max_file_store`, указав вместо `10gb` требуемое значение (например, `50gb`). Значение зависит от индивидуальных условий использования Кибер Бэкап.
3. Перезапустите службу:

```
systemctl restart acronis_asm
```

Примечание

Если данная настройка проводится после возникновения ошибки, необходимо после увеличения размера хранилища NATS вручную перезапустить пропущенные из-за сбоя операции.

Сервер управления на машине с ОС Windows, использующий СУБД Microsoft SQL Server

Требования к оборудованию

Машина для сервера управления

Для работы сервера управления необходимы следующие ресурсы:

- как минимум 6 ядер ЦП (для установок продукта Кибер Бэкап с большим количеством агентов и виртуальных устройств рекомендуется 8 ядер),
- 16 ГБ ОЗУ,
- не менее 150 ГБ дискового пространства.

Важно

Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Windows.

Машина для Microsoft SQL Server

Для работы СУБД Microsoft SQL Server и размещения баз данных сервера управления необходимы следующие ресурсы:

- 4 ядра ЦП,
- 16 ГБ ОЗУ,
- не менее 100 ГБ дискового пространства.

Важно

Для работы операционной системы необходимы дополнительные ресурсы, количество которых зависит от версии и редакции используемой ОС Windows.

Рекомендуемая конфигурация продукта Кибер Бэкап

В продукте Кибер Бэкап, развернутом на оборудовании с описанными выше характеристиками, рекомендуется:

- Использовать не более 8 000 лицензий (для повышения производительности рекомендуется использовать одну корпоративную лицензию, в которую включены все необходимые агенты и виртуальные устройства).

  Для установок Кибер Бэкап с большим количеством контролируемых ресурсов рекомендуется добавлять лицензии до регистрации агентов и добавления устройств.
- Добавлять не более 8 000 устройств (физических и виртуальных машин, почтовых ящиков, баз данных и других ресурсов, отображаемых в веб-консоли Кибер Бэкап в разделе **Устройства**).
- Добавлять не более 50 виртуальных устройств (virtual appliance).
- Включать в общий план не более 100 устройств (общий план включает в себя отдельные устройства).
- Включать в групповой план не более 500 устройств (групповой план включает в себя группы устройств).
- Создавать не более 500 общих и групповых планов.
- Выполнять не более 500 одновременных операций резервного копирования и восстановления.
- Создавать не более 500 отделов.
- Использовать не более 10 уровней в иерархии отделов.
- Создавать в отделе не более 300 подотделов одного уровня.

Кроме того, общее количество записей в таблице `resources` БД службы учетных записей (Account Server) не должно превышать 60 000. Чем ближе общее количество записей к этой границе, тем ниже производительность сервера управления.

Важно

При несоблюдении этих рекомендаций производительность сервера управления может заметно снизиться.

Примечание

Реальная производительность сервера управления зависит от профиля нагрузки. Например, в случае, когда виртуальные машины размещены в кластерах, включающих в себя большое количество серверов, производительность может быть значительно меньше, чем в случае, когда серверы не объединены в кластеры или кластеры содержат небольшое количество серверов.

Дополнительная настройка

Дополнительная настройка машины для сервера управления

- Количество портов, входящих в диапазон динамических портов для протокола TCP, должно быть в 1,5-2 раза больше общего количества агентов и виртуальных устройств, зарегистрированных в Кибер Бэкап.

  Текущий диапазон динамических портов можно просмотреть с помощью команды

  ```
  netsh int ipv4 show dynamicport tcp
  ```

  Например:

  ```
  netsh int ipv4 show dynamicport tcp


  Protocol tcp Dynamic Port Range
  ---------------------------------
  Start Port      : 49152
  Number of Ports : 16384
  ```

  Задать новый диапазон динамических портов можно с помощью команды

  ```
  netsh int ipv4 set dynamicport tcp start=<start_port> num=<number_of_ports>
  ```

  где `<start_port>` задает начальный порт, а `<number_of_ports>` — количество портов.

- Антивирусное ПО может замедлять работу сервера управления. В таком случае нужно настроить антивирус.

Настройка NATS для высоконагруженных конфигураций

При развёртывании Кибер Бэкап в инфраструктуре со значительным объёмом событий по стримам NATS стандартного размера хранилища в 10 ГБ может быть недостаточно. При достижении этого лимита в журнале фиксируется ошибка:

```
[ERR] JetStream resource limits exceeded for server
```

Журнал находится в следующем файле: `C:\ProgramData\Acronis\NatsServer\Logs\nats-server.log`.

Такое переполнение хранилища может привести к нарушению связи между сервисами и критическим сбоям в продукте (например, прекратится отправка уведомлений на электронную почту и работа счётчиков лицензий). При этом часть событий может быть утеряна, так как новые события будут отброшены на стороне сервисов-отправителей, а механизмы повторной отправки (retry) будут недоступны.

Чтобы этого избежать, увеличьте объём хранилища JetStream в конфигурационном файле NATS Server. Для этого выполните следующие действия:

1. Откройте конфигурационный файл `C:\Program Files\Acronis\NatsServer\nats.cfg`.
2. В блоке настроек `jetstream` замените значение параметра `max_file_store`, указав вместо `10gb` требуемое значение (например, `50gb`). Значение зависит от индивидуальных условий использования Кибер Бэкап.
3. Перезапустите службу:

   ```
   net stop asm
   net start asm
   ```

Примечание

Если данная настройка проводится после возникновения ошибки, необходимо после увеличения размера хранилища NATS вручную перезапустить пропущенные из-за сбоя операции.

Поддержка файловых систем

Агент защиты может создать резервную копию любой файловой системы, доступной из операционной системы, в которой установлен агент. Например, агент для Windows может выполнить резервное копирование и восстановление файловой системы ext4, если соответствующий драйвер установлен в Windows.

В следующей таблице представлена сводная информация о файловых системах, в отношении которых можно выполнять резервное копирование и восстановление. Ограничения применяются как к агентам, так и к загрузочным носителям.

Файловая система	Поддержка			Ограничения
	Агенты	Загрузочный носитель WinPE	Загрузочные носители на основе Linux	
FAT16/32	Все агенты	+	+	Без ограничений
NTFS		+	+	
ext2/ext3/ext4		+	+	
JFS	Агент для Linux	—	+	• Файлы невозможно исключить из резервной копии диска. • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование.
ReiserFS3		—	+	
ReiserFS4		—	+	• Файлы невозможно исключить из резервной копии диска. • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование. • Невозможно изменить размер томов при выполнении восстановления.
ReFS	Все агенты	+	+	• Файлы невозможно исключить из резервной копии диска. • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование. • Невозможно изменить размер томов при выполнении восстановления. • Невозможно восстановить файлы на диски с ReFS при использовании загрузочного носителя на основе Linux.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Файловая система	Поддержка			Ограничения
	Агенты	Загрузочный носитель WinPE	Загрузочные носители на основе Linux	
XFS	Все агенты	+	+	• Файлы невозможно исключить из резервной копии диска. • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование. • Невозможно изменить размер томов при выполнении восстановления. • Восстановление файлов из резервной копии, которая хранится на ленточном накопителе, не поддерживается.
Linux SWAP	Агент для Linux	—	+	Без ограничений
exFAT	Все агенты	+	+ Если резервная копия хранится в файловой системе exFAT, загрузочный носитель невозможно использовать для восстановления	• Поддерживается только резервное копирование дисков/томов. • Файлы невозможно исключить из резервной копии. • Отдельные файлы невозможно восстановить из резервной копии. • Невозможно изменить размер томов при выполнении восстановления.

Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами. Посекторное резервное копирование возможно для любой файловой системы, которая:

- основана на блоках;

- занимает один диск;
- имеет стандартную схему разделов MBR/GPT.

Если файловая система не соответствует этим требованиям, процесс резервного копирования завершится сбоем.

Дедупликация данных

ОС Windows Server позволяет включить функцию дедупликации данных для тома NTFS. Дедупликация данных дает возможность уменьшить объем используемого пространства тома путем однократного сохранения повторяющихся фрагментов файлов на томе.

Предусмотрена возможность создавать резервные копии и восстанавливать тома с включенной дедупликацией данных на уровне диска без каких-либо ограничений. Поддерживается резервное копирование на уровне файлов (за исключением использования поставщика VSS). Для восстановления файлов из резервной копии диска запустите виртуальную машину из резервной копии или *подключите резервную копию* на машине под управлением Windows Server и скопируйте файлы с подключенного тома.

Функциональные средства дедупликации данных Windows Server не имеют никакого отношения к функциональным средствам дедупликации Кибер Бэкапа.

Настройки прокси-сервера

Агенты защиты могут передавать данные через прокси-сервер HTTP/HTTPS. Сервер должен функционировать через HTTP-тоннель без сканирования или изменения трафика HTTP. Промежуточные прокси-серверы не поддерживаются.

Windows

Если прокси-сервер настроен в Windows (**Панель управления** → **Свойства браузера** → **Подключения**), то программа установки считает настройки прокси-сервера из реестра и использует их автоматически. Кроме того, можно задать настройки прокси-сервера во время установки (см. *Установка агентов*) или указать их заранее, используя процедуру, описанную ниже. С помощью той же процедуры эти параметры можно изменить после установки.

Указание параметров прокси-сервера в Windows:

1. Создайте новый текстовый документ и откройте его в текстовом редакторе, например Notepad.
2. Скопируйте и вставьте в этот файл следующие строки:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. Замените `proxy.company.com` именем хоста или IP-адресом прокси-сервера, а `000001bb` — шестнадцатеричным значением номера порта. Например, `000001bb` соответствует номеру порта 443.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо строк `proxy_login` и `proxy_password` укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните документ с именем **proxy.reg**.
6. Запустите файл от имени администратора.
7. Подтвердите изменение реестра Windows.
8. Если агент защиты еще не установлен, то можно установить его сейчас. В противном случае можно перезапустить агент (см. п. 14).
9. Откройте файл `%programdata%\Acronis\Agent\etc\aakore.yaml` в текстовом редакторе.
10. Найдите раздел `env` или создайте его и добавьте следующие строки:

```
env:
http-proxy: proxy_login:proxy_password@proxy_address:port
https-proxy: proxy_login:proxy_password@proxy_address:port
```

11. Замените `proxy_login` и `proxy_password` учетными данными прокси-сервера, а `proxy_address:port` - адресом и номером порта прокси-сервера.
12. В меню **Пуск** нажмите **Выполнить**, введите: `cmd` и нажмите **ОК**.
13. Перезапустите службу aakore, используя следующие команды:

```
net stop aakore
net start aakore
```

14. Перезапустите агент, используя следующие команды:

```
net stop mms
net start mms
```

Linux

Запустите файл установки с параметрами `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`. Чтобы изменить параметры прокси-сервера после установки, используйте описанную ниже процедуру.

Указание параметров прокси-сервера в Linux:

1. Откройте файл `/etc/Acronis/Global.config` в текстовом редакторе.
2. Выполните одно из следующих действий:
   - Если параметры прокси-сервера были заданы во время установки агента, найдите следующий раздел:

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - В противном случае скопируйте приведенные выше строки и вставьте в файл между тегами `<registry name="Global">...</registry>`.
3. Замените `АДРЕС` новым именем хоста или IP-адресом прокси-сервера, а `ПОРТ` — номером порта в десятичном формате.
4. Если на прокси-сервере необходимо пройти аутентификацию, вместо дескрипторов `ИМЯ ВХОДА` и `ПАРОЛЬ` укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
5. Сохраните файл.
6. Откройте файл `/opt/acronis/etc/aakore.yaml` в текстовом редакторе.
7. Найдите раздел `env` или создайте его и добавьте следующие строки:

```
env:
http-proxy: proxy_login:proxy_password@proxy_address:port
https-proxy: proxy_login:proxy_password@proxy_address:port
```

8. Замените `proxy_login` и `proxy_password` учетными данными прокси-сервера, а `proxy_address:port` - адресом и номером порта прокси-сервера.
9. Перезапустите службу aakore, используя следующую команду:

```
sudo service aakore restart
```

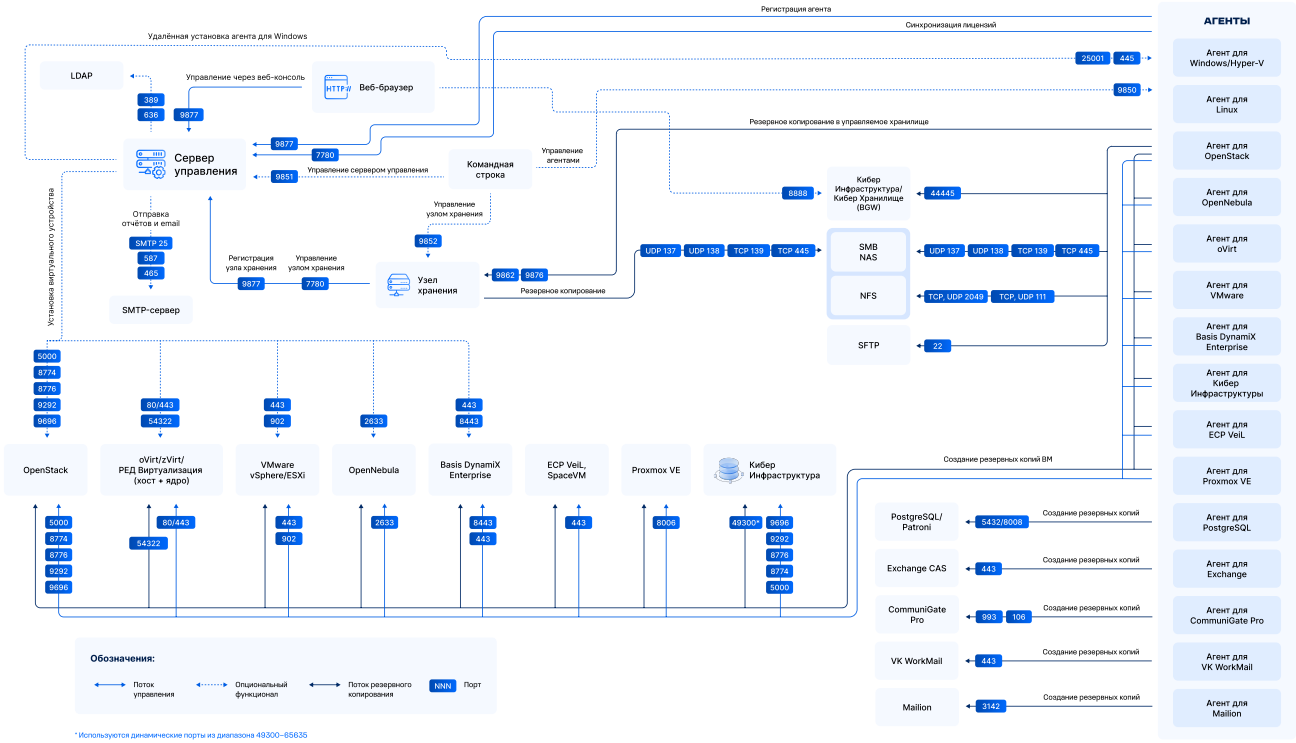
10. Перезапустите агент, выполнив следующую команду в любом каталоге:

```
sudo service acronis_mms restart
```

Развертывание Кибер Бэкап

Развертывание Кибер Бэкап включает в себя установку ряда программных компонентов, которые описаны в разделе *Компоненты*.

На схеме ниже показано взаимодействие основных компонентов продукта.



Описание подключений по указанным портам приведено в Базе знаний.

Установка сервера управления

Установка в ОС Windows

Перед установкой сервера управления убедитесь, что машина соответствует *системным требованиям*.

Установка сервера управления

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Не меняйте настройку по умолчанию **Установите агент защиты и сервер управления**.
5. Выполните любое из следующих действий:

   - Нажмите **Установить**.

     Это самый легкий способ установить продукт. Для большинства параметров установки будут использоваться значения по умолчанию.

     По умолчанию устанавливаются следующие компоненты:

     - Сервер управления
     - Компоненты для удаленной установки
     - Агент для Windows
     - Другие агенты (агент для Hyper-V, агент для Exchange, агент для SQL и агент для Active Directory), если на машине обнаружен соответствующий гипервизор или приложение
     - Мастер создания загрузочных носителей
     - Программа командной строки
     - Мониторинг Защиты Данных

   - Щёлкните **Настройка параметров установки**, чтобы настроить программу установки.

     Можно будет выбрать компоненты для установки и указать дополнительные параметры. Дополнительную информацию см. в разделе *Настройка параметров установки*.

   - Щёлкните **Создать MST- и MSI-файлы для автоматической установки**, чтобы извлечь пакеты установки. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **Создать**. Для этой процедуры не требуется никаких дополнительных шагов.

Чтобы развернуть агенты через групповую политику, см. раздел *Развертывание агентов с использованием групповой политики*.

6. Приступите к установке.
7. После завершения установки нажмите кнопку **Закрыть**.

Что дальше

- *Настройка параметров установки в ОС Windows*

При необходимости настройте размер хранилища NATS для высоконагруженных конфигураций (см. *Рекомендуемые конфигурации оборудования для сервера управления*).

Настройка параметров установки в ОС Windows

В этом разделе описаны настройки, которые можно изменить при установке.

Общие параметры

- Устанавливаемые компоненты

Компонент	Описание
Сервер управления	Сервер управления — это центр управления всеми резервными копиями.
Агент для Windows	Этот агент создает резервную копию дисков, томов и файлов. Он устанавливается на машинах Windows. Он устанавливается в любом случае (не подлежит выбору).
Агент для Hyper-V	Этот агент создает резервную копию виртуальных машин Hyper-V. Он устанавливается на хостах Hyper-V. Если этот компонент выбран, и на машине обнаружена роль Hyper-V, он будет установлен.
Агент для SQL	Этот агент создает резервную копию баз данных SQL Server. Он устанавливается на машинах с Microsoft SQL Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для Exchange	Этот агент создает резервную копию баз данных и почтовых ящиков Exchange. Он устанавливается на машинах с ролью почтового ящика Microsoft Exchange Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Компонент	Описание
Агент для Active Directory	Этот агент создает резервную копию данных доменных служб Active Directory. Он устанавливается на контроллерах домена. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для VMware (Windows)	Этот агент создает резервную копию виртуальных машин VMware. Он устанавливается на виртуальных машинах Windows с сетевым доступом к vCenter Server. Если этот компонент выбран, он будет установлен.
Агент для Oracle	Этот агент создает резервную копию баз данных Oracle. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.
Агент для PostgreSQL	Этот агент создает резервную копию баз данных PostgreSQL. Если этот компонент выбран, он будет установлен.
Узел хранения	Этот компонент используется для организации управляемых хранилищ и дедупликации резервных копий. Он устанавливается на машину с агентом для Windows.
Мониторинг Защиты Данных	Этот компонент позволяет пользователю отслеживать выполнение запущенных заданий в области уведомлений, приостанавливать запуск планов защиты, устанавливать особые пароли для резервных копий машины. Он устанавливается на машинах Windows. Если этот компонент выбран, он будет установлен.
Программа командной строки	Кибер Бэкап поддерживает интерфейс командной строки с утилитой acrocmd. acrocmd не содержит никаких инструментов, которые физически выполняют команды. Она просто обеспечивает интерфейс командной строки для компонентов Кибер Бэкап — агентов и сервера управления. Если этот компонент выбран, он будет установлен.

- Папка, в которую будет установлен продукт.
- Учетная запись, с использованием которой будут запускаться службы.

  Можно выбрать один из следующих вариантов:

  - **Использовать учетные записи пользователя службы** (по умолчанию для службы агента)

    Учетные записи пользователя услуги — это системные учетные записи Windows, которые используются для запуска служб. Преимущество этой настройки состоит в том, что политики безопасности домена не влияют на права пользователей этих учетных записей. По умолчанию агент запускается в учетной записи **Локальная система**.

  - **Создать учетную запись** (по умолчанию для службы сервера управления и службы узла хранения)

Учетные записи будут иметь имена **Agent User**, **CMS User** и **CSN User** для агента, сервера управления и служб узла хранения соответственно.

- **Использовать следующую учетную запись**

  При установке продукта на контроллер домена программа установки предложит указать существующие учетные записи (или ту же учетную запись) для каждой службы. В целях безопасности программа установки не может автоматически создавать учетные записи на контроллере домена.

  Эта настройка также позволяет использовать на сервере управления существующий сервер Microsoft SQL, установленный на другой машине, а также проверку подлинности Windows для SQL Server.

При выборе параметра **Создать учетную запись** или **Использовать следующую учетную запись** убедитесь, что политики безопасности домена не повлияют на права соответствующих учетных записей. Если права пользователя не были заданы для учетной записи при установке, данный компонент может работать неправильно или вообще не работать.

Права, требуемые для учетной записи входа

На машине Windows агент запускается как Managed Machine Service (MMS). Для надлежащей работы агента учетная запись, под которой запускается агент, должна иметь специальные права. Поэтому пользователю MMS необходимо назначить следующие права:

1. Учетная запись должна входить в группы **Операторы архива** и **Администраторы**. На контроллере домена пользователь должен входить в группу **Администраторы домена**.
2. Предоставляется разрешение **Полный доступ** в отношении папки `%PROGRAMDATA%\Acronis` и ее подпапок.
3. Разрешение **Полный доступ** в отношении определенных разделов реестра в следующем разделе: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Назначены следующие права пользователя:
   - Вход в качестве службы
   - Настройка квот памяти для процесса
   - Замена маркера уровня процесса
   - Изменение параметров среды изготовителя

Пользователь узла хранения должен иметь права локального администратора на машине с установленным узлом хранения Киберпротект.

Назначение прав пользователя

Ниже описаны инструкции по назначению прав пользователя (в этом примере используется право пользователя **Вход в качестве службы**, однако все действия идентичны и для других прав пользователя):

1. Войдите на компьютер с учетной записью с правами администратора.
2. В разделе **Панель управления** откройте **Инструменты Windows** (или щёлкните `Win+R`, введите `control admintools` и нажмите клавишу `Ввод`), затем откройте **Локальная политика безопасности**.
3. Разверните **Локальные политики** и щёлкните **Назначение прав пользователя**.
4. В правой панели щёлкните правой кнопкой мыши **Вход в качестве службы** и выберите **Свойства**.
5. Чтобы добавить нового пользователя, нажмите кнопку **Добавить пользователя или группу…**.
6. В окне выбора пользователей, компьютеров, учетных записей служб или групп найдите пользователя, которого необходимо ввести, и щёлкните **ОК**.
7. Чтобы сохранить изменения, щёлкните **ОК** в разделе **Свойства** (**Вход в качестве службы**).

> **Важно**
>
> Убедитесь, что пользователь, добавленный в правило **Вход в качестве службы**, не указан в политике **Отказать во входе в качестве службы** в разделе **Локальная политика безопасности**.

Обратите внимание, что не рекомендуется вручную менять учетные записи входа после окончания установки.

Установка сервера управления

- База данных, которая должна использоваться сервером управления. По умолчанию используется встроенная база данных SQLite.

  Можно выбрать любую из указанных ниже версий Microsoft SQL Server:

  - Microsoft SQL Server 2016,
  - Microsoft SQL Server 2017 (в Windows),
  - Microsoft SQL Server 2019 (в Windows),
  - Microsoft SQL Server 2022 (в Windows),
  - Microsoft SQL Server 2025 (в Windows).

  Выбранный экземпляр может использоваться и другими программами.

Если для экземпляра используется имя по умолчанию — **MSSQLSERVER** — необходимо указать только имя машины, на которой расположен этот экземпляр. Если используется настраиваемое имя экземпляра, необходимо указать имя машины и имя экземпляра.

Перед выбором установленного на другой машине экземпляра убедитесь, что на этой машине включены служба обозревателя SQL Server и протокол TCP/IP. Инструкции по запуску службы браузера SQL Server см. на странице http://msdn.microsoft.com/en-us/library/ms189093.aspx. Включить протокол TCP/IP можно с помощью аналогичной процедуры.

- База данных, которая должна использоваться службой сканирования. Служба сканирования может использовать ту же базу данных Microsoft SQL Server, которая указана для сервера управления, или отдельную базу данных PostrgeSQL Server. Службу сканирования невозможно использовать со встроенной базой данных SQLite.
- Порт, который будет использоваться веб-браузером для доступа к серверу управления (по умолчанию 9877) и порт, который будет использоваться для связи между компонентами продукта (по умолчанию 7780). Изменение последнего порта после установки потребует перерегистрации всех компонентов.

  Брандмауэр Windows настраивается автоматически при установке. Если используется другой брандмауэр, убедитесь, что порты открыты как для входящих, так и для исходящих запросов, проходящих через этот брандмауэр.

Установка в Linux

Перед установкой сервера управления убедитесь, что машина соответствует *системным требованиям*.

Подготовка

1. В системе, в которой не используется диспетчер пакетов RPM, необходимо установить этот диспетчер вручную. Как привилегированный пользователь выполните команду (например):

   ```
   apt-get install rpm
   ```

2. Убедитесь в том, что на машине установлены *необходимые пакеты для ОС Linux*.
3. Дайте разрешение на исполнение установочному файлу. Выполните следующую команду:

   ```
   chmod +x CyberBackup_*
   ```

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE ознакомьтесь с разделом *Совместимость с ОС Astra Linux SE* и выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

```
tar --xattrs --xattrs-include=* -xvf CyberBackup_18_64-bit.x86_64.tar
```

2. Запустите файл установки с правами привилегированного пользователя:

```
./CyberBackup_18_64-bit.x86_64
```

3. Обновите образы initramfs:

```
update-initramfs -u -k all
```

4. Перезагрузите систему.

Подготовка СУБД PostgreSQL / Patroni / Jatoba (JaDog)

Если планируется использовать СУБД PostgreSQL или кластерную конфигурацию Jatoba (JaDog) или Patroni для сервера управления, выполните следующие шаги:

1. Установите PostgreSQL на машину, предназначенную для сервера управления, либо на отдельную машину. Для установки можно использовать:

   - PostgreSQL или Postgres Pro версии 14, 15, 16, 17, 18;
   - Platform V Pangolin SE 6.1.7;
   - СУБД Jatoba 5—18;
   - СУБД Tantor 14—17.

   Пример установки PostgreSQL 15 в ОС CentOS 7:

```
yum install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-7-x86_64/pgdg-
↪redhat-repo-latest.noarch.rpm
yum install -y postgresql15-server
/usr/pgsql-15/bin/postgresql-15-setup initdb
systemctl enable postgresql-15
systemctl start postgresql-15
```

2. На машину с PostgreSQL установите пакет `postgresql-contrib`, например:

```
yum -y install postgresql15-contrib
```

Версия пакета должна соответствовать версии PostgreSQL.

3. При установке сервера управления необходимо будет указать учетные данные пользователя с привилегиями LOGIN и SUPERUSER. От его имени будет настроена СУБД PostgreSQL. Если такой пользователь есть, можно использовать его учетные данные. Если такого пользователя нет, зайдите на машину с PostgreSQL от имени администратора и создайте его. Например:

```
sudo -u postgres psql -c "CREATE ROLE cyberbackup WITH LOGIN SUPERUSER PASSWORD
↪'69c64fee29d24024b219578ecd9f5d88';"
```

Для подключения сервера управления к PostgreSQL в процессе установки будет автоматически создан пользователь cyberprotect.

4. Измените конфигурационный файл `postgresql.conf` так, как показано в примерах ниже.

   - PostgreSQL и сервер управления на одной машине.

     ```
     <...>
     listen_addresses = '127.0.0.1'
     max_connections = 600
     password_encryption = scram-sha-256
     <...>
     ```

   - PostgreSQL и сервер управления на разных машинах.

     ```
     <...>
     listen_addresses = '10.10.10.10'
     max_connections = 600
     password_encryption = scram-sha-256
     <...>
     ```

     В этом примере 10.10.10.10 — это IP-адрес машины с PostgreSQL.

Примечание

- Минимальное значение параметра `max_connections` — 200, рекомендуемое значение для установок Кибер Бэкап с большим количеством агентов и виртуальных устройств — 600.
- Подробные сведения о возможных значениях параметра `listen_addresses` см. в документации установленной версии PostgreSQL.

После внесения изменений перезагрузите PostgreSQL. Например:

```
systemctl restart postgresql-15
```

5. Настройте аутентификацию в PostgreSQL для сервера управления.

   1. На машине с PostgreSQL измените файл `pg_hba.conf` так, как показано в примерах.

      - PostgreSQL и сервер управления на одной машине.

        ```
        # TYPE  DATABASE        USER            ADDRESS                 METHOD
        # "local" is for Unix domain socket connections only
        local   all             all                                     peer
        # Cyber Backup connections
        host    all             cyberbackup             127.0.0.1/32            scram-sha-256
        host    all             cyberprotect            127.0.0.1/32            scram-sha-256
        <...>
        ```

        В этом примере cyberbackup — пользователь, с помощью привилегий которого СУБД PostgreSQL будет настроена при установке, а cyberprotect — пользователь, от имени которого сервер управления будет подключаться к PostgreSQL.

      - PostgreSQL и сервер управления на разных машинах.

        ```
        # TYPE  DATABASE        USER            ADDRESS                 METHOD
        # "local" is for Unix domain socket connections only
        local   all             all                                     peer
        # Cyber Backup connections
        host    all             cyberbackup             10.10.10.11/32          scram-sha-
        ↪256
        host    all             cyberprotect            10.10.10.11/32          scram-sha-
        ↪256
        <...>
        ```

        В этом примере cyberbackup — пользователь, с помощью привилегий которого СУБД PostgreSQL будет настроена при установке, а cyberprotect — пользователь, от имени которого сервер управления будет подключаться к PostgreSQL. Кроме того, 10.10.10.11 — IP-адрес машины, предназначенной для сервера управления.

      Примечание

      - Сервер управления не поддерживает локальные подключения к базам данных PostgreSQL через доменные сокеты Unix (тип подключения local в `pg_hba.conf`).

- Сервер управления поддерживает подключения к базам данных PostgreSQL только по протоколу IPv4.
- Кроме метода аутентификации scram-sha-256, сервер управления также поддерживает методы аутентификации md5 и trust.

2. Примените изменения. Например:

```
systemctl reload postgresql-15
```

6. В случае размещения PostgreSQL и сервера управления на разных машинах:
   - брандмауэр должен разрешать подключения с машины, предназначенной для сервера управления, к машине с PostgreSQL через TCP-порт, используемый PostgreSQL (5432 по умолчанию);
   - время на машинах должно быть синхронизировано.

> **Предупреждение**
>
> Не переводите системное время вперед и обратно при работе Кибер Бэкап.

7. Убедитесь, что с машины, предназначенной для сервера управления, можно подключаться к PostgreSQL с учетными данными созданного ранее пользователя.
   - PostgreSQL и сервер управления на одной машине.

```
[root@cb-mn-srv ~]# psql -h 127.0.0.1 -U cyberbackup -d postgres
Пароль пользователя cyberbackup:
psql (15.0)
Введите "help", чтобы получить справку.

postgres=#
```

   - PostgreSQL и сервер управления на разных машинах.

```
[root@cb-mn-srv ~]# psql -h 10.10.10.10 -U cyberbackup -d postgres
Пароль пользователя cyberbackup:
psql (15.0)
Введите "help", чтобы получить справку.

postgres=#
```

Для использования кластерной конфигурации Jatoba (JaDog) или Patroni произведите аналогичную настройку машин PostgreSQL и обратитесь к официальной документации Jatoba и Patroni для настройки кластера. Для установки можно использовать JaDog (Jatoba) версий 4.0 — 4.3 и Patroni версии 3.0 – 3.2.1.

Установка сервера управления

Для установки сервера управления необходимо как минимум 4 ГБ свободного места на диске.

1. Запустите файл установки (файл .i686 или .x86_64) как привилегированный пользователь:

   ```
   ./CyberBackup_19_64-bit.x86_64
   ```

2. Примите условия лицензионного соглашения.
3. [Необязательно] Выберите компоненты, которые требуется установить.

   По умолчанию устанавливаются следующие компоненты:

   - Сервер управления
   - Агент для Linux
   - Мастер создания загрузочных носителей
4. Выберите систему управления базами данных (СУБД) для сервера управления — **SQLite** или **PostgreSQL/Patroni**. По умолчанию выбрана встроенная СУБД SQLite.

   > **Важно**
   >
   > СУБД PostgreSQL / Patroni / Jatoba (JaDog) должна быть подготовлена до установки сервера управления по приведенной выше инструкции.

5. [Для СУБД PostgreSQL / Patroni / Jatoba (JaDog)] Укажите сведения для подключения и аутентификации:

   - **Хост** — IPv4-адрес или DNS-имя машины с PostgreSQL или с балансировщиком нагрузки кластера Patroni или Jatoba (JaDog). По умолчанию установлено значение localhost.
   - **Порт** — порт для подключения к PostgreSQL / Patroni / Jatoba (JaDog). По умолчанию установлено значение 5432.
   - **Пользователь** и **Пароль** — имя и пароль пользователя для подключения к PostgreSQL / Patroni / Jatoba (JaDog). Необходимо указать учетные данные пользователя, который был создан при подготовке СУБД. По умолчанию указан пользователь postgres.

6. Укажите порт, который будет использоваться в веб-браузере для доступа к серверу управления. Значение по умолчанию составляет 9877.
7. Укажите порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию установлено значение 7780.
8. Нажмите кнопку **Далее**, чтобы продолжить установку.

> **Примечание**
>
> Мастер установки может потребовать пакет openjdk-8-jre-headless. Устанавливать его не нужно.

9. По окончании установки выберите **Открыть веб-консоль**, затем нажмите кнопку **Выход**. Веб-консоль Кибер Бэкап откроется в веб-браузере по умолчанию.

При необходимости настройте размер хранилища NATS для высоконагруженных конфигураций (см. *Рекомендуемые конфигурации оборудования для сервера управления*).

Настройка отказоустойчивого кластера

В этом разделе приведены описание типовой архитектуры и пример настройки двухузлового отказоустойчивого кластера для программного обеспечения резервного копирования и восстановления данных Кибер Бэкап в операционной системе Ред ОС 7.3 Муром. В качестве программного обеспечения для поддержания целостности кластера и выполнения сигнальных функций используется Corosync, а для управления ресурсами кластера — Pacemaker.

В разделе описываются общие принципы настройки кластера Pacemaker/Corosync, перечень и рекомендуемые настройки ресурсов кластера для Кибер Бэкап, пример настройки типового двухузлового кластера на физических серверах с выделенной виртуальной машиной-свидетелем.

Подход, используемый в данном разделе, может быть применен как при построении кластеров высокой доступности, расположенных целиком на одной площадке, так и при построении катастрофоустойчивых кластеров, распределенных по нескольким центрам обработки данных.

Данный раздел не является руководством по программному обеспечению Pacemaker/Corosync и не заменяет техническую документацию по указанным продуктам.

Архитектура

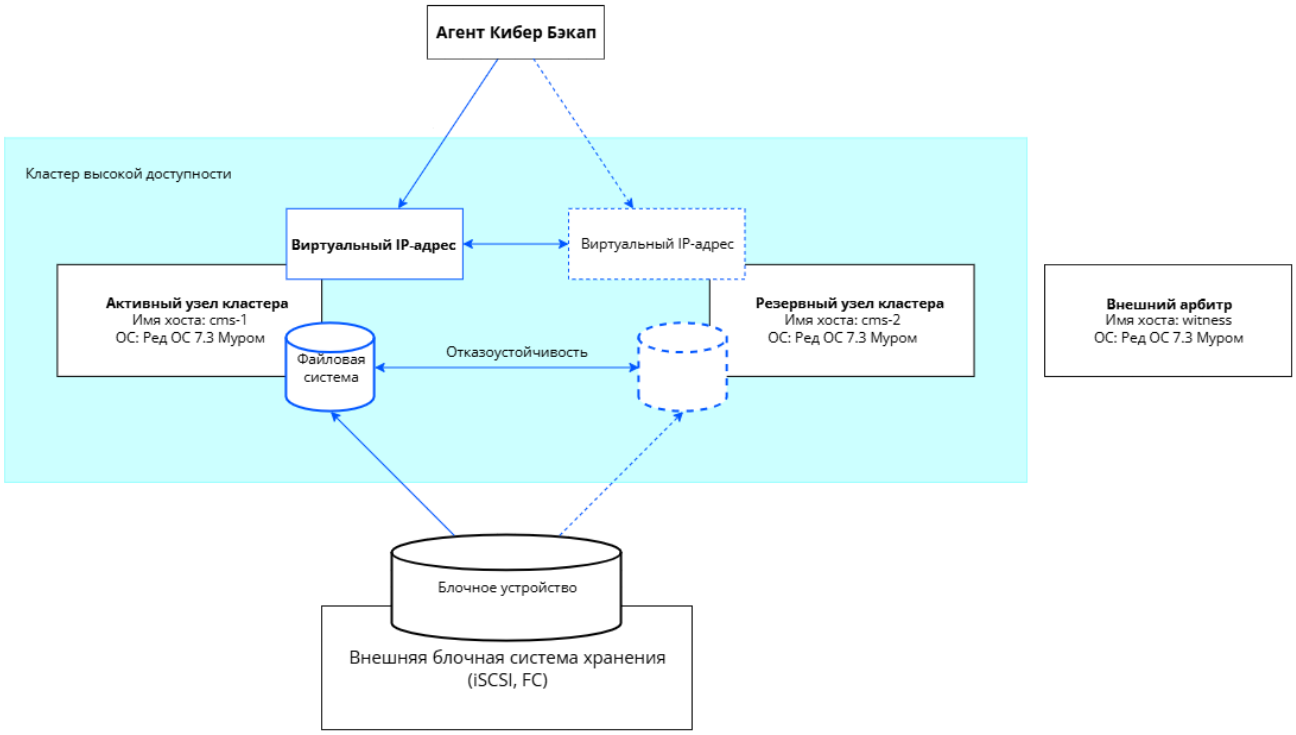
Компоненты кластера

В разделе рассмотрен способ кластеризации Кибер Бэкап, включающий задействование следующих компонентов:

- Два аппаратных сервера с выделенными IPMI-интерфейсами;
- Внешняя блочная система хранения, доступная по протоколу iSCSI;
- Выделенный сервер, предпочтительно виртуализованный для кворумного устройства (так называемый ”свидетель” или ”арбитр”).

Кластер Кибер Бэкап является классическим отказоустойчивым кластером с общими разделяемыми дисками и виртуальным IP-адресом сервиса. Целостность кластера обеспечивается механизмами Stonith с использованием функционала IPMI и защитой от split brain при помощи внешнего арбитра.

Схема компонентов кластера:

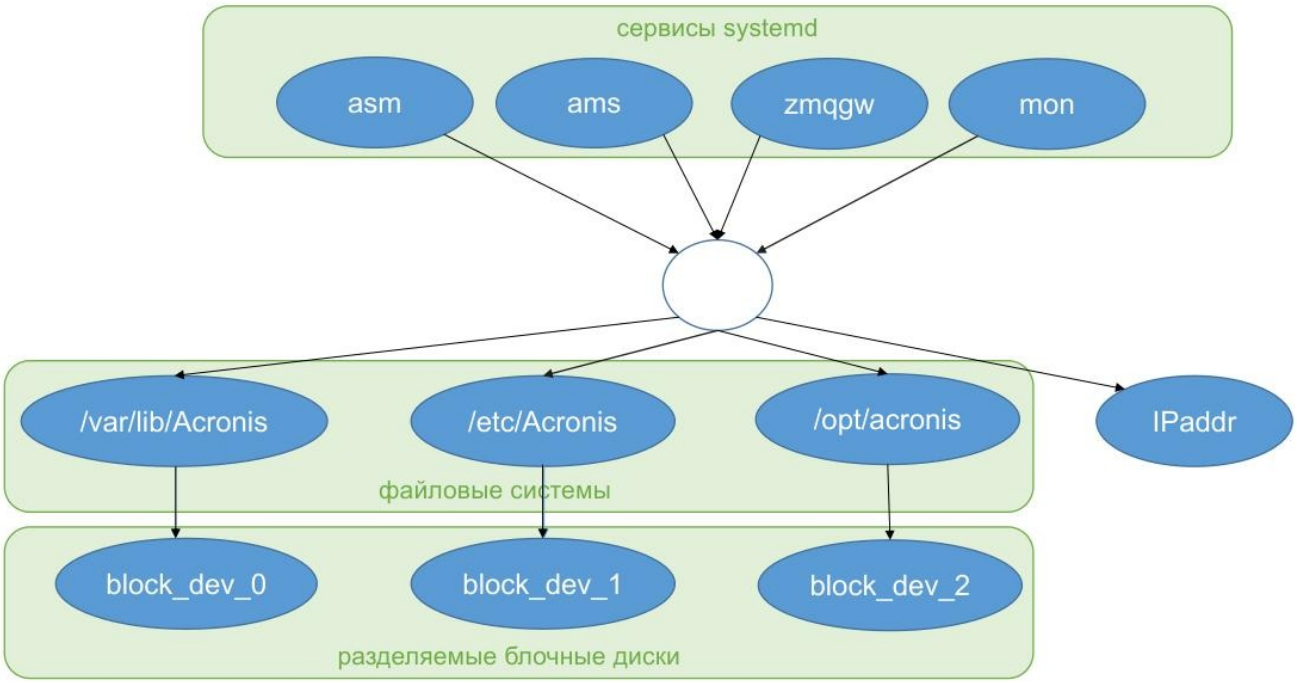


Ресурсы кластера

Для функционирования кластера необходимо настроить следующие типы кластерных ресурсов:

- Разделяемые блочные дисковые устройства;
- Перемещаемые файловые системы;
- Перемещаемый (виртуальный) IP-адрес, также называемый vIP (Virtual IP);
- Службы Кибер Бэкап;
- IPMI-ресурсы.

Дерево зависимостей ресурсов кластера изображено на следующем рисунке.



Развертывание и настройка

Настройка сети

Требования к организации сети

Узлам кластера, IPMI-интерфейсам и внешнему арбитру должны быть назначены статические адреса IPv4. Адреса узлов кластера и перемещаемый IP-адрес должны находиться в одном сегменте сети. Адреса внешнего арбитра и IPMI-интерфейсов могут находиться в отдельных сегментах сети, доступных с использованием сетевой маршрутизации, но также должна быть обеспечена сетевая связность со стороны узлов кластера.

Тип	ОС	Имя хоста	IP-адрес	IPMI-интерфейс	Виртуальный IP-адрес	Описание
Узел кластера	РЕД ОС 7.3.3 x64	cms-1	10.77.44.58/22	10.77.0.58/22	10.77.44.57/22	Первый узел кластера для сервера управления Кибер Бэкап. Вариант установки: ”сервер минимальный”.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Тип	ОС	Имя хоста	IP-адрес	IPMI-интерфейс	Виртуальный IP-адрес	Описание
		cms-2	10.77.44.59/22	10.77.0.59/22		Второй узел кластера для сервера управления Кибер Бэкап. Вариант установки: ”сервер минимальный”.
Арбитр		witness	10.77.44.61/22	—	—	Арбитр с кворумным устройством для предотвращения split brain. Вариант установки: ”сервер минимальный”. Допустимо использование виртуальной машины.

Настройка сетевых интерфейсов

На всех узлах кластера и арбитре настройте статические сетевые адреса, шлюз по умолчанию и адреса серверов имен (файл `/etc/sysconfig/network-scripts/ifcfg-ens3`):

```
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
NAME=ens3
DEVICE=ens3
ONBOOT=yes
IPADDR=10.77.44.58
PREFIX=22
GATEWAY=10.77.44.1
DNS1=10.77.29.101
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
DNS2=10.77.29.10
```

В файл `/etc/hosts` на узлах кластера и арбитре добавьте записи с остальными компонентами кластера, чтобы целостность кластера не зависела от стабильности работы внешних DNS-серверов:

```
10.77.44.57 cms     # Virtual (floating) cluster IP address
10.77.44.58 cms-1   # Node 1 static address
10.77.44.59 cms-2   # Node 2 static address
10.77.44.61 witness # Cluster witness with quorum device
```

Перезагрузите серверы и проверьте:

- Наличие статических адресов на интерфейсах;
- Наличие маршрута по умолчанию;
- Сетевую связность между всеми компонентами кластера.

```
[root@cms-1 network-scripts]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen¬
↪1000
    link/ether 56:6f:93:3c:00:64 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet 10.77.44.58/22 brd 10.77.47.255 scope global noprefixroute ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::546f:93ff:fe3c:64/64 scope link
        valid_lft forever preferred_lft forever

[root@cms-1 ~]# ip route
default via 10.77.44.1 dev ens3 proto static metric 100
10.77.44.0/22 dev ens3 proto kernel scope link src 10.77.44.58 metric 100
```

Подготовка узлов кластера

Установка кластерного программного обеспечения

Установите программное обеспечение для кластера, используя следующую таблицу.

Тип	Имя хоста	Команды

Узел кластера	cms-1	`# dnf update`
		`# dnf install pcs pacemaker corosync corosync-qdevice lsyncd`
		`# dnf install iscsi-initiator-utils`

Узел кластера	cms-2	`# dnf update`
		`# dnf install pcs pacemaker corosync corosync-qdevice lsyncd`
		`# dnf install iscsi-initiator-utils`

Арбитр	witness	`# dnf update` `# dnf install pcs corosync-qnetd`

Отключение SELinux

Для отключения SELinux на узлах кластера и арбитре выполните следующую команду:

```
setenforce 0
```

В конфигурационном файле `/etc/selinux/config` измените значение **enforcing** на **disabled**:

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these three values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Настройка доступа по SSH-ключам

Для root настройте доступ между узлами кластера по SSH-ключам:

```
[root@cms-1 ~]# ssh-copy-id root@cms-2

[root@cms-2 ~]# ssh-copy-id root@cms-1
```

Настройка lsyncd

На первом узле кластера (cms-1) создайте конфигурационные файлы для автоматической двунаправленной синхронизации следующих системных файлов:

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`
- `/etc/security/acronisagent.conf`

Конфигурационный файл `lsyncd` (`/etc/lsyncd.conf`):

```
settings {
    logfile = ”/var/log/lsyncd.log”
}

sync {
    default.rsyncssh,
    source = ”/etc”,
    host = ”cms-2”,
    targetdir = ”/etc”,
    delete = 'false',
    rsync = {
        update = ”true”,
        whole_file = ”true”,
        _extra = {
            ”--include-from=/etc/lsyncd.list”,
            ”--exclude=*”
        }
    }
}

sync {
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
    default.rsyncssh,
    source = ”/etc/security”,
    host = ”cms-2”,
    targetdir = ”/etc/security”,
    delete = 'false',
    rsync = {
        update = ”true”,
        whole_file = ”true”,
        _extra = {
            ”--include=acronisagent.conf”,
            ”--exclude=*”
        }
    }
}
```

Создайте список файлов для синхронизации (`/etc/lsyncd.list`):

```
passwd
shadow
group
```

Перезапустите сервис `lsyncd`:

```
systemctl enable lsyncd --now
```

Выполните аналогичную процедуру на втором узле кластера (cms-2). В конфигурационном файле `/etc/lsyncd.conf` необходимо изменить имя хоста на cms-1.

Настройка кластера

Пользователь hacluster

На узлах кластера и арбитре задайте пароль для пользователя **hacluster**:

```
passwd hacluster
```

Кластерные службы

На узлах кластера добавьте запуск кластерных служб при перезагрузке:

```
systemctl enable pcsd pacemaker corosync
```

Инициализация кластера

На всех узлах кластера и на свидетеле запустите `pscd`:

```
systemctl start pcsd
```

На одном из узлов кластера выполните команды по инициализации кластера:

```
pcs host auth cms-1 cms-2 -u hacluster # Запросит пароль hacluster
pcs cluster setup CyberBackup cms-1 cms-2
pcs cluster enable --all
pcs cluster start --all
```

где `cms-1` и `cms-2` — имена узлов кластера; `CyberBackup` — имя кластера.

Настройка арбитра

Инициализируйте на арбитре кворумное устройство и запустите `pcsd`:

```
[root@witness ~]# pcs qdevice setup model net --enable --start
Quorum device 'net' initialized
quorum device enabled
Starting quorum device...
quorum device started

[root@witness ~]# systemctl enable pcsd --now
Created symlink /etc/systemd/system/multi-user.target.wants/pcsd.service →
/usr/lib/systemd/system/pcsd.service.
```

Активируйте и запустите `corosync-qdevice` на каждом узле кластера:

```
[root@cms-1 ~]# systemctl enable corosync-qdevice
Created symlink /etc/systemd/system/multi-user.target.wants/corosyncqdevice.
service → /usr/lib/systemd/system/corosync-qdevice.service.
```

Для инициализации и настройки кворумного устройства на одном из узлов кластера выполните следующие команды:

```
[root@cms-1 ~]# pcs host auth witness
Username: hacluster
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Password:
witness: Authorized

[root@cms-1 ~]# pcs quorum device add model net host=witness algorithm=ffsplit
Setting up qdevice certificates on nodes...
cms-1: Succeeded
cms-2: Succeeded
Enabling corosync-qdevice...
cms-1: corosync-qdevice enabled
cms-2: corosync-qdevice enabled
Sending updated corosync.conf to nodes...
cms-1: Succeeded
cms-2: Succeeded
cms-1: Corosync configuration reloaded
Starting corosync-qdevice...
cms-2: corosync-qdevice started
cms-1: corosync-qdevice started

[root@cms-1 ~]# pcs quorum status
Quorum information
------------------
Date:                   Thu Nov 16 21:50:29 2023
Quorum provider: corosync_votequorum
Nodes:                  2
Node ID:                1
Ring ID:                1.6a
Quorate:                Yes

Votequorum information
----------------------
Expected votes:     3
Highest expected:   3
Total votes:        3
Quorum:             2
Flags:              Quorate Qdevice

Membership information
----------------------
Nodeid      Votes    Qdevice          Name
1             1        A,V,NMW      cms-1 (local)
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
2          1          A,V,NMW      cms-2
0          1          Qdevice
```

Настройка механизма stonith / fencing

Для обеспечения целостности разделяемых данных в кластере существует механизм, называемый stonith или fencing. В случае сетевой недоступности неисправного узла кластера он всё еще может выполнять доступ к разделяемым данным, поэтому уцелевшая часть кластера должна иметь механизм для предотвращения доступа узла кластера, не отвечающего на запросы. Чаще всего это реализуется с помощью аппаратных средств, например, перезагрузка узла при помощи интерфейса управления IPMI, временного прерывания подачи питания через управляемые устройства распределения питания PDU (Power Distribution Unit), отключение портов узла на LAN/SAN-коммутаторах и т.п. Возможно использование одновременно несколько fencing-методов.

> **Важно**
>
> Промышленная эксплуатация кластера без настроенного механизма stonith / fencing недопустима и ведет к риску порчи данных.

Ниже приведен вариант настройки fencing с использованием IPMI-совместимых модулей управления физического сервера.

1. Включите механизм fencing:

```
pcs property set stonith-enabled=true
```

2. Установите на узлы кластера пакет с fencing-агентом:

```
dnf install fence-agents-ipmilan
```

3. Для каждого узла кластера создайте fencing-ресурс:

```
pcs stonith create cms1_ipmi fence_ipmilan pcmk_host_list=”cms-1” \
    ip=10.77.0.58 username=testuser password=acd123 privlvl=operator \
    lanplus=1 op monitor interval=60s

pcs stonith create cms2_ipmi fence_ipmilan pcmk_host_list=”cms-2” \
    ip=10.77.0.59 username=testuser password=acd123 privlvl=operator \
    lanplus=1 op monitor interval=60s
```

Все параметры, доступные при создании fencing-ресурса, можно уточнить следующей командой:

```
pcs stonith describe fence_ipmilan
```

4. Создайте правила, запрещающие fencing-ресурсу для отключения узла запускаться на этом же самом узле:

```
pcs constraint location cms1_ipmi avoids cms-1
pcs constraint location cms2_ipmi avoids cms-2
```

5. Работа механизма fencing должна быть протестирована как отдельно, так и при тестировании отработки сценариев отказа кластером. Ручное тестирование интеграции возможно с использованием следующей команды, которая должна перезагрузить сервер cms-1 с использованием IPMI-интерфейса:

```
[root@cms-2 ~]# stonith_admin --reboot cms-1
```

В тестовых кластерах, которые не содержат данных, представляющих ценность и используются только с целью проверки совместимости или отработки какой-либо гипотезы, допустимо отключение механизма fencing. Такие кластеры могут быть целиком реализованы внутри виртуальных машин и не иметь работающего механизма fencing. В таком случае его необходимо отключить:

```
pcs property set stonith-enabled=false
```

Монтирование блочных iSCSI-устройств

Выполните подключение блочных iSCSI-устройств на одном из узлов кластера. Сканируйте доступные из системы устройства с именем хоста `iscsi-tgt`.

```
[root@cms-1 ~]# iscsiadm --mode discovery --type st --portal iscsi-tgt --login
10.77.44.62:3260,1 iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c
Logging in to [iface: default, target: iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c, portal: 10.77.44.62,3260]
Login to [iface: default, target: iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c, portal: 10.77.44.62,3260] successful.
```

Проверьте наличие активных iSCSI-сессий до целевого устройства и отключите автоматическое подключение iSCSI-клиентом дисков с внешней системы хранения:

```
[root@cms-2 ~]# iscsiadm --mode session
tcp: [1] 10.77.44.62:3260,1 iqn.2003-01.org.linux-iscsi.iscsitgt.
x8664:sn.bfbc1ebb624c (non-flash)

[root@cms-2 ~]# iscsiadm --mode node --portal iscsi-tgt --op update \
    --name node.startup --value manual
```

Проверьте доступность новых блочных устройств:

```
[root@cms-1 ~]# lsblk
NAME     MAJ:MIN  RM  SIZE  RO  TYPE  MOUNTPOINTS
...
sdc             8:32           0     5G         0    disk
sdd             8:48           0     100G    0    disk
sde             8:64           0     20G       0    disk
...
```

Отформатируйте новые диски в `ext4` и смонтируйте файловые системы:

```
[root@cms-1 ~]# mkfs.ext4 -m 0 -L etc /dev/sdc
[root@cms-1 ~]# mkfs.ext4 -m 0 -L var /dev/sdd
[root@cms-1 ~]# mkfs.ext4 -m 0 -L opt /dev/sde

[root@cms-1 ~]# mkdir -p /etc/Acronis /opt/acronis /var/lib/Acronis
[root@cms-2 ~]# mkdir -p /etc/Acronis /opt/acronis /var/lib/Acronis

[root@cms-1 ~]# mount /dev/sdc /etc/Acronis
[root@cms-1 ~]# mount /dev/sdd /var/lib/Acronis
[root@cms-1 ~]# mount /dev/sde /opt/acronis

[root@cms-1 ~]# lsblk -f
NAME                    FSTYPE      FSVER      LABEL      UUID
FSAVAIL      FSUSE%   MOUNTPOINTS
...
sdc                     ext4 1.0 etc cdbcd761-01fc-4f13-ad48-
cdcee09a6dd2 4,8G 0% /etc/Acronis
sdd                     ext4 1.0 var eda7bfbb-edd8-4af3-b866-
1bdfa26879d6 97,7G 0% /var/lib/Acronis
sde                     ext4 1.0 opt 1fa314b9-765f-460a-b0ef-
9f3c56c0dd81 19,5G 0% /opt/acronis
...
```

Кластерные ресурсы и файловые системы

На одном из узлов кластера создайте кластерные ресурсы:

```
pcs resource create rsc_shared_disks ocf:heartbeat:iscsi udev=”no” \
    portal=10.77.44.62 target=iqn.2003-01.org.linux-iscsi.iscsi-tgt.x8664:sn.bfbc1ebb624c \
    op monitor interval=60s timeout=30s

pcs resource create rsc_fs_etc ocf:heartbeat:Filesystem \
    device=”/dev/disk/by-uuid/cdbcd761-01fc-4f13-ad48-cdcee09a6dd2” \
    directory=”/etc/Acronis” fstype=”ext4” options=”lazytime” \
    force_unmount=”true” \
    op monitor interval=60 timeout=60 OCF_CHECK_LEVEL=20 \
    meta migration-threshold=2 failure-timeout=1d

pcs resource create rsc_fs_var ocf:heartbeat:Filesystem \
    device=”/dev/disk/by-uuid/eda7bfbb-edd8-4af3-b866-1bdfa26879d6” \
    directory=”/var/lib/Acronis/” fstype=”ext4” options=”lazytime” \
    force_unmount=”true” \
    op monitor interval=60 timeout=60 OCF_CHECK_LEVEL=20 \
    meta migration-threshold=2 failure-timeout=1d

pcs resource create rsc_fs_opt ocf:heartbeat:Filesystem \
    device=”/dev/disk/by-uuid/1fa314b9-765f-460a-b0ef-9f3c56c0dd81” \
    directory=”/opt/acronis” fstype=”ext4” options=”lazytime” \
    force_unmount=”true” \
    op monitor interval=60 timeout=60 OCF_CHECK_LEVEL=20 \
    meta migration-threshold=2 failure-timeout=1d

pcs constraint colocation set rsc_fs_etc rsc_fs_var rsc_fs_opt \
    sequential=false set rsc_shared_disks setoptions id=col_fs

pcs constraint order set rsc_shared_disks set rsc_fs_etc rsc_fs_var \
    rsc_fs_opt sequential=false require-all=true setoptions id=ord_fs
```

Установка Кибер Бэкап

Установите Кибер Бэкап на узле с примонтированными файловыми системами стандартным образом (см. раздел *Установка*). После успешной установки сервера управления Кибер Бэкап необходимо установить его также на второй узел. Для этого остановите службы Кибер Бэкап и переместите файловые системы на второй узел:

```
[root@cms-1 ~]# systemctl stop acronis_ams
[root@cms-1 ~]# systemctl stop acronis_asm
[root@cms-1 ~]# systemctl stop acronis_zmqgw
[root@cms-1 ~]# systemctl stop acronis_monitoring_service
[root@cms-1 ~]# pcs resource move rsc_shared_disks --autodelete

[root@cms-1 ~]# pcs status
Cluster name: CyberBackup
Cluster Summary:
    * Stack: corosync (Pacemaker is running)
    * Current DC: cms-1 (version 2.1.6-1.el7-6fdc9deea29) - partition with quorum
    * Last updated: Wed Nov  1 09:58:45 2023 on cms-1
    * Last change:  Wed Nov  1 09:58:43 2023 by root via crm_resource on cms-1
    * 2 nodes configured
    * 9 resource instances configured

Node List:
    * Online: [ cms-1 cms-2 ]

Full List of Resources:
    * rsc_shared_disks    (ocf::custom:iscsi):     Started cms-2
    * rsc_fs_etc  (ocf::heartbeat:Filesystem):     Started cms-2
    * rsc_vip (ocf::heartbeat:IPaddr2):    Started cms-1
    * rsc_fs_var  (ocf::heartbeat:Filesystem):     Started cms-2
    * rsc_fs_opt  (ocf::heartbeat:Filesystem):     Started cms-2

Daemon Status:
    corosync: active/enabled
    pacemaker: active/enabled
    pcsd: active/enabled
```

Кластерные ресурсы и службы Кибер Бэкап

Создайте кластерные ресурсы для служб Кибер Бэкап на одном из узлов кластера.

Важно

В параметре `portal` ресурса `rsc_vip` обязательно укажите IP-адрес, а не доменное имя.

```
pcs resource create rsc_vip ocf:heartbeat:IPaddr2 \
    ip=”10.77.44.57” cidr_netmask=”22” \
    op monitor interval=”30”

pcs resource create rsc_ams systemd:acronis_ams \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d


pcs resource create rsc_asm systemd:acronis_asm \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d


pcs resource create rsc_mon systemd:acronis_monitoring_service \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d


pcs resource create rsc_zmqgw systemd:acronis_zmqgw \
    op start interval=0 timeout=60 \
    op stop interval=0 timeout=60 \
    op monitor interval=10 \
    meta target-role=Started \
    migration-threshold=2 failure-timeout=1d

pcs constraint colocation set rsc_ams rsc_asm rsc_mon rsc_zmqgw \
        sequential=false set rsc_fs_etc rsc_fs_var rsc_fs_opt setoptions \
        id=col_services

pcs constraint order set rsc_fs_etc rsc_fs_var rsc_fs_opt sequential=false \
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        require-all=true set rsc_ams rsc_asm rsc_mon rsc_zmqgw sequential=false \
        setoptions id=ord_services

pcs constraint colocation add rsc_vip with rsc_ams id=col_vip



[root@cms-2 ~]# pcs resource cleanup

[root@cms-2 ~]# pcs  status
Cluster name: CyberBackup
Cluster Summary:
    * Stack: corosync (Pacemaker is running)
    * Current DC: cms-1 (version 2.1.6-1.el7-6fdc9deea29) - partition with quorum
    * Last updated: Wed Nov  1 10:04:32 2023 on cms-2
    * Last change:  Wed Nov  1 09:58:43 2023 by root via crm_resource on cms-1
    * 2 nodes configured
    * 9 resource instances configured

Node List:
    * Online: [ cms-1 cms-2 ]

Full List of Resources:
    * rsc_shared_disks    (ocf::custom:iscsi):     Started cms-2
    * rsc_fs_etc  (ocf::heartbeat:Filesystem):     Started cms-2
    * rsc_vip (ocf::heartbeat:IPaddr2):    Started cms-2
    * rsc_fs_var  (ocf::heartbeat:Filesystem):     Started cms-2
    * rsc_fs_opt  (ocf::heartbeat:Filesystem):     Started cms-2
    * rsc_ams (systemd:acronis_ams):   Started cms-2
    * rsc_asm (systemd:acronis_asm):   Started cms-2
    * rsc_mon (systemd:acronis_monitoring_service):    Started cms-2
    * rsc_zmqgw   (systemd:acronis_zmqgw):     Started cms-2

Daemon Status:
    corosync: active/enabled
    pacemaker: active/enabled
    pcsd: active/enabled
```

Убедитесь, что авторизация в веб-консоли по публичному адресу или его имени http://cms:9877 проходит успешно.

Подключение агентов

Для корректной работы клиентов после переключения активного узла кластера необходимо, чтобы регистрация агентов была выполнена с использованием плавающего кластерного адреса сервера управления. Данный адрес соответствует адресу, указанному в кластерном ресурсе `rsc_vip`.

Если агент ранее был зарегистрирован на некластеризованном сервере управления, то необходимо выполнить его перерегистрацию с явным указанием кластерного адреса. Пример перерегистрации агента из клиентской Linux-системы с использованием одноразового токена:

```
root@cbclient:~# /usr/lib/Acronis/RegisterAgentTool/RegisterAgent --
operation unregister
Success.
200
null

root@cbclient:~# /usr/lib/Acronis/RegisterAgentTool/RegisterAgent --
operation register --address cms --token 8D77-CEDC-433B
Success.
200
null
```

В этом примере:

- `cms` — кластерное доменное имя или vIP-адрес сервера управления;
- `8D77-CEDC-433B` — токен, полученный в консоли управления Кибер Бэкап для регистрации агента.

Подробное описание дополнительных возможностей и вариантов регистрации агентов см. в отдельной статье.

Добавление машин через веб-интерфейс

Чтобы приступить к добавлению машины на сервер управления, щёлкните **Физические и виртуальные машины** → **Добавить**.

Если сервер управления установлен в Linux, будет предложено выбрать программу установки в соответствии с типом машины, которую нужно добавить. После скачивания программы установки запустите ее локально на этой машине.

Операции, описанные далее в этом разделе, возможны, если сервер управления установлен в Windows. В большинстве случаев развертывание агента на выбранной машине выполняется без вывода сообщений.

Добавление машины с ОС Windows

Подготовка

1. Для установки на удаленной машине, *не* входящей в домен Active Directory, контроль учетных записей (UAC) на этой машине должен быть *отключен*. Чтобы получить дополнительную информацию о том, как отключить его, выберите *Требования к контролю учетных записей пользователей (UAC)* > ”Как отключить UAC”.
2. По умолчанию для выполнения удаленной установки на любой машине Windows требуются учетные данные встроенной учетной записи администратора. Для удаленной установки с использованием учетных данных другого администратора, ограничения удаленного контроля учетных записей (UAC) должны быть *отключены*. Чтобы получить дополнительную информацию о том, как отключить их, выберите *Требования к контролю учетных записей пользователей (UAC)* > ”Порядок отключения ограничений удаленного контроля учетных записей (UAC)”.
3. Общий доступ к файлам и принтерам на удаленной машине должен быть *включен*. Для получения доступа к этому параметру выберите **Панель управления → Брандмауэр Windows (Брандмауэр Защитника Windows в Windows 10) → Центр управления сетями и общим доступом → Изменить дополнительные параметры общего доступа**.
4. Кибер Бэкап использует TCP-порты 445, 25001 и 43234 для удаленной установки.

   Порт 445 открывается автоматически при выборе параметра ”Общий доступ к файлам и принтерам”. В брандмауэре Windows порты 43234 и 25001 открыты автоматически. При использовании другого брандмауэра убедитесь, что эти три порта открыты (добавлены в исключения) как для входящих, так и исходящих запросов.

   По окончанию удаленной установки порт 25001 автоматически закрывается брандмауэром Windows. Если в дальнейшем нужно обновлять агент удаленно, порты 445 и 43234 должны быть открыты. В брандмауэре Windows порт 25001 открывается и закрывается автоматически в ходе каждого обновления. Если используется другой брандмауэр, сохраните все эти порты открытыми.

Примечание

Удаленная установка не поддерживается для контроллеров домена. Процедуру установки агента защиты на контроллер домена см. в разделе *Установка в ОС Windows*. Необходимо настроить параметры установки, выбрав в разделе **Учетная запись для входа службы агента** параметр **Использовать следующую учетную запись**. Дополнительную информацию об этом параметре см. в разделе *Настройка параметров установки*.

Компоненты для удаленной установки

Для установки агентов на удаленные машины используются компоненты для удаленной установки, размещенные на сервере управления. В зависимости от операционной системы машины, на которой работает сервер управления, компоненты размещаются в следующих локальных папках:

- `%ProgramFiles%\Acronis\RemoteInstallationFiles\installation_files\<номер сборки продукта>` (ОС Windows; задается в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles\<номер сборки продукта>`),
- `/usr/lib/Acronis/RemoteInstallationFiles/installation_files/<номер сборки продукта>` (ОС Linux).

На сервер управления с ОС Windows компоненты для удаленной установки устанавливаются по умолчанию. Ручная установка компонентов может понадобиться в следующих случаях:

- Компоненты не были установлены при установке сервера управления на машину с ОС Windows.
- Используется сервер управления, установленный на машину с ОС Linux.
- Компоненты были удалены с сервера управления.

Порядок размещения компонентов на сервере управления с ОС Linux

1. В веб-консоли Кибер Бэкап щёлкните значок учетной записи в правом верхнем углу и выберите пункт **Загрузки**.
2. Щёлкните **Офлайн-установщик для Windows (64-bit)** и получите установщик продукта.
3. Загрузите установщик продукта на машину с ОС Windows и запустите его.
4. В мастере установки продукта нажмите **Создание MST- и MSI-файлов для автоматической установки**.
5. В разделе **Устанавливаемые компоненты** выберите компоненты **Сервер управления**, **Компоненты для удаленной установки** и **Агент для Windows** и извлеките их файлы.
6. На сервере управления создайте папку `x64` в папке `/usr/lib/Acronis/RemoteInstallationFiles/installation_files/<номер сборки продукта>`, а затем разместите извлеченные ранее файлы в созданной папке.
7. Убедитесь, что в папке `/usr/lib/Acronis/RemoteInstallationFiles/installation_files` есть файл `web_installer.exe`. При необходимости в разделе **Загрузки** веб-консоли Кибер Бэкап получите файл онлайн-установщика для Windows, сохраните его в эту папку и переименуйте в `web_installer.exe`.
8. Перезапустите службу Acronis Management Server с помощью команды `systemctl restart acronis_ams`.

Агент развертывания

Чтобы установить агентов защиты на удаленных машинах из веб-консоли Кибер Бэкап, в вашей среде должен быть установлен хотя бы один агент защиты для Windows. Этот агент будет служить как агент развертывания для удаленной установки, а также будет подключаться к серверу управления и целевой удаленной машине.

При развертывании сервера управления на машине с ОС Windows, как правило, устанавливается агент защиты, который можно использовать как агент развертывания. При использовании сервера управления на машине с ОС Linux необходимо установить агента защиты на одну из имеющихся машин с ОС Windows.

> **Примечание**
>
> При установке агентов защиты на нескольких машинах агент защиты для Windows может также использоваться как агент обнаружения.

Принцип работы агента развертывания:

1. Агент развертывания подключается к серверу управления и получает файл `web_installer.exe`.
2. Агент развертывания подключается к удаленной машине по имени хоста или IP-адресу этой машины с использованием указанных вами учетных данных администратора, а затем передает на эту машину файл `web_installer.exe`.
3. Файл `web_installer.exe` выполняется на удаленной машине в автоматическом режиме.
4. В зависимости от области требуемой установки веб-установщик получает дополнительные компоненты с сервера управления, а затем устанавливает их на целевую машину с использованием команды `msiexec`.

   В зависимости от операционной системы машины, на которой работает сервер управления, компоненты размещаются в следующих локальных папках:

   - `%ProgramFiles%\Acronis\RemoteInstallationFiles\installation_files\<номер сборки продукта>` (ОС Windows; задается в разделе реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles\<номер сборки продукта>`),
   - `/usr/lib/Acronis/RemoteInstallationFiles/installation_files/<номер сборки продукта>` (ОС Linux).
5. По окончании установки агент удаленной машины регистрируется на сервере управления.

Добавление машины

1. Щёлкните **Физические и виртуальные машины** → **Добавить**.
2. Щёлкните **Windows** или кнопку, соответствующую приложению, которое необходимо защитить. В зависимости от того, какая кнопка нажата, будет выбран один из следующих вариантов:
   - Агент для Windows
   - Агент для Hyper-V
   - Агент для SQL + агент для Windows
   - Агент для Exchange + агент для Windows

     Если при наличии хотя бы одного зарегистрированного агента для Exchange щёлкнуть **Microsoft Exchange Server** → **Почтовые ящики Exchange**, будет выполнен переход непосредственно к шагу 6.
   - Агент для Active Directory + агент для Windows
3. Выберите агент развертывания.
4. Укажите имя хоста или IP-адрес целевой машины и учетные данные учетной записи с правами администратора на этой машине.

   Удаленная установка должна выполняться пользователем со встроенной учетной записью администратора. Если нужно использовать другую учетную запись пользователя, искомый пользователь должен входить в группу ”Администраторы”. Кроме того, необходимо внести изменения в реестр на машине, которая добавляется, согласно инструкциям по следующей ссылке: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. Нажмите **Установить**.
7. Если на шаге 2 вы выбрали **Microsoft Exchange Server** → **Почтовые ящики Exchange**, укажите машину, на которой включена роль сервера **Client Access** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе *Резервное копирование почтовых ящиков*.

Требования к контролю учетных записей пользователей (UAC)

На машине с ОС Windows, которая не входит в домен Active Directory, для операций централизованного управления (включая удаленную установку) необходимо, чтобы контроль учетных записей пользователей (UAC) и ограничения удаленного контроля учетных записей пользователей были отключены.

Порядок отключения UAC

1. Откройте редактор реестра.
2. Найдите следующий раздел реестра:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
3. Для параметра **EnableLUA** измените значение на `0`.
4. Перезапустите машину.

Порядок отключения ограничений удаленного контроля учетных записей (UAC)

1. Откройте редактор реестра.
2. Найдите следующий раздел реестра:
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
3. Для параметра **LocalAccountTokenFilterPolicy** измените значение на `1`.

   Если параметр **LocalAccountTokenFilterPolicy** не существует, создайте его как DWORD (32 бита). Дополнительную информацию об этом значении см. в документации Microsoft.

> **Примечание**
>
> Из соображений безопасности после выполнения операции управления (например, удаленной установки) рекомендуется вернуть для обеих настроек их исходные значения: `EnableLUA=1` и `LocalAccountTokenFilterPolicy=0`.

Добавление машины с ОС Linux

1. Щёлкните **Физические и виртуальные машины** → **Добавить**.
2. Щёлкните **Linux**. Будет загружен файл установки.
3. На машине, которую нужно защитить, *запустите программу установки локально*.

Добавление vCenter или хоста ESXi

Добавить vCenter или автономный хост ESXi на сервер управления можно четырьмя способами:

- *Развертывание агента для VMware (виртуальное устройство)*

  Этот способ рекомендуется в большинстве случаев. Виртуальное устройство будет автоматически развернуто на каждом хосте, находящемся под управлением указанной системы vCenter. Можно выбрать хосты и настроить параметры виртуальных устройств.

- *Установка агента для VMware (Windows)*

  Возможно, вы решите установить агент для VMware на физической машине с ОС Windows в целях резервного копирования с помощью третьей машины или без использования локальной сети.

  - **Резервное копирование с помощью третьей машины**

    Используйте в том случае, если нагрузка на рабочие хосты ESXi так велика, что запускать на них виртуальные устройства нежелательно.

  - **Резервное копирование без использования локальной сети**

    Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Подробные инструкции см. в разделе *Резервное копирование без использования локальной сети посредством Windows-агента для VMware*.

  Если сервер управления выполняется в Windows, агент будет автоматически развернут на указанной машине. В противном случае необходимо установить агент вручную.

- *Регистрация установленного агента для VMware*

  Это необходимый этап после переустановки сервера управления. Кроме того, можно зарегистрировать и настроить агент для VMware (виртуальное устройство, развернутое из шаблона OVF). Агент можно подключить только к одному vCenter Server или автономному хосту ESXi.

- *Настройка уже зарегистрированного агента для VMware*

  Это необходимый этап после установки агента для VMware (Windows) вручную или развертывания программно-аппаратного комплекса Кибер Бэкап. Кроме того, можно связать уже настроенный агент для VMware с другим сервером vCenter Server или автономным хостом ESXi.

Развертывание агента для VMware (виртуальное устройство) через веб-интерфейс

1. Щёлкните **Физические и виртуальные машины** → **Добавить**.
2. Щёлкните **VMware ESXi**.
3. Выберите **Разверните виртуальное устройство на каждом хосте vCenter**.
4. Укажите адрес и учетные данные для доступа к vCenter Server или автономному хосту ESXi. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с *необходимыми привилегиями* на хосте vCenter Server или ESXi.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. [Необязательно] Щёлкните **Настройки**, чтобы настроить параметры развертывания:
   - хосты ESXi, на которых необходимо развернуть агент (только если на предыдущем шаге был указан сервер vCenter Server);
   - имя виртуального устройства;
   - хранилище данных, в котором будет находиться устройство;
   - пул ресурсов или контейнер vApp, в котором будет содержаться устройство;
   - сеть, к которой будет подключен сетевой адаптер виртуального устройства;
   - настройки сети виртуального устройства. Можно выбрать автоматическую настройку DHCP или вручную указать значения, включая статический IP-адрес.
7. Щёлкните **Развернуть**.

Установка агента для VMware (Windows)

Подготовка

Выполните инструкции по подготовке, описанные в разделе *Добавление машины с Windows*.

Установка

1. Щёлкните **Физические и виртуальные машины** → **Добавить**.
2. Щёлкните **VMware ESXi**.
3. Выберите **Удаленно установить на машине под управлением Windows**.
4. Выберите агент развертывания.
5. Укажите имя хоста или IP-адрес целевой машины и учетные данные учетной записи с правами администратора на этой машине.
6. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
7. Щёлкните **Подключиться**.
8. Укажите адрес и учетные данные для vCenter Server или автономного хоста ESXi, а затем щёлкните **Подключиться**. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с *необходимыми привилегиями* на хосте vCenter Server или ESXi.

   > **Примечание**
   >
   > Агент можно подключить только к одному vCenter Server или автономному хосту ESXi. Если требуется подключить еще один автономный хост ESXi, то необходимо развернуть новый агент.

9. Щёлкните **Установить**.

Регистрация установленного агента для VMware

В этом разделе описана регистрация агента для VMware через веб-интерфейс.

Альтернативные способы регистрации указаны ниже.

- Можно зарегистрировать агент для VMware (виртуальное устройство), указав сервер управления в интерфейсе виртуального устройства. См. шаг 3 в теме ”Настройка виртуального устройства” раздела Развертывание агента для VMware (виртуальное устройство) из шаблона OVF.
- Агент для VMware (Windows) регистрируется при его *локальной установке*.

Регистрация агента для VMware

1. Щёлкните **Физические и виртуальные машины** → **Добавить**.
2. Щёлкните **VMware ESXi**.
3. Выберите **Зарегистрировать уже установленный агент**.
4. Выберите агент развертывания.
5. При регистрации *агента для VMware (Windows)* укажите имя хоста или IP-адрес машины, на которой установлен агент, и данные учетной записи с правами администратора на этой машине.

   При регистрации *агента для VMware (виртуальное устройство)* укажите имя хоста или IP-адрес виртуального устройства и учетные данные сервера vCenter Server или автономного хоста ESXi, на котором работает устройство.
6. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
7. Щёлкните **Подключиться**.
8. Укажите имя хоста либо IP-адрес сервера vCenter Server или хоста ESXi и учетные данные для доступа к нему, а затем щёлкните **Подключение**. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с *необходимыми привилегиями* на хосте vCenter Server или ESXi.
9. Щёлкните **Зарегистрировать**, чтобы зарегистрировать агент.

Настройка уже зарегистрированного агента для VMware

В этом разделе описан порядок связывания агента для VMware с vCenter Server или ESXi в веб-интерфейсе. Как вариант, это можно сделать в консоли агента для VMware (виртуальное устройство).

Эта процедура позволяет изменить существующую связь агента с vCenter Server или ESXi. Как вариант, это можно сделать в агенте для VMware (виртуальное устройство) или последовательно выбрав пункты **Настройки** → **Агенты** → **Подробнее** → **vCenter/ESXi**.

Настройка агента для VMware

1. Щёлкните **Физические и виртуальные машины** → **Добавить**.
2. Щёлкните **VMware ESXi**.
3. В данном программном обеспечении отображается ненастроенный агент для VMware, который идет первым в алфавитном порядке.

   Если настроены все агенты, зарегистрированные на сервере управления, щёлкните **Настроить уже зарегистрированный агент**. После этого в программе отобразится агент, который идет первым в алфавитном порядке.
4. При необходимости щёлкните **Машина с агентом** и выберите агент для настройки.
5. Укажите или измените имя хоста либо IP-адрес сервера vCenter Server или хоста ESXi и учетные данные для доступа к ним. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с *необходимыми привилегиями* на хосте vCenter Server или ESXi.
6. Щёлкните **Настроить**, чтобы сохранить изменения.

Установка агентов

В этом разделе приводятся инструкции по установке и развертыванию агентов для таких программных компонентов, как операционные системы, платформы виртуализации, Кибер Инфраструктура и некоторых других. Установка агентов для защиты приложений, почтовых сервисов и баз данных рассматривается в разделе *Защита приложений, сервисов, баз данных*.

После установки и развертывания необходимых агентов убедитесь, что устройство, предназначенное к защите, доступно в *веб-консоли* в разделе **Устройства**. Затем можно приступать непосредственно к резервному копированию (подробнее об этом см. в разделе *Резервное копирование*).

Установка агентов в ОС Windows вручную

Установка агента для Windows, агента для Hyper-V, агента для Exchange, агента для SQL или агента для Active Directory

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Выберите **Установить агент защиты**.

5. Выполните любое из следующих действий:

   - Нажмите **Установить**.

     Это самый легкий способ установить продукт. Для большинства параметров установки будут использоваться значения по умолчанию.

     По умолчанию устанавливаются следующие компоненты:

     - Агент для Windows
     - Другие агенты (агент для Hyper-V, агент для Exchange, агент для SQL и агент для Active Directory), если на машине обнаружен соответствующий гипервизор или приложение
     - Мастер создания загрузочных носителей
     - Программа командной строки
     - Мониторинг Защиты Данных

   - Щёлкните **Настройка параметров установки**, чтобы настроить программу установки.

     Можно будет выбрать компоненты для установки и указать дополнительные параметры. Дополнительную информацию см. в разделе *Настройка параметров установки*.

   - Щёлкните **Создать MST- и MSI-файлы для автоматической установки**, чтобы извлечь пакеты установки. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **Создать**. Для этой процедуры не требуется никаких дополнительных шагов.

     Чтобы развернуть агенты через групповую политику, выполните действия, указанные в разделе *Развертывание агентов с использованием групповой политики*.

6. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:

   1. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   2. Укажите учетные данные администратора сервера управления или маркер регистрации.

      Дополнительную информацию о создании маркера регистрации см. в разделе *Развертывание агентов с использованием групповой политики*.

   3. Нажмите кнопку **Готово**.

7. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе *Отделы и*

административные учетные записи.

8. Приступите к установке.
9. После завершения установки нажмите кнопку **Закрыть**.
10. Если установлен агент для Exchange, можно будет выполнять резервное копирование баз данных Exchange. Чтобы создать резервную копию почтовых ящиков Exchange, откройте веб-консоль Кибер Бэкап, щёлкните **Добавить** → **Microsoft Exchange Server** → **Почтовые ящики Exchange** и укажите машину, на которой включена роль сервера **клиентского доступа** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе *Резервное копирование почтовых ящиков*.

Порядок установки агента для VMware (Windows), агента для Oracle или агента для Exchange на машину без сервера Microsoft Exchange Server

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Выберите **Установить агент защиты**, затем щёлкните **Настройка параметров установки**.
5. Рядом с пунктом **Устанавливаемые компоненты** щёлкните **Изменить**.
6. Установите флажок, соответствующий агенту, который необходимо установить. Снимите флажки для компонентов, которые не нужно устанавливать. Чтобы продолжить, нажмите кнопку **Готово**.
7. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
    1. Перейдите на **Сервер управления** и щёлкните **Указать**.
    2. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
    3. Укажите учетные данные администратора сервера управления или маркер регистрации.

       Дополнительную информацию о создании маркера регистрации см. в разделе *Развертывание агентов с использованием групповой политики*.
    4. Нажмите кнопку **Готово**.
8. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе *Отделы и*

административные учетные записи.

9. [Необязательно] Измените другие настройки установки, как описано в разделе *Настройка параметров установки*.
10. Нажмите **Установить**, чтобы продолжить установку.
11. После завершения установки нажмите кнопку **Закрыть**.
12. [Только при установке агента для VMware (Windows)] Выполните процедуру, которая описана в разделе *Настройка уже зарегистрированного агента для VMware*.
13. [Только при установке агента для Exchange] Откройте веб-консоль Кибер Бэкап, щёлкните **Добавить** → **Microsoft Exchange Server** → **Почтовые ящики Exchange** и укажите машину, на которой включена роль сервера **клиентского доступа** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе *Резервное копирование почтовых ящиков*.

Установка агентов в ОС Linux вручную

Подготовка

1. В системе, в которой не используется диспетчер пакетов RPM, необходимо установить этот диспетчер вручную. Как привилегированный пользователь выполните команду (например):

   ```
   apt-get install rpm
   ```

2. Убедитесь в том, что на машине установлены *необходимые пакеты для ОС Linux*.
3. Дайте разрешение на исполнение установочному файлу. Выполните следующую команду:

   ```
   chmod +x CyberBackup_*
   ```

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE ознакомьтесь с разделом *Совместимость с ОС Astra Linux SE* и выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

   ```
   tar --xattrs --xattrs-include=* -xvf CyberBackup_18_64-bit.x86_64.tar
   ```

2. Запустите файл установки с правами привилегированного пользователя:

```
./CyberBackup_18_64-bit.x86_64
```

3. Обновите образы initramfs:

```
update-initramfs -u -k all
```

4. Перезагрузите систему.

Установка

Для установки агента для Linux необходимо как минимум 2,0 ГБ свободного места на диске.

Установка агента для Linux

1. Запустите файл установки (файл .i686 или .x86_64) как привилегированный пользователь:

```
./CyberBackup_19_64-bit.x86_64
```

2. Примите условия лицензионного соглашения.
3. Укажите устанавливаемые компоненты:
    1. Снимите флажок **Сервер управления**.
    2. Установите флажки для агентов, которые необходимо установить. Доступны следующие агенты:
        - Агент для Linux (базовый агент);
        - Агент для Oracle;
        - Агент для PostgreSQL;
        - Агент для MySQL/MariaDB;
        - Агент для Kubernetes;
        - Агент для oVirt;
        - Агент для CommuniGate Pro;
        - Агент для VK WorkMail;
        - Агент для Mailion;
        - Агент для RuPost;
        - Rescue Media Builder (компонент необходим для удаленного восстановления всей машины и дисков).

Для агентов для Oracle, PostgreSQL, MySQL/MariaDB, Kubernetes, oVirt, CommuniGate Pro, VK WorkMail также требуется установленный агент для Linux.

Агент для oVirt (локальный), установленный через установщик Кибер Бэкап, предназначен для резервного копирования с использованием аппаратных моментальных снимков (см. раздел *Настройка хранилища данных YADRO TATLIN.UNIFIED*). Для резервного копирования виртуальных машин устанавливайте агент для oVirt (виртуальное устройство), как описано в разделе *Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация)*.

3. Нажмите кнопку **Далее**.

4. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:

   1. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   2. Укажите имя пользователя и пароль администратора сервера управления.

      Если в вашей организации есть отделы, установка учетных данных может понадобиться, чтобы добавить машину в отдел, которым управляет указанный администратор. Дополнительные сведения см. в разделе *Отделы и административные учетные записи*.

   3. Нажмите кнопку **Далее**.

5. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов, затем нажмите клавишу **ВВОД**.

   Этот запрос появляется, если учетная запись, указанная в предыдущем шаге, является администратором одного отдела или организации как минимум с одним отделом.

   Примечание

   Если в процессе установки возникнет ошибка сборки модуля ядра ”Не удалось построить модуль ядра SnapAPI. Операции с резервными копиями на уровне дисков будут недоступны”, продолжите установку. После завершения установки решите проблему с помощью статьи базы знаний Сборка модуля SnapAPI для Linux.

6. Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните пароль, который следует использовать (пароль привилегированного пользователя).

   Примечание

   В процессе установки создается новый ключ, который используется для подписи модулей ядра. Необходимо зарегистрировать этот ключ в списке владельцев ключей машины (Machine Owner

Key, MOK), перезапустив машину. Если не зарегистрировать ключ, агент не будет работать. Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 6.

7. После завершения установки выполните одно из следующих действий.

   - Нажмите кнопку **Перезапустить**, если в предыдущем шаге вам было предложено перезапустить систему.

     Во время перезапуска системы выберите управление ключом владельца машины (MOK), выберите **Зарегистрировать MOK** и зарегистрируйте ключ, используя пароль, предложенный в предыдущем шаге.

   - В противном случае нажмите **Выход**.

Сведения об устранении неполадок представлены в файле `/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`.

Установка агентов для ОС Linux из RPM-репозитория

С версии 19.0 в Кибер Бэкап поддерживается возможность установки из локального или сетевого RPM-репозитория следующих компонентов: агентов для ОС Linux и компонентов загрузочного носителя для ОС Linux.

⚠ Предупреждение

Если на машине ранее были установлены компоненты Кибер Бэкап с помощью BIN-установщика, во избежание ошибок и сбоев полностью удалите их перед установкой агента из RPM-репозитория. При удалении старого агента снимите флажок **Очистить все следы продукта (удалить журналы продукта и параметры конфигурации)** — это позволит сохранить конфигурацию. Подробнее об удалении компонентов Кибер Бэкап см. в разделе *Удаление продукта*.

Инструкции по развёртыванию RPM-репозитория и установке из него агента и компонентов загрузочного носителя для ОС Linux, а также порядок удаления такого агента приведены далее.

Ограничения

- Менеджер пакетов позволяет установить только агент для ОС Linux и компоненты загрузочного носителя для ОС Linux. Установка других агентов и компонентов с помощью менеджера пакетов не поддерживается. Для их развёртывания воспользуйтесь BIN-установщиком.
- Для обновления компонентов используйте BIN-установщик. Обновление через менеджер пакетов

не поддерживается.

- Пакет поставляется как единое целое. Установка и удаление компонентов по отдельности не поддерживается менеджером пакетов: пакет устанавливается и удаляется только целиком.
- Развёртывание RPM-репозитория и установка агента для ОС Linux возможны только в RPM-совместимых ОС.
- Установка компонентов из RPM-репозитория на целевых машинах с включённым режимом Secure Boot не поддерживается.
- Развёртывание из RPM-репозитория не поддерживается в операционных системах с активированным режимом FIPS.
- При использовании проверки цифровых подписей (`gpgcheck=1`) убедитесь, что в общесистемных криптографических политиках ОС Linux (crypto-policies) включена поддержка алгоритмов SHA-1 и DSA. В некоторых дистрибутивах (например, CentOS 10) эти алгоритмы могут быть отключены по умолчанию, что приведёт к ошибке проверки цифровой подписи при установке пакетов.

Развёртывание RPM-репозитория

Установка RPM-репозитория может быть выполнена в RPM-совместимой операционной системе (ОС), например: РЕД ОС, CentOS, ROSA Linux. Также допускается установка в ОС семейства Альт (в этом случае процесс настройки имеет свои особенности; обратитесь к документации используемой ОС). Перечень версий поддерживаемых ОС приведён в разделе *Поддерживаемые операционные системы*.

Способы установки RPM-репозитория:

- локально (в этом случае архив с RPM-пакетами сохраняется непосредственно на ту же целевую машину, на которую планируется установить агент);
- в сетевую папку (этот метод используется, когда архив с пакетами хранится на удалённом сервере, а установка агентов выполняется на другие машины по сети).

Порядок установки и настройки репозитория для обоих случаев приведён далее в этом разделе. Указанные команды должны выполняться от имени привилегированного пользователя (root).

Загрузка RPM-пакетов

Чтобы загрузить RPM-пакеты репозитория, выполните следующие действия:

1. На целевой машине создайте директорию для организации RPM-репозитория и перейдите в неё, например:

```
cd /opt
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
mkdir <имя_папки>
cd <имя_папки>
```

Здесь `<имя_папки>` — имя целевой директории для создания RPM-репозитория (например, `repo`).

2. Скачайте архив RPM-репозитория:

```
wget <веб-ссылка>
```

Здесь `<веб-ссылка>` — URL-адрес для скачивания архива RPM-репозитория с веб-ресурса Киберпротект.

3. Распакуйте скачанный архив с RPM-пакетами в целевую директорию, созданную на шаге 1:

```
tar xfz <архив>
```

В этой команде `<архив>` — имя скачанного файла с архивом RPM-репозитория в формате .TAR.GZ.

4. Проверьте содержимое директории, чтобы убедиться в успешности извлечения компонентов, например:

```
ls -la
итого 1470484
drwxr-xr-x. 3  504  504      4096 сен  9 10:47 .
dr-xr-x---. 6 root root      4096 сен  9 11:19 ..
-rwxr-xr-x. 1  504  504 232546983 сен  9 10:31 BackupAndRecoveryAgent-19.0. 43183-1.x86_64.
↪rpm
-rwxr-xr-x. 1  504  504 302439882 сен  9 10:31 BackupAndRecoveryBootableComponents-19.0.
↪43183-1.x86_64.rpm
-rwxr-xr-x. 1  504  504      6285 сен  9 10:31 CyberBackupAgent-19.0.43183-1. noarch.rpm
-rwxr-xr-x. 1  504  504     78624 сен  9 10:31 dkms-3.0.3.3-103.noarch.rpm
-rwxr-xr-x. 1  504  504  77034941 сен  9 10:31 file_protector-3.0-423.noarch.rpm
drwxr-xr-x. 2 root root      4096 сен  9 10:47 repodata
-rwxr-xr-x. 1  504  504 142265855 сен  9 10:31 snapapi26_modules-2.2.10-1.noarch.rpm
...
```

Загрузка GPG-ключа безопасности

Проверить подлинность загруженных RPM-пакетов можно с помощью публичного GPG-ключа безопасности. Чтобы загрузить его, выполните следующие действия:

1. Скачайте файл с GPG-ключом и сохраните его на целевой машине под именем `gpg.key`:

```
wget <веб-ссылка> -O gpg.key
```

Здесь `<веб-ссылка>` — URL-адрес для скачивания файла с GPG-ключом с веб-ресурса Киберпротект.

2. Импортируйте GPG-ключ, например:

```
rpm --import gpg.key
```

3. Убедитесь, что импорт выполнен успешно, например:

```
rpm -qi 'gpg-pubkey-*'
```

После этого подключите RPM-репозиторий (локальный или сетевой), как описано в соответствующем подразделе далее.

Подключение локального RPM-репозитория

Чтобы подключить локальный RPM-репозиторий, выполните следующе действия:

1. Создайте файл конфигурации локального RPM-репозитория:

```
cd /etc/yum.repos.d/
touch <имя_файла>.repo
```

Здесь `<имя_файла>` — имя созданного файла конфигурации с расширением .REPO (например, `local-cb.repo`).

2. Используя текстовый редактор, откройте созданный конфигурационный файл и укажите необходимые параметры, в том числе абсолютный путь к папке с распакованным архивом, например:

```
name=Local CyberBackup repository
baseurl=file://<путь_к_папке>
enabled=1
gpgcheck=0
```

В этом примере:

- `<путь_к_папке>` — абсолютный путь к папке с распакованным архивом (например, `/opt/repo`).
- `gpgcheck` — параметр, определяющий необходимость проверки устанавливаемых пакетов GPG-ключом. Укажите значение `1`, чтобы включить обязательную проверку подлинности пакетов, или значение `0`, чтобы отключить её (рекомендуется, если на машине установлена

ОС семейства Альт).

> **Примечание**
>
> При указании параметра `gpgcheck` со значением `1`:
>
> - Убедитесь, что GPG-ключ был импортирован в систему ранее, либо укажите путь к нему в параметре `gpgkey`.
> - Проверьте, что в общесистемных криптографических политиках ОС Linux (crypto-policies) включена поддержка алгоритмов SHA-1 и DSA. В некоторых дистрибутивах (например, CentOS 10) эти алгоритмы могут быть отключены по умолчанию, что приведёт к ошибке проверки цифровой подписи при установке пакетов.

3. Обновите базу данных менеджера пакетов, например:

```
dnf makecache
CentOS Stream 10 - BaseOS                                                ¬
↪                                                                       18 kB/
↪s |  13 kB     00:00
CentOS Stream 10 - AppStream                                             ¬
↪                                                                       74 kB/
↪s |  13 kB     00:00
CentOS Stream 10 - Extras packages                                       ¬
↪                                                                       79 kB/
↪s |  16 kB     00:00
Local CyberBackup repository                                             ¬
↪                                                                      2.9 MB/
↪s | 3.0 kB     00:00
```

   В случае успешной инициализации репозитория будет отображено сообщение:

```
Создан кэш метаданных.
```

Подключение сетевого RPM-репозитория

Чтобы подключить сетевой RPM-репозиторий, выполните следующе действия:

1. На сервере с сохранёнными компонентами RPM-репозитория установите и настройте HTTP-сервер (например, Nginx или Apache) в соответствии с документацией используемого HTTP-сервера.

2. На машине, предназначенной для установки агента, перейдите в каталог конфигурации менеджера пакетов и создайте файл конфигурации RPM-репозитория:

```
cd /etc/yum.repos.d/
touch <имя_файла>.repo
```

Здесь `<имя_файла>` — имя созданного файла конфигурации с расширением .REPO (например, `cyberbackup.repo`).

3. Используя текстовый редактор, откройте созданный конфигурационный файл и укажите необходимые параметры, в том числе путь к сетевой директории с RPM-пакетами, например:

```
name=CyberProtect RPM repo
baseurl=http://<IP-адрес_или_имя_сервера>/<имя_папки>
enabled=1
gpgcheck=0
```

В этом примере:

- `<IP-адрес_или_имя_сервера>` — IP-адрес или доменное имя сервера, на котором сохранён архив RPM-репозитория.
- `<имя_папки>` — имя опубликованной сетевой директории с RPM-архивом.
- `gpgcheck` — параметр, определяющий необходимость проверки устанавливаемых пакетов GPG-ключом. Укажите значение `1`, чтобы включить обязательную проверку подлинности пакетов, или значение `0`, чтобы отключить её (рекомендуется, если на машине установлена ОС семейства Альт).

> **Примечание**
>
> При указании параметра `gpgcheck` со значением `1`:
>
> - Убедитесь, что GPG-ключ был импортирован в систему ранее, либо укажите путь к нему в параметре `gpgkey`.
> - Проверьте, что в общесистемных криптографических политиках ОС Linux (crypto-policies) включена поддержка алгоритмов SHA-1 и DSA. В некоторых дистрибутивах (например, CentOS 10) эти алгоритмы могут быть отключены по умолчанию, что приведёт к ошибке проверки цифровой подписи при установке пакетов.

4. Обновите базу данных менеджера пакетов, например:

```
dnf makecache
CentOS Stream 10 -       BaseOS                                          ¬
↪                                                                        ¬
↪      25 kB/s |  14       kB     00:00
CentOS Stream 10 -       AppStream                                       ¬
↪                                                                        ¬
↪      24 kB/s |  14       kB     00:00
CentOS Stream 10 - Extras       packages                                 ¬
↪                                                                        ¬
↪      29 kB/s |  16 kB           00:00
CyberProtect RPM       repo                                             ¬
↪                                                                        ¬
↪      79 kB/s | 2.      5 kB     00:00
```

В случае успешной инициализации репозитория будет отображено сообщение:

```
Создан кэш метаданных.
```

Установка агентов из RPM-репозитория

В этом разделе приведён порядок установки агентов для ОС Linux из RPM-репозитория как вручную (отдельными командами для установки и регистрации агента), так и в автоматизированном режиме (установка и регистрация выполняются одной командой). Все команды должны выполняться от имени привилегированного пользователя (root).

Примечание

- Для установки агента из RPM-репозитория целевая машина должна работать под управлением RPM-совместимой ОС (например, РЕД ОС, CentOS, ROSA Linux). Перечень версий поддерживаемых ОС приведён в разделе *Поддерживаемые операционные системы*.
- Перед установкой агента убедитесь в наличии *необходимых пакетов для ОС Linux* на целевой машине. Отсутствие требуемых пакетов приведёт к сбою в процессе установки компонента.

Установка на целевую машину вручную

Чтобы установить агент для ОС Linux из RPM-репозитория, выполните следующие действия:

1. На целевой машине выполните команду:

```
dnf install CyberBackupAgent -y
```

Если в ОС целевой машины отключена поддержка алгоритмов SHA-1 и DSA (например, как в CentOS 10), а в настройках репозитория активирована проверка цифровой подписи (`gpgcheck=1`), установка завершится с ошибкой. Чтобы обойти это ограничение без изменения криптографических политик ОС, запустите установку с игнорированием проверки GPG-ключа:

```
dnf install CyberBackupAgent -y --nogpgcheck
```

В результате будет установлен пакет `CyberBackupAgent`, а также его зависимости (`BackupAndRecoveryAgent`, `BackupAndRecoveryBootableComponents`, `dkms`, `file_protector`, `snapapi26_modules`).

2. Зарегистрируйте установленный агент на сервере управления Кибер Бэкап с помощью скрипта автоматической настройки:

```
/var/lib/Cyberprotect/setup.bash -a <URL_сервера_управления> --token <маркер_регистрации>
```

Здесь:

- `<URL_сервера_управления>` — полный сетевой адрес сервера управления Кибер Бэкап с указанием протокола и порта.
- `<маркер_регистрации>` — последовательность из 12 символов, разделённых дефисами на три части. Дополнительную информацию о создании маркера регистрации см. в разделе *Развертывание агентов с использованием групповой политики*.

В результате скрипт выполнит установку модулей ядра, инициализацию и запуск сервисов, а также регистрацию на сервере управления Кибер Бэкап.

Автоматизированный запуск служб при установке агентов

Для автоматизированного запуска служб при установке агента для ОС Linux воспользуйтесь переменными окружения:

```
CB_MANAGEMENT_SERVER=${ADDRESS} CB_REG_TOKEN=${TOKEN} dnf install CyberBackupAgent -y
```

Если в ОС целевой машины отключена поддержка алгоритмов SHA-1 и DSA (например, как в CentOS 10), а в настройках репозитория активирована проверка цифровой подписи (`gpgcheck=1`), установка завершится с ошибкой. Чтобы обойти это ограничение без изменения криптографических политик ОС, запустите установку с игнорированием проверки GPG-ключа:

```
CB_MANAGEMENT_SERVER=${ADDRESS} CB_REG_TOKEN=${TOKEN} dnf install CyberBackupAgent -y --nogpgcheck
```

В этих командах:

- `CB_MANAGEMENT_SERVER` — переменная окружения со значением IP-адреса сервера управления Кибер Бэкап.
- `CB_REG_TOKEN` — переменная окружения со значением маркера регистрации.

При выполнении этих команд установка модулей, инициализация служб, их запуск, а также регистрация будет выполнена в процессе установки агента для ОС Linux.

Диагностика ошибок при пакетной установке

В случае возникновения ошибок во время установки для их диагностики воспользуйтесь журналом `/var/log/cyberprotect_setup.log`.

Коды типовых ошибок и рекомендации при их возникновении приведены в таблице далее.

Код ошибки	Описание ошибки	Рекомендации
1	Ошибка регистрации: недоступен сервер управления Кибер Бэкап.	Убедитесь, что сервер управления Кибер Бэкап запущен, затем проверьте корректность адреса. При необходимости обратитесь к специалистам Киберпротект.
2	Ошибка регистрации: недоступна служба агента.	При необходимости обратитесь к специалистам Киберпротект.
3	Общая ошибка регистрации.	Для получения более подробной информации воспользуйтесь журналом `/var/log/cyberprotect_setup.log`.
6	Ошибка установки SnapAPI на целевой машине с ОС Linux.	Для получения более подробной информации воспользуйтесь журналом `/var/log/cyberprotect_setup.log`, а также обратитесь к статье базы знаний.
7	Ошибка установки File Protector на целевой машине с ОС Linux.	Для получения более подробной информации воспользуйтесь журналом `/var/log/cyberprotect_setup.log`, а также обратитесь к статье базы знаний.
8	Не удалось инициализировать сервисы.	Обратитесь к специалистам Киберпротект.
9	Не удалось создать группу ”acronis”.	Обратитесь к специалистам Киберпротект.

Удаление агентов для ОС Linux, установленных из RPM-репозитория

Для удаления агента для ОС Linux, установленного из RPM-репозитория, на целевой машине выполните команду от имени привилегированного пользователя (root):

```
dnf remove CyberBackupAgent
```

Эта команда удалит также пакеты зависимостей (`BackupAndRecoveryAgent`, `BackupAndRecoveryBootableComponents`, `dkms`, `file_protector`, `snapapi26_modules`), если ранее они были установлены вместе с агентом.

Если пакеты зависимостей были установлены отдельно от агента, удалите их вручную. Например, выполните следующую команду от имени привилегированного пользователя (root):

```
dnf remove BackupAndRecoveryAgent BackupAndRecoveryBootableComponents dkms file_protector¬
↪snapapi26_modules
```

Ручная установка агента для VMware (виртуальное устройство) из шаблона OVF

Перед началом

Системные требования для агента

По умолчанию виртуальному устройству назначается 4 ГБ ОЗУ и 2 виртуальных ЦП. Для большинства операций этого достаточно. Чтобы повысить производительность резервного копирования в случае, когда ожидается, что скорость передачи трафика резервного копирования превысит 100 МБ в секунду (например, в сетях с пропускной способностью 10 Гбит/с), рекомендуем повысить объем ОЗУ до 8 ГБ и использовать 4 виртуальных ЦП.

Виртуальные диски устройства занимают не более 6 ГБ. Формат диска (”толстый” или ”тонкий”) не влияет на производительность устройства.

Необходимое число агентов

Несмотря на то, что одно виртуальное устройство может защитить всю среду vSphere, рекомендуется развернуть по одному виртуальному устройству на каждый кластер vSphere (или на каждый хост при отсутствии кластера). Это позволит ускорить процессы резервного копирования, поскольку устройство с помощью транспорта HotAdd может присоединить диски, для которых созданы резервные копии. В этом случае трафик резервного копирования направляется от одного локального диска к другому.

Вполне нормально одновременно использовать виртуальное устройство и агент для VMware (Windows), когда они подключены к одному vCenter Server *или* разным хостам ESXi. Избегайте сценариев, когда

один агент подключен к хосту ESXi напрямую, а другой агент подключен к vCenter Server, который управляет этим хостом ESXi.

Если у вас несколько агентов, не рекомендуем использовать локальное хранилище данных (т. е. хранить резервные копии на виртуальных дисках, добавленных в виртуальное устройство). Дополнительную информацию см. в разделе *Использование локально присоединенного хранилища*.

Отключить автоматический DRS для агента

Если виртуальное устройство развернуто в кластере vSphere, убедитесь, что для него отключено автоматическое применение vMotion. В настройках DRS кластера включите уровни автоматизации отдельной виртуальной машины. После этого задайте параметру **Уровень автоматизации** виртуального устройства значение **Отключено**.

Развертывание шаблона OVF

Чтобы развернуть шаблон OVF, выполните следующие действия:

1. Скачайте пакет установки агента для VMware с сайта компании и извлеките его из архива, чтобы получить файл OVA.
2. Убедитесь, что файлы шаблона OVF доступны с машины, на которой выполняется клиент vSphere.
3. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
4. Разверните шаблон OVF.
    - При настройке хранилища данных выберите общее хранилище данных, если оно существует. Формат диска (”толстый” или ”тонкий”) не имеет значения, поскольку не влияет на производительность устройства.
    - При настройке сетевых подключений выберите сеть с сервером управления.

Настройка виртуального устройства

1. **Запуск виртуального устройства**

   В клиенте vSphere откройте раздел **Инвентаризация**, щёлкните правой кнопкой имя виртуального устройства и выберите команду **Питание** → **Включить**. Выберите вкладку **Консоль**.

2. **Прокси-сервер**

   Если в вашей сети есть прокси-сервер:

   1. Чтобы запустить командную оболочку, в пользовательском интерфейсе виртуального устройства нажмите клавиши CTRL+SHIFT+F2.

2. Откройте файл `/etc/Acronis/Global.config` в текстовом редакторе.
3. Выполните одно из следующих действий:
   - Если параметры прокси-сервера были заданы во время установки агента, найдите следующий раздел:

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - В противном случае скопируйте приведенные выше строки и вставьте в файл между тегами `<registry name="Global">...</registry>`.
4. Замените `АДРЕС` новым именем хоста или IP-адресом прокси-сервера, а `ПОРТ` — номером порта в десятичном формате.
5. Если на прокси-сервере необходимо пройти аутентификацию, вместо дескрипторов `ИМЯ ВХОДА` и `ПАРОЛЬ` укажите учетные данные прокси-сервера. В противном случае удалите эти строки из файла.
6. Сохраните файл.
7. Откройте файл `/opt/acronis/etc/aakore.yaml` в текстовом редакторе.
8. Найдите раздел `env` или создайте его и добавьте туда следующие строки:

   ```
   env:
    http-proxy: proxy_login:proxy_password@proxy_address:port
    https-proxy: proxy_login:proxy_password@proxy_address:port
   ```

9. Вместо `proxy_login` и `proxy_password` укажите учетные данные прокси-сервера, а вместо `proxy_address:port` — адрес и номер порта прокси-сервера.
10. Выполните команду `reboot`.

В противном случае пропустите этот шаг.

3. **Сетевые настройки**

Сетевое подключение агента настраивается автоматически с помощью протокола DHCP. Чтобы изменить конфигурацию по умолчанию, в подразделе **eth0** раздела **Параметры агента** нажмите

кнопку **Изменить** и укажите нужные сетевые настройки.

4. **vCenter/ESX(i)**

   В окне **Параметры агента** в области **vCenter/ESX(i)** нажмите кнопку **Изменить** и укажите имя или IP-адрес vCenter Server. Агент сможет выполнять резервное копирование и восстановление любых виртуальных машин, управляемых vCenter Server.

   Если vCenter Server не используется, укажите имя или IP-адрес хоста ESXi, резервное копирование и восстановление виртуальных машин которого необходимо выполнить. Обычно резервное копирование происходит быстрее, когда агент создает резервные копии виртуальных машин, размещенных на его собственном хосте.

   Укажите учетные данные, которые будут использоваться агентом для подключения к vCenter Server или ESXi. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с *необходимыми привилегиями* на хосте vCenter Server или ESXi.

   С помощью команды **Проверить подключение** можно проверить правильность учетных данных для доступа.

5. **Сервер управления**

   1. На **сервере управления** в разделе **Параметры агента** щёлкните **Изменить**.
   2. В разделе **Имя/IP-адрес сервера** выберите **Локальное**. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   3. В полях **Имя пользователя** и **Пароль** укажите имя пользователя и пароль администратора сервера управления.

6. **Часовой пояс**

   В разделе **Виртуальная машина** в подразделе **Часовой пояс** нажмите кнопку **Изменить**. Выберите свой часовой пояс, чтобы запланированные операции выполнялись в правильное время.

   После изменения часового пояса перезагрузите виртуальное устройство.

7. **[Необязательно] Локальные хранилища данных**

   К виртуальному устройству можно присоединить дополнительный диск, чтобы агент для VMware мог сохранять резервные копии на этом *локально присоединенном хранилище*.

   Добавьте диск, изменив параметры виртуальной машины и нажав кнопку **Обновить**. Ссылка **Создать хранилище** станет доступной. Щёлкните эту ссылку, выберите диск и задайте для него метку.

Порядок обновления агента для VMware (виртуального устройства) в веб-консоли Кибер Бэкап

1. Щёлкните **Настройки** → **Агенты**.

   В программе будет выведен список машин. Машины с агентами устаревших версий будут помечены оранжевым восклицательным знаком.

2. Выберите машины, на которых нужно обновить агенты. Машины должны быть включены.

3. Щёлкните **Обновить агент**.

Примечание

При выполнении обновления все выполняющиеся резервные копии завершатся сбоем.

Порядок обновления агента для VMware (виртуальное устройство) версий, более ранних, чем 12.5.23094

1. Удалите агент для VMware (виртуальное устройство), как описано в разделе *Удаление продукта*. В шаге 5 удалите агент из раздела **Настройки** → **Агенты**, даже если вы планируете установить агент снова.

2. Разверните агент для VMware (виртуальное устройство), как описано в разделе *Развертывание шаблона OVF*.

3. Настройте агент для VMware (виртуальное устройство), как описано в разделе *Настройка виртуального устройства*.

   Чтобы восстановить локальное хранилище данных, в шаге 7 выполните следующие действия:

   1. Добавьте на виртуальное устройство диск с локальным хранилищем данных.
   2. Последовательно выберите пункты **Обновить** → **Создать хранилище** → **Подключить**.
   3. В программе отображается оригинальная **буква** и **метка** диска. Не меняйте их.
   4. Нажмите кнопку **ОК**.

   В результате планы защиты, примененные к старому агенту, автоматически применяются к новому агенту.

4. Для планов с включенным резервным копированием с поддержкой приложений необходимо заново ввести учетные данные гостевой ОС. Измените эти планы и заново введите учетные данные.

5. Для планов, которые выполняют резервное копирование конфигурации ESXi, необходимо заново ввести пароль привилегированного пользователя (root). Измените эти планы и заново введите пароль.

Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация)

Для развертывания агента oVirt вам понадобятся установленные и настроенные системы:

- Система управления виртуализацией (например, ROSA Virtualization).
- Решение Кибер Бэкап.

Кроме того, агенту нужно предоставить права пользователя со следующими ролями:

- oVirt/RHV версии 4.3: DiskCreator, UserVmManager, TagManager, UserVmRunTimeManager, VmCreator;
- oVirt/RHV версии 4.4 и новее: SuperUser.

  Начиная с версии oVirt 4.4, создание новых дисков без прав учетной записи SuperUser невозможно.

По умолчанию используется учетная запись admin@internal или admin@zvirt@internal.

Вы можете установить агент двумя способами:

- *Автоматически* из интерфейса Кибер Бэкап.
- *Вручную*, используя установочный файл агента oVirt в формате OVA.

После установки настройте агент в системе управления виртуализацией (например, ROSA Virtualization) и *создайте план защиты ваших виртуальных устройств*.

Настройка LDAP-аутентификации для агента для zVirt

Система управления виртуализацией zVirt, благодаря интеграции с системой управления учетными данными и доступом Keycloack, позволяет подключать службы каталогов (например, Active Directory, FreeIPA или SambaDC), предоставлять доступ в ее порталы пользователям служб каталогов, разрешать им выполнение операций. Список поддерживаемых служб каталогов см. в документации zVirt.

Для того чтобы можно было использовать учетные данные пользователя службы каталогов при настройке виртуального устройства (агента для zVirt), необходимо выполнить следующие действия:

1. На портале Keycloack подключите необходимую службу каталогов согласно инструкции в документации zVirt.
2. Подготовьте учетные данные пользователя службы каталога. Можно использовать существующего пользователя или создать нового.
3. На портале администрирования zVirt:

1. В разделе **Управление** → **Пользователи** добавьте пользователя службы каталогов. При добавлении в поле **Поиск** необходимо выбрать **internalsso (...)**.
2. Предоставьте добавленному пользователю такие же разрешения, как у пользователя `admin`.

4. Убедитесь, что можно войти на портал управления zVirt с учетными данными этого пользователя.

После выполнения этих действий можно будет использовать учетные данные пользователя службы каталогов для автоматической или ручной настройки виртуального устройства. Имя пользователя необходимо указать в формате `<name>@internalsso`.

Автоматическая установка агента для oVirt

> **Примечание**
>
> Убедитесь, что у сервера управления есть доступ к дистрибутиву через сеть Интернет. Если доступ есть, переходите сразу к установке агента (п.4 и далее). Если у сервера управления нет интернет-доступа к дистрибутиву, вначале загрузите дистрибутив вручную на хост с вашими виртуальными машинами, для которых вы будете использовать Кибер Бэкап, по SSH или другим доступным способом, и поместите в папку (см. п.3), не распаковывая его.

Чтобы установить агент, выполните действия:

1. Перейдите на страницу обновления Кибер Бэкап.
2. Нажмите **Скачать** рядом с файлом **Пакет установки агента для oVirt**.
3. Загрузите файл дистрибутива агента для oVirt и поместите его в папку на сервере управления Кибер Бэкап:
   - `C:\ProgramData\Acronis\VaDeployer\va-images` (Windows),
   - `/var/lib/Acronis/VaDeployer/va-images` (Linux).
4. Войдите в веб-консоль Кибер Бэкап.
5. Добавьте лицензию:
   1. Откройте раздел **Настройки** → **Лицензии**.
   2. Нажмите кнопку **Добавить ключи**.
   3. В поле введите один или несколько лицензионных ключей в формате XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX-XXXXXXXX.
   4. Нажмите кнопку **Добавить**.

6. Добавьте виртуальное устройство:

    1. Откройте раздел **Устройства** → **Физические и виртуальные машины**.
    2. В правом верхнем углу окна нажмите кнопку **Добавить**.
    3. В окне **Добавить устройства** в разделе **Платформы виртуализации** выберите один из вариантов в зависимости от системы oVirt, которую вы используете:
        - Red Hat Virtualization (oVirt),
        - ROSA Virtualization (oVirt),
        - zVirt (oVirt),
        - РЕД Виртуализация (oVirt).
    4. В открывшемся окне введите параметры сервера.

        Например, если вы выбрали ROSA Virtualization (oVirt), укажите имя или IP-адрес сервера ROSA Virtualization (например, `https://my-ovirt`), имя пользователя (например, `admin@internal`) и пароль доступа к ROSA Virtualization.

        > **Примечание**
        >
        > При установке агента в систему управления виртуализацией zVirt имя пользователя службы каталогов необходимо указать в формате `<name>@internalsso`. Подробные сведения см. в разделе *Настройка LDAP-аутентификации для агента для zVirt*.

    5. В списке выберите доменное имя или IP-адрес сервера управления Кибер Бэкап.
    6. Нажмите кнопку **Настройки**.
    7. В окне дополнительных настроек задайте имя виртуального устройства, выберите кластер, домен и сеть, с которыми будет взаимодействовать виртуальное устройство. Если вы хотите автоматически получить сетевые параметры по DHCP, установите флажок.
    8. Нажмите кнопку **Развернуть**.

Агент будет установлен и появится в системе oVirt в списке виртуальных машин под именем `ovirt_virtual_appliance`.

Ручная установка агента для oVirt

Чтобы установить агент вручную, выполните действия:

1. Скачайте дистрибутив агента oVirt (файл формата OVA).
2. Загрузите дистрибутив на хост с вашими виртуальными машинами, для которых вы будете использовать Кибер Бэкап, по SSH или другим доступным способом.
3. Распакуйте архив, выполнив команду `bzip2 -d <полное имя файла с версией>.ova`. Например: `bzip2 -d OVirtAppliance_v15.0.25879.ova`.
4. Войдите в систему ROSA Virtualization через браузер.
5. В списке ресурсов выберите **Виртуальные машины**.
6. В меню действий над виртуальными машинами выберите **Импорт**.
7. В открывшейся форме задайте следующие параметры:
   - Дата-центр, в котором находится хост, на который вы загрузили OVA-файл.
   - Источник: Виртуальное устройство (OVA).
   - Имя хоста, на который вы загрузили OVA-файл.
   - Путь к файлу - полный путь к директории, в которую вы загрузили OVA-файл.
8. Нажмите кнопку **Загрузить**. Загруженный OVA-файл появится в списке Виртуальные машины источника. `Внимание! Если OVA-файл с дистрибутивом агента не появился в списке, убедитесь, что вы указали корректный путь к файлу и что архив с дистрибутивом не поврежден.`
9. Выберите OVA-файл `ovirt_virtual_appliance` в списке и переместите его в список **Виртуальные машины для импорта**.
10. Нажмите кнопку **Далее**.
11. В открывшемся окне укажите домен и кластер, в который вы хотите установить агент.
12. Нажмите на имя виртуального устройства. Раскроется меню.
13. Выберите вкладку **Сетевые интерфейсы**.
14. Задайте имя сети `ovirtmgmt` и профиль `ovirtmgmt`.
15. Нажмите кнопку **OK**.

Выполненные действия должны привести к следующим результатам:

Агент oVirt будет установлен и появится в списке виртуальных машин под именем `ovirt_virtual_appliance`.

Настройка агента в ROSA Virtualization

Независимо от того, каким способом вы установили агент ROSA Virtualization (oVirt), необходимо его настроить.

Чтобы настроить агент в ROSA Virtualization, выполните действия:

1. Войдите в систему ROSA Virtualization через браузер.
2. В списке ресурсов выберите **Виртуальные машины**.
3. В списке виртуальных машин выберите **ovirt_virtual_appliance**.
4. В меню выберите **Консоль** и откройте консоль. Вы увидите интерфейс настройки агента ROSA Virtualization (oVirt).
5. Чтобы изменить параметры в консоли, выберите параметр и нажмите **Change**, затем **OK**.

   Настройте следующие параметры:

   oVirt

   Укажите имя или адрес сервера ROSA Virtualization, на который вы устанавливаете агент (например, `https://my-ovirt`), имя пользователя (например, `admin@internal`) и пароль доступа к ROSA Virtualization. Нажмите **Check connection** чтобы проверить соединение. Ошибки при подключении могут указывать как на некорректность введенных данных, так и на проблемы с сетью.

   > **Примечание**
   >
   > При настройке агента для системы управления виртуализацией zVirt имя пользователя службы каталогов необходимо указать в формате `<name>@internalsso`. Подробные сведения см. в разделе *Настройка LDAP-аутентификации для агента для zVirt*.

   Management Server

   Укажите имя или IP-адрес компьютера, на котором установлено решение Кибер Бэкап, имя пользователя и пароль доступа к нему.

   Eth0

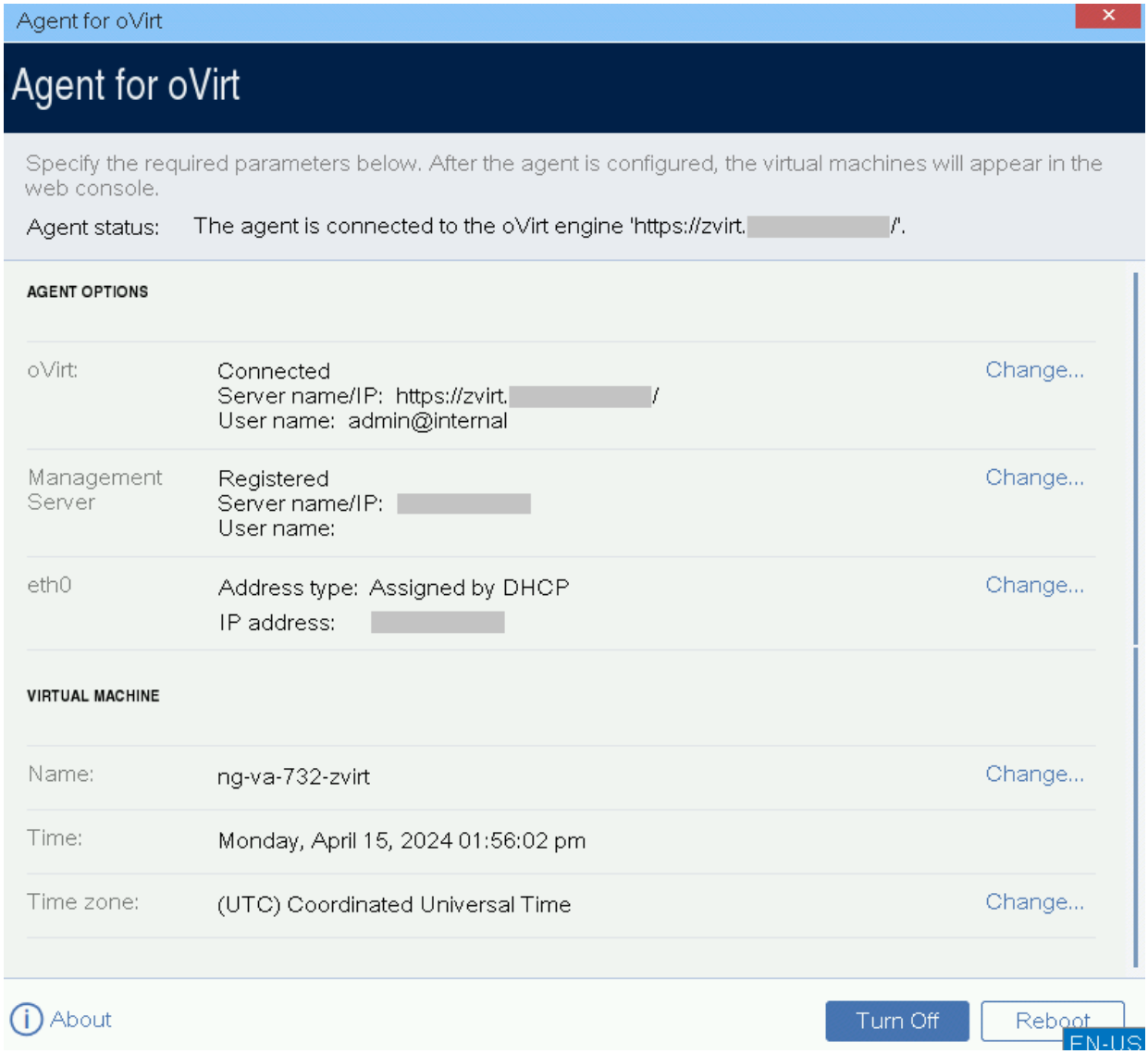
   Если необходимо, задайте параметры сетевого интерфейса, для которого вы будете использовать агент (IP-адрес, маску сети, шлюз и DNS). По умолчанию используется DHCP.

   Name

   Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.

Time zone

Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.



Выполненные действия должны привести к следующим результатам в веб-консоли Кибер Бэкап:

- в разделе **Настройки** → **Агенты** отобразится агент ROSA Virtualization (oVirt),
- в разделе **Устройства** появится подраздел oVirt.

Развертывание резервного копирования для Кибер Инфраструктуры

Общие сведения

Для развертывания резервного копирования для продукта Кибер Инфраструктура вам понадобятся установленные и настроенные системы:

- Решение Кибер Инфраструктура (список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*).
- Решение Кибер Бэкап.

Установка проводится в несколько этапов:

- Создание и регистрация пользователя.
- Установка виртуального устройства.
- Подключение виртуального устройства к серверу управления.

Известные проблемы и ограничения

- Восстановление невозможно, если выполнено резервное копирование машины, на которой находятся сервер управления и агент. Восстановление с Кибер Инфраструктурой компьютера с системным диском, на котором находится сервер управления, завершается ошибкой ”Не удалось подключиться к службе ядра агента на этом компьютере”.
- Виртуальное устройство оперирует данными обо всех виртуальных машинах во всех доменах, вне зависимости от того в каком домене оно развернуто, и передает их серверу управления, в то время как пользователь не должен иметь доступ за пределы своего домена. В результате сервер управления имеет доступ к машинам за пределами домена виртуального устройства. Эти машины доступны для резервного копирования, но восстановление в домены за пределами виртуального устройства невозможно.

Создание и регистрация пользователя

Для настройки виртуального устройства необходимо создать специального пользователя в Кибер Инфраструктуре и предоставить ему доступ ко всем проектам с виртуальными машинами, для которых требуется выполнять резервное копирование и восстановление. Этого пользователя можно создать в любом домене и назначить ему любую роль.

Для получения подробной информации об управлении пользователями см. раздел ”Управление доменами, пользователями и проектами” в руководстве администратора продукта Кибер Инфраструктура.

Чтобы предоставить пользователю доступ ко всем проектам домена, выполните следующие действия на сервере управления Кибер Инфраструктуры:

1. Подготовьтесь для работы с интерфейсом командной строки OpenStack с правами администратора системы:
    1. Создайте RC-файл для OpenStack, в котором указаны учетные данные администратора системы.

```
su - vstoradmin
kolla-ansible post-deploy
exit
```

2. Задайте переменные среды, необходимые для клиента командной строки OpenStack.

```
. /etc/kolla/admin-openrc.sh
```

2. Предоставьте пользователю доступ.

```
openstack --insecure user set --project <project> --project-domain <project-domain> --domain
↪<user-domain> <username>
openstack --insecure role add --domain <project-domain> --user <username> --user-domain
↪<user-domain> admin --inherited
```

В этих командах:

- `<project-domain>` — имя целевого домена с проектами, к которым будет предоставлен доступ.
- `<project>` — имя любого проекта из целевого домена.
- `<user-domain>` — имя домена пользователя, которому будет предоставлен доступ.
- `<username>` — имя пользователя Кибер Инфраструктуры. Виртуальное устройство будет использовать этого пользователя для резервного копирования и восстановления виртуальных машин в проектах целевого домена.

При необходимости можно просмотреть роли, назначенные пользователю Кибер Инфраструктуры.

- Команда `openstack --insecure role assignment list --user <username> --names` выводит только те роли, которые назначены пользователю `<username>` явно, например:

```
openstack --insecure role assignment list --user johndoe --names
+--------------+-----------------+-------+---------+-------------+--------+-----------+
| Role         | User            | Group | Project | Domain      | System | Inherited |
+--------------+-----------------+-------+---------+-------------+--------+-----------+
| admin        | johndoe@Default |       |         | MyNewDomain |        | True      |
| compute      | johndoe@Default |       |         | Default     |        | True      |
| domain_admin | johndoe@Default |       |         | Default     |        | True      |
| domain_admin | johndoe@Default |       |         | Default     |        | False     |
+--------------+-----------------+-------+---------+-------------+--------+-----------+
```

- Команда `openstack --insecure role assignment list --user <username> --names --effective` выводит список всех ролей, назначенных пользователю `<username>` как явно, так и неявно,

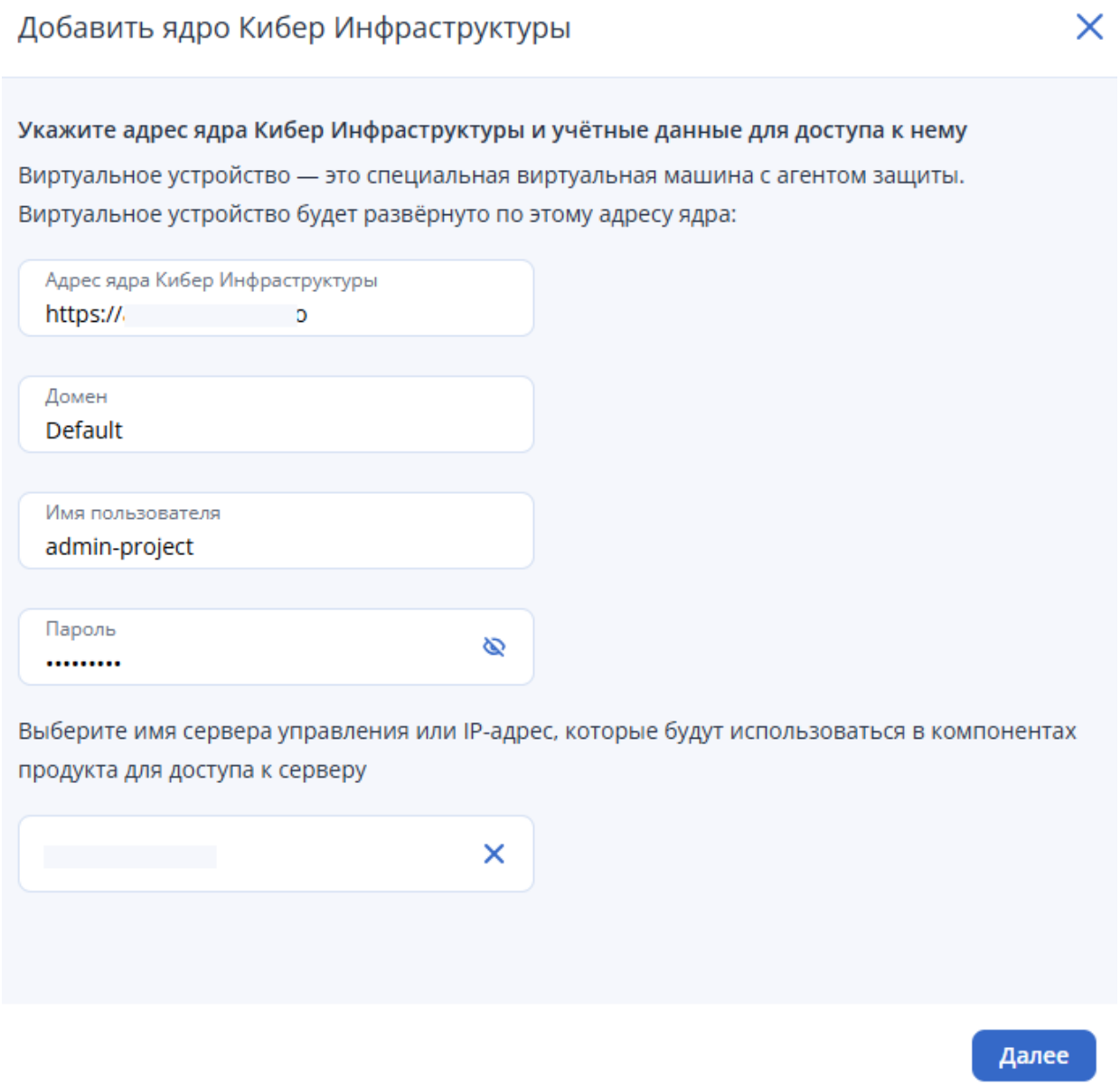
например:

```
openstack --insecure role assignment list --user johndoe --names --effective
+--------------+-----------------+-------+-----------------+---------+--------+-----------+
| Role         | User            | Group | Project         | Domain  | System | Inherited |
+--------------+-----------------+-------+-----------------+---------+--------+-----------+
| domain_admin | johndoe@Default |       |                 | Default |        | False     |
| compute      | johndoe@Default |       | admin@Default   |         |        | True      |
| compute      | johndoe@Default |       | service@Default |         |        | True      |
| domain_admin | johndoe@Default |       | admin@Default   |         |        | True      |
| domain_admin | johndoe@Default |       | service@Default |         |        | True      |
| project_user | johndoe@Default |       | service@Default |         |        | True      |
| member       | johndoe@Default |       | service@Default |         |        | True      |
| reader       | johndoe@Default |       | service@Default |         |        | True      |
| project_user | johndoe@Default |       | admin@Default   |         |        | True      |
| member       | johndoe@Default |       | admin@Default   |         |        | True      |
| reader       | johndoe@Default |       | admin@Default   |         |        | True      |
| project_user | johndoe@Default |       |                 | Default |        | False     |
| member       | johndoe@Default |       |                 | Default |        | False     |
| reader       | johndoe@Default |       |                 | Default |        | False     |
+--------------+-----------------+-------+-----------------+---------+--------+-----------+
```

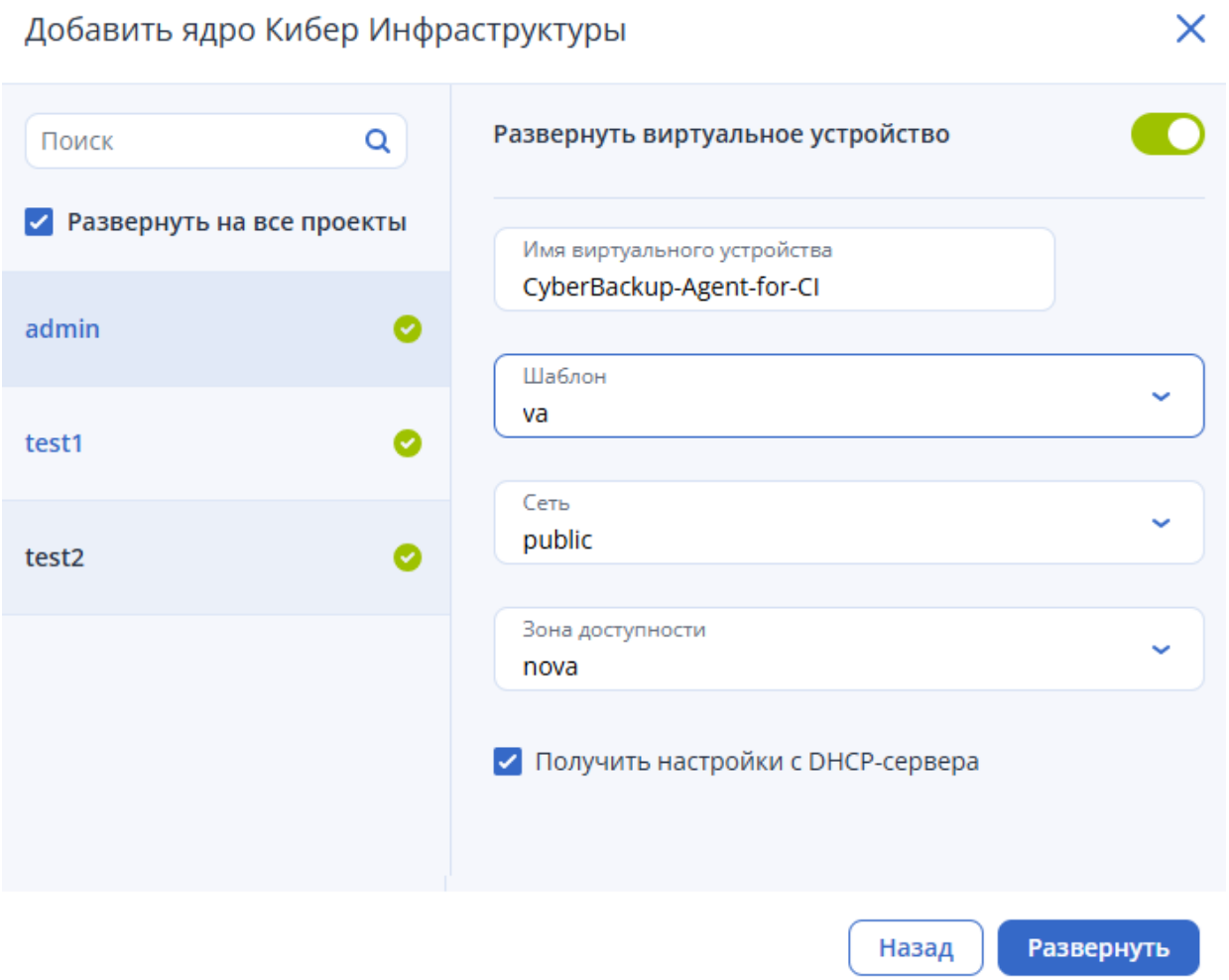
Автоматическая установка агента для Кибер Инфраструктуры

Чтобы добавить хост Кибер Инфраструктуры на сервер управления и автоматически развернуть агент, выполните следующие шаги в веб-интерфейсе Кибер Бэкап:

1. На вкладке **Устройства** → **Физические и виртуальные машины** щёлкните **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **Платформы виртуализации** выберите **Кибер Инфраструктура**. Откроется окно **Добавить ядро Кибер Инфраструктуры**.



3. В поле **Адрес ядра Кибер Инфраструктуры** укажите адрес сервера управления Кибер Инфраструктуры.
4. В поле **Домен** укажите домен Кибер Инфраструктуры.
5. В соответствующих полях укажите имя пользователя и пароль пользователя в Кибер Инфраструктуре с правами в целевом домене (см. раздел *Создание и регистрация пользователя*).
6. Нажмите **Далее**. Откроется окно **Добавить ядро Кибер Инфраструктуры**.



7. Для каждого необходимого проекта включите ползунок **Развернуть виртуальное устройство** и укажите параметры виртуального устройства:
   - **Имя виртуального устройства**.
   - **Шаблон**. Необходимо минимум 4 ГБ ОЗУ, 2 ядра ЦП и 8 ГБ дискового пространства.
   - **Сеть**. Должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап.
   - **Зона доступности**.
8. При необходимости можно снять флажок **Получить настройки с DHCP-сервера** и указать параметры сети вручную.
9. Указав необходимые параметры, нажмите **Развернуть**.

В Кибер Инфраструктуре будет создано виртуальное устройство, на которое будет установлен агент. При этом пакет установки агента для Кибер Инфраструктуры будет загружен с официального сайта Киберпротект. Если это невозможно, архив агента будет взят локально с машины, на которой установлен сервер управления Кибер Бэкап: из директории `C:\ProgramData\Acronis\VaDeployer\va-images` (в ОС

Windows) или из директории `/var/lib/Acronis/VaDeployer/va-images` (в ОС Linux).

Перейдите в **Настройки** → **Агенты** и убедитесь, что в списке появился агент для резервного копирования Кибер Инфраструктуры.

Установка агента для Кибер Инфраструктуры вручную

Чтобы установить агент:

1. Скачайте пакет установки агента для Кибер Инфраструктуры, распакуйте его, извлеките файл `CIAppliance.qcow2`.
2. В Кибер Инфраструктуре перейдите в **Вычисления** → **Виртуальные машины** → **Образы** и нажмите **Добавить образ**.
3. В поле **Файл образа** укажите путь к нужному образу виртуальной машины.
4. При необходимости в поле **Имя** измените наименование образа.
5. В поле **Выберите дистрибутив ОС** укажите нужный дистрибутив и нажмите **Добавить**.
6. Перейдите на вкладку **Виртуальные машины** и нажмите **Создать виртуальную машину**.
7. В разделе **Образ** нажмите **Укажите** и в открывшемся окне выберите необходимый образ.
8. В разделе **Тип ВМ** нажмите **Укажите** и в открывшемся окне выберите тип ВМ. Для промышленных сборок рекомендуется выбрать тип ВМ, содержащий как минимум 2 ЦП и 4 ГБ памяти.
9. В разделе **Сетевые интерфейсы** нажмите **Укажите** и в открывшемся окне выберите подходящий сетевой интерфейс. Нажмите **Добавить** и в поле **Сеть** выберите нужный сетевой интерфейс. Убедитесь, что виртуальное устройство имеет доступ к внутренним сетям кластера со следующими типами трафика (сети и назначенные им типы трафика можно просмотреть в разделе **Инфраструктура** → **Сети**):
   - **VM backups**,
   - **Compute API**,
   - **Storage** (не обязательно).

   Доступ к **VM backups** разрешает передачу данных от виртуальной машины к резервным копиям и обратно. Доступ к **Compute API** позволяет использовать дополнительные возможности, например, взаимодействие с OpenStack, создание моментальных снимков резервных копий.
10. Введите имя виртуальной машины и по окончании ввода данных нажмите **Развернуть**.
11. Перейдите снова в раздел **Виртуальные машины** и убедитесь, что имя виртуальной машины появилось в списке виртуальных машин.

Примечание

Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Подключение виртуального устройства к серверу управления

1. Перейдите в **Вычисления** → **Виртуальные машины**.
2. В списке виртуальных машин выберите имя виртуальной машины и перейдите в **Консоль**.
3. В поле **Server name/IP** введите адрес сервера управления Кибер Инфраструктуры в формате `https://<address>:5000`.
4. В поле **User domain name** укажите имя системного домена.
5. В остальных полях укажите нужные параметры, нажмите **Check connection**, чтобы проверить соединение и затем **OK**.
6. В открывшемся окне **Register agent** укажите данные для подключения к серверу управления Кибер Бэкап и нажмите **OK**.
7. В открывшемся окне **Rename Agent for Cyber Infrastructure** введите имя агента Кибер Инфраструктуры и нажмите **Отправить комбинацию клавиш**.
8. По окончании настроек откройте Кибер Бэкап и выберите вкладку **Устройства**. Убедитесь, что в подменю слева появилась вкладка **Кибер Инфраструктура**.
9. Перейдите в **Настройки** → **Агенты** и убедитесь, что в списке агентов появился агент для резервного копирования Кибер Инфраструктуры.

Ручная установка агента для SpaceVM

Для развертывания агента для SpaceVM и настройки его интеграции с Кибер Бэкап вам понадобятся установленные и настроенные системы:

- Система SpaceVM версии (список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*).
- Решение Кибер Бэкап.

Планирование количества агентов для SpaceVM

Чтобы создавать резервные копии всех виртуальных машин, как правило, нужно развернуть несколько агентов для SpaceVM. Это связано с тем, что агенты могут получить доступ только к пулам данных, подключенным к серверу (хосту), на котором развернут агент.

Если вы используете только локальные пулы данных, разверните по одному агенту для SpaceVM на каждом сервере.

Если вы используете общие пулы данных, доступные на всех серверах, достаточно развернуть один агент для SpaceVM.

Дополнительные агенты также могут потребоваться в ситуации, когда в системе имеется очень большое число виртуальных машин, и суммарное время создания резервных копий окажется слишком большим.

Процедура развертывания

Выполняйте действия по развертыванию агента для SpaceVM в следующем порядке:

1. *Установите продукт*.
2. *Установите необходимое количество агентов для SpaceVM*.
3. *Создайте план защиты виртуальных машин*.

Известные проблемы и ограничения

1. Текущие версии платформы SpaceVM не позволяют осуществлять резервное копирование следующих типов виртуальных машин:
    - виртуальные машины, являющиеся ”тонким клоном”, в которых уже после операции создания ”тонкого клона” был изменен набор дисков;
    - виртуальные машины с SCSI-контроллером типа lsilogic.
2. Текущие версии платформы SpaceVM не поддерживают резервное копирование с хранилищ LVM ввиду ограничений самой платформы - моментальные снимки на хранилищах этого типа невозможны.
3. Резервное копирование доступно лишь для виртуальных машин в пределах той локации, в которой развернуто виртуальное устройство. Если виртуальное устройство расположено на любом хосте в пределах одной локации, резервное копирование доступно для:
    - виртуальных машин, расположенных на всех хранилищах того же хоста;
    - всех виртуальных машин, которые находятся на сетевых хранилищах всех хостов в пределах этой локации.

4. Виртуальные машины, являющиеся ”тонким клоном”, можно восстановить только в новые ВМ.

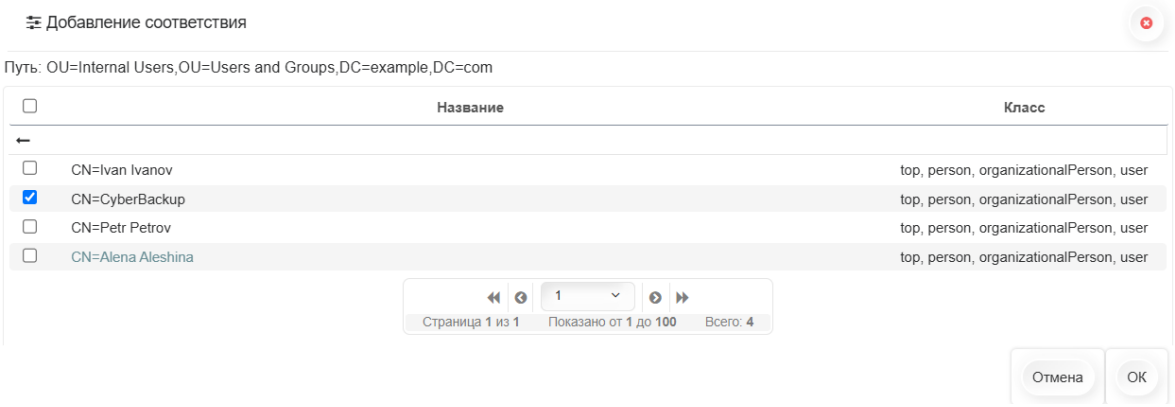
Настройка LDAP-аутентификации для агента для SpaceVM

Если система виртуализации использует службу каталогов для аутентификации пользователей, то перед развертыванием агента выполните дополнительную настройку службы:

1. В веб-панели управления системой виртуализации перейдите в раздел **Безопасность** → **Службы каталогов**.
2. Щелкните по имени службы каталогов и перейдите в раздел **Соответствия**.
3. Нажмите **Добавить соответствие** и выполните следующие действия в окне **Добавление соответствия**:
    1. Укажите имя для соответствия.
    2. Выберите роли **Администратор** и **Администратор безопасности**.
    3. Введите описание соответствия.
    4. Нажмите **Добавить объекты LDAP** и добавьте LDAP-объект, представляющий пользователя, от имени которого агент будет выполнять операции резервного копирования и восстановления в системе виртуализации. При необходимости можно добавить LDAP-объект, представляющий группу, в которую входит требуемый пользователь.

        Чтобы просмотреть дочерние LDAP-объекты некоторого LDAP-объекта, щелкните по его имени в списке. Чтобы добавить LDAP-объект, поставьте галочку рядом с его именем и нажмите **OK**.

        Пример для Active Directory:

    5. Нажмите **OK**, чтобы завершить создание соответствия.
4. Убедитесь, что пользователь, для которого создано соответствие, может войти в веб-панель управления системой виртуализации и обладает в ней указанными ролями.

Установка агента для SpaceVM

Чтобы установить агент для SpaceVM, выполните следующие действия:

1. Загрузите пакет установки агента для SpaceVM и извлеките из архива файл пакета (например, `file.ova`).
2. Войдите в систему SpaceVM через браузер.
3. В консоли управления SpaceVM в меню слева перейдите в раздел **Хранилища** → **Файлы**.
4. В верхнем меню выберите **Загрузить из файловой системы**.
5. В файловой системе выберите распакованный на первом шаге файл, далее выберите пул данных, по возможности доступный на всех хостах, и нажмите **OK**.
6. После завершения загрузки файла нажатием на имя файла раскройте его свойства.
7. В верхнем меню выберите **Обновить информацию**, подтвердите свое решение нажатием на кнопку **Да**.
8. В верхнем меню выберите **Конфигурация копии ВМ**.
9. В открывшемся окне выберите **Восстановление ВМ**, укажите узел, на который вы хотите восстановить виртуальную машину, нажмите **OK**.
10. После завершения создания виртуальной машины на указанном узле в меню слева перейдите в раздел **Виртуальные машины**.
11. В списке виртуальных машин выберите созданную виртуальную машину. Имя виртуальной машины по умолчанию: ”CyberBackup_Agent_for_SpaceVM”. Если вы планируете развернуть несколько виртуальных машин, рекомендуется переименовать каждую из них.
12. В открывшемся окне запустите эту виртуальную машину нажатием на стрелку в верхнем меню.
13. Подключитесь к консоли виртуальной машины: на мини-экране ВМ выберите **VNC** или **Spice**.
14. После завершения запуска виртуальной машины в консоли переходите по ссылкам **Change...** для настройки параметров:

    1. Укажите адрес контроллера SpaceVM (например, `https://space.my-company.ru`), имя пользователя (например, `admin`) и пароль доступа к SpaceVM.

       Если система SpaceVM использует службу каталогов для аутентификации пользователей, установите флажок **Use LDAP authentication**.

       Нажмите **Check connection**, чтобы проверить соединение. Ошибки при подключении могут указывать как на некорректность введенных данных, так и на проблемы с сетью.

2. Укажите имя или IP-адрес сервера управления — компьютера, на котором установлено решение Кибер Бэкап, имя пользователя и пароль доступа к нему.
3. Если необходимо, задайте параметры сетевого интерфейса Eth0 (IP-адрес, маску сети, шлюз и DNS). По умолчанию используется DHCP.
4. Если вы планируете развернуть несколько агентов для SpaceVM, измените имя агента для SpaceVM. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
5. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

15. При необходимости установите агент на других серверах, выполняя шаги установки из этой инструкции.

Выполненные действия должны привести к следующим результатам:

- В веб-консоли Кибер Бэкап в разделе **Настройки** → **Агенты** отобразится агент для SpaceVM;
- В веб-консоли Кибер Бэкап в разделе **Устройства** появятся устройства SpaceVM.

Ручная установка агента для ECP VeiL

Для развертывания агента для ECP VeiL и настройки его интеграции с Кибер Бэкап вам понадобятся установленные и настроенные системы:

- Система ECP VeiL (список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*).
- Решение Кибер Бэкап.

Планирование количества агентов для ECP VeiL

Чтобы создавать резервные копии всех виртуальных машин, как правило, нужно развернуть несколько агентов для ECP VeiL. Это связано с тем, что агенты могут получить доступ только к пулам данных, подключенным к серверу (хосту), на котором развернут агент.

Если вы используете только локальные пулы данных, разверните по одному агенту для ECP VeiL на каждом сервере.

Если вы используете общие пулы данных, доступные на всех серверах, достаточно развернуть один агент для ECP VeiL.

Дополнительные агенты также могут потребоваться в ситуации, когда в системе имеется очень большое число виртуальных машин, и суммарное время создания резервных копий окажется слишком большим.

Процедура развертывания

Выполняйте действия по развертыванию агента для ECP VeiL в следующем порядке:

1. *Установите продукт*.
2. *Установите необходимое количество агентов для ECP VeiL*.
3. *Создайте план защиты виртуальных машин*.

Известные проблемы и ограничения

1. Текущие версии платформы ECP VeiL не позволяют осуществлять резервное копирование следующих типов виртуальных машин:
    - виртуальные машины, являющиеся ”тонким клоном”, в которых уже после операции создания ”тонкого клона” был изменен набор дисков;
    - виртуальные машины с SCSI-контроллером типа lsilogic.
2. Текущие версии платформы ECP VeiL не поддерживают резервное копирование с хранилищ LVM ввиду ограничений самой платформы - моментальные снимки на хранилищах этого типа невозможны.
3. Версии ECP VeiL 4.x.x не поддерживают резервное копирование виртуальных машин, которые расположены на пулах хранения ZFS. Поддержка резервного копирования таких виртуальных машин реализована в ECP VeiL, начиная с версии 5.1.4.
4. Резервное копирование доступно лишь для виртуальных машин в пределах той локации, в которой развернуто виртуальное устройство. Если виртуальное устройство расположено на любом хосте в пределах одной локации, резервное копирование доступно для:
    - виртуальных машин, расположенных на всех хранилищах того же хоста;
    - всех виртуальных машин, которые находятся на сетевых хранилищах всех хостов в пределах этой локации.

Если вышеперечисленные ограничения являются для вас критичными, пожалуйста, обратитесь в службу поддержки НИИ ”Масштаб”.

Настройка LDAP-аутентификации для агента для ECP Veil

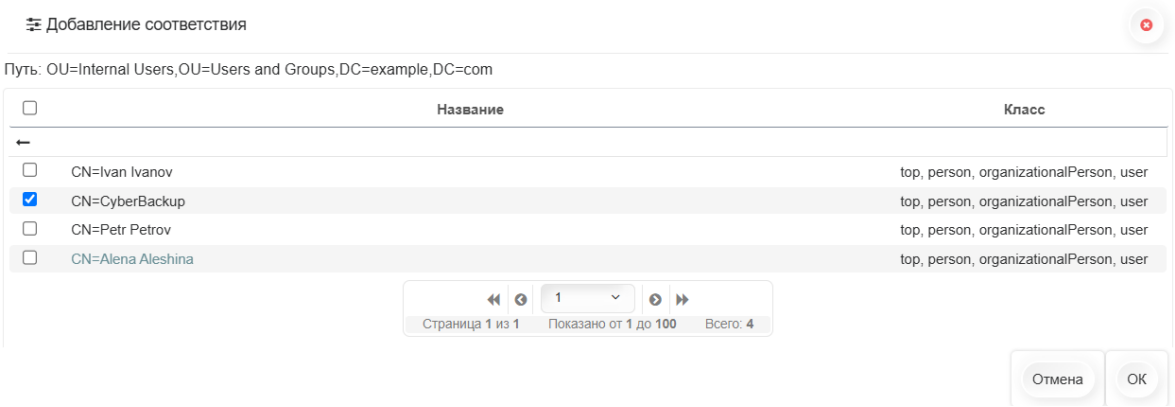
Если система виртуализации использует службу каталогов для аутентификации пользователей, то перед развертыванием агента выполните дополнительную настройку службы:

1. В веб-панели управления системой виртуализации перейдите в раздел **Безопасность** → **Службы каталогов**.

2. Щелкните по имени службы каталогов и перейдите в раздел **Соответствия**.
3. Нажмите **Добавить соответствие** и выполните следующие действия в окне **Добавление соответствия**:
    1. Укажите имя для соответствия.
    2. Выберите роли **Администратор** и **Администратор безопасности**.
    3. Введите описание соответствия.
    4. Нажмите **Добавить объекты LDAP** и добавьте LDAP-объект, представляющий пользователя, от имени которого агент будет выполнять операции резервного копирования и восстановления в системе виртуализации. При необходимости можно добавить LDAP-объект, представляющий группу, в которую входит требуемый пользователь.

        Чтобы просмотреть дочерние LDAP-объекты некоторого LDAP-объекта, щелкните по его имени в списке. Чтобы добавить LDAP-объект, поставьте галочку рядом с его именем и нажмите **OK**.

        Пример для Active Directory:

    5. Нажмите **OK**, чтобы завершить создание соответствия.
4. Убедитесь, что пользователь, для которого создано соответствие, может войти в веб-панель управления системой виртуализации и обладает в ней указанными ролями.

Установка агента для ECP VeiL

Чтобы установить агент для ECP VeiL, выполните следующие действия:

1. Загрузите пакет установки агента для ECP VeiL и извлеките из архива файл пакета (например, `file.ova`).
2. Войдите в систему ECP VeiL через браузер.
3. В консоли управления ECP VeiL в меню слева перейдите в раздел **Хранилища** → **Файлы**.

4. В верхнем меню выберите **Загрузить из файловой системы**.
5. В файловой системе выберите распакованный на первом шаге файл, далее выберите пул данных, по возможности доступный на всех хостах, и нажмите **OK**.
6. После завершения загрузки файла нажатием на имя файла раскройте его свойства.
7. В верхнем меню выберите **Обновить информацию**, подтвердите свое решение нажатием на кнопку **Да**.
8. В верхнем меню выберите **Конфигурация копии ВМ**.
9. В открывшемся окне выберите **Восстановление ВМ**, укажите узел, на который вы хотите восстановить виртуальную машину, нажмите кнопку **Отправить**.
10. После завершения создания виртуальной машины на указанном узле в меню слева перейдите в раздел **Виртуальные машины**.
11. В списке виртуальных машин выберите созданную виртуальную машину. Имя виртуальной машины по умолчанию: ”CyberBackup_Agent_for_ECP_VeiL”. Если вы планируете развернуть несколько виртуальных машин, рекомендуется переименовать каждую из них.
12. В открывшемся окне запустите эту виртуальную машину нажатием на стрелку в верхнем меню.
13. Подключитесь к консоли виртуальной машины: на мини-экране ВМ выберите **VNC** или **Spice**.
14. После завершения запуска виртуальной машины в консоли переходите по ссылкам **Change...** для настройки параметров:
    1. Укажите адрес контроллера ECP VeiL (например, `https://my-veil.my-company.ru`), имя пользователя (например, `admin`) и пароль доступа к ECP VeiL.

       Если система ECP Veil использует службу каталогов для аутентификации пользователей, установите флажок **Use LDAP-authentication**.

       Нажмите **Check connection**, чтобы проверить соединение. Ошибки при подключении могут указывать как на некорректность введенных данных, так и на проблемы с сетью.
    2. Укажите имя или IP-адрес сервера управления — компьютера, на котором установлено решение Кибер Бэкап, имя пользователя и пароль доступа к нему.
    3. Если необходимо, задайте параметры сетевого интерфейса Eth0 (IP-адрес, маску сети, шлюз и DNS). По умолчанию используется DHCP.
    4. Если вы планируете развернуть несколько агентов для ECP VeiL, измените имя агента для ECP VeiL. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
    5. Убедитесь, что в системе установлено корректное время. При необходимости установите

часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

15. При необходимости установите агент на других серверах, выполняя шаги установки из этой инструкции.

Выполненные действия должны привести к следующим результатам:

- В веб-консоли Кибер Бэкап в разделе **Настройки** → **Агенты** отобразится агент для ECP VeiL;
- В веб-консоли Кибер Бэкап в разделе **Устройства** появятся устройства ECP VeiL.

Установка агента для OpenStack

Общие сведения

Кибер Бэкап поддерживает резервное копирование и восстановление виртуальных машин OpenStack и РУСТЭК.

Резервная копия такой виртуальной машины содержит ее параметры и моментальный снимок ее дисков. Такую резервную копию можно восстановить на любой совместимый по версии хост. Восстановление будет выполнено в новую виртуальную машину, которая будет создана с необходимыми параметрами и к которой будут подключены моментальные снимки дисков.

Поддерживаемые конфигурации

Вам понадобятся установленные и настроенные системы:

- Решение Кибер Бэкап 16 или новее.
- Одна из следующих платформ виртуализации:
  - OpenStack;
  - VK Cloud;
  - РУСТЭК.

  Подробнее о поддерживаемых версиях платформ виртуализации см. раздел *Поддерживаемые платформы виртуализации*.

Планирование количества агентов

Если в системе имеется очень большое число виртуальных машин, то суммарное время создания резервных копий может быть слишком велико. В этом случае можно развернуть несколько виртуальных устройств с агентами на одном проекте OpenStack или РУСТЭК.

Производительность резервного копирования одного агента можно настроить с помощью параметра **Планирование** плана защиты (см. *Планирование*).

Установка

Для работы Кибер Бэкап с платформами виртуализации OpenStack и РУСТЭК необходимо установить агент для OpenStack. В процессе установки происходит добавление хоста OpenStack (или РУСТЭК) на сервер управления Кибер Бэкап и развертывание на хосте виртуального устройства (виртуальная машина с агентом Кибер Бэкап).

Порядок установки для OpenStack

1. Установка агента для OpenStack в *автоматическом режиме* или *вручную*.

Порядок установки для РУСТЭК

1. *Подготовка хостов РУСТЭК*.
2. Установка агента для OpenStack в *автоматическом режиме* или *вручную*.

Известные проблемы и ограничения

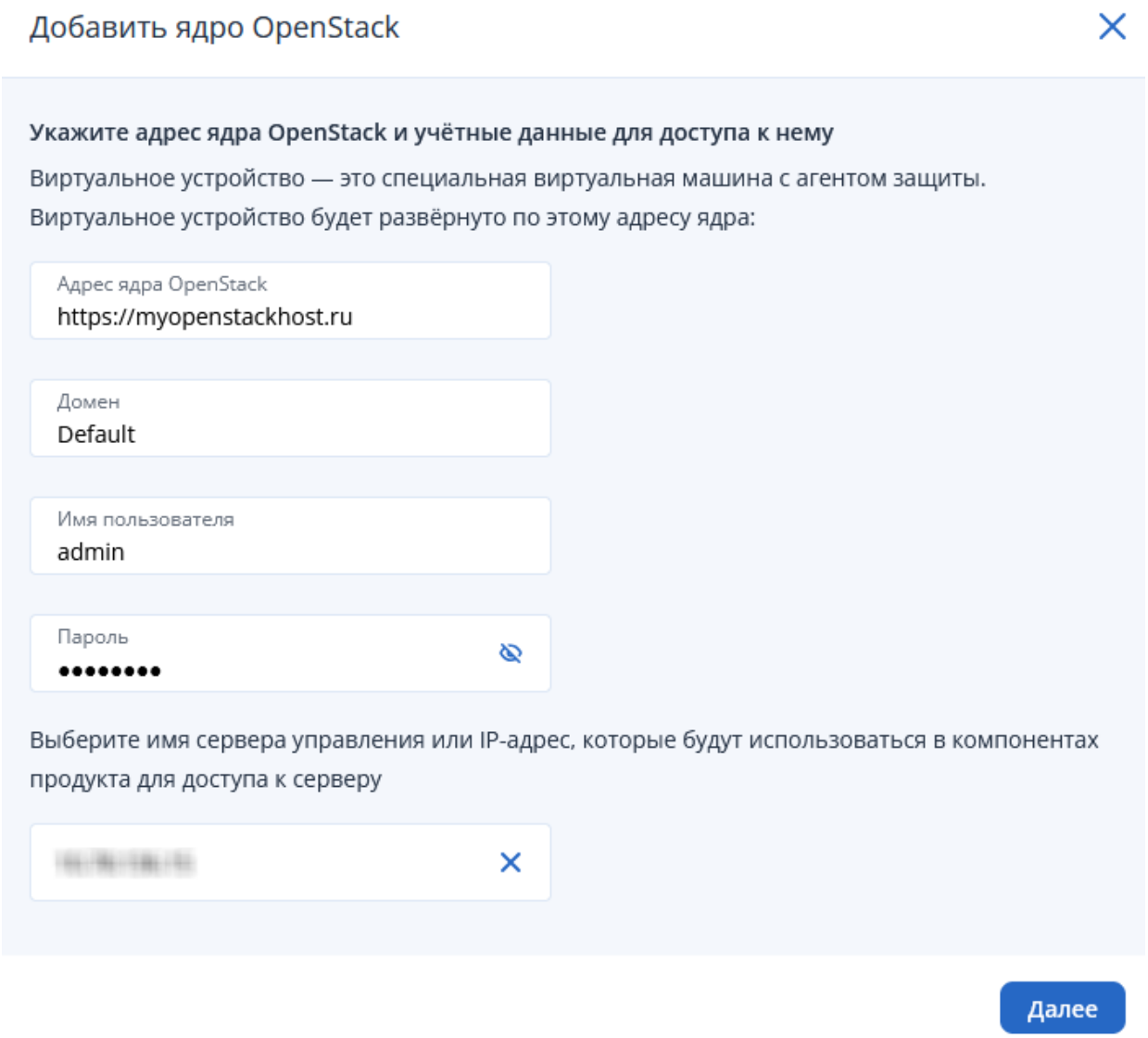
- Не поддерживается резервное копирование виртуальных машин с эфемерными дисками.
- Не поддерживается восстановление в текущую виртуальную машину.

Автоматическая установка агента для OpenStack

> **Примечание**
>
> При установке агента для OpenStack в РУСТЭК вначале необходимо выполнить *подготовку хоста РУСТЭК*.

Для автоматической установки агента выполните следующие шаги в веб-интерфейсе Кибер Бэкап:

1. На вкладке **Устройства** → **Физические и виртуальные машины** щёлкните **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **Платформы виртуализации** щёлкните **OpenStack**. Откроется окно **Добавить ядро OpenStack**.

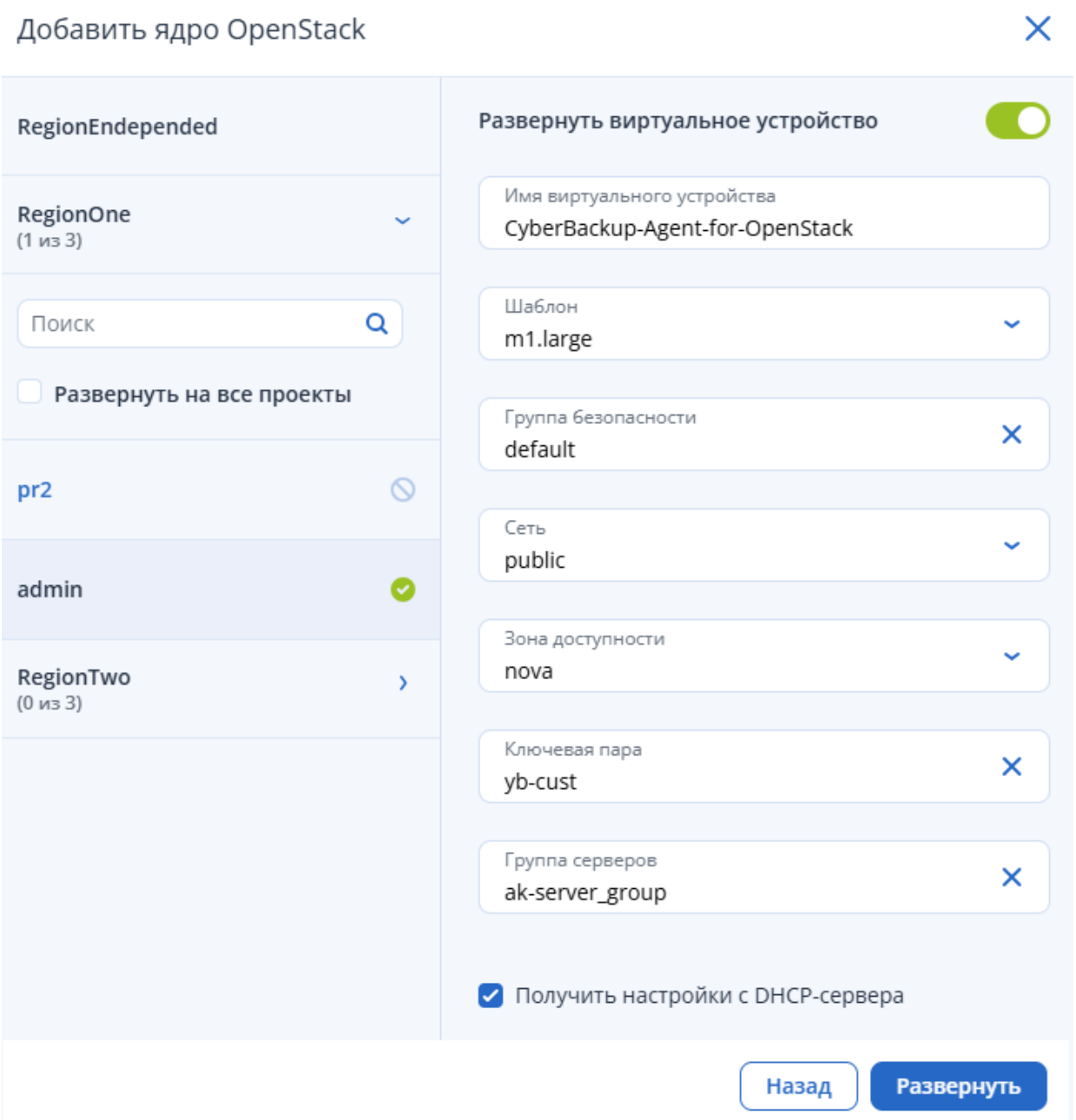


3. В поле **Адрес ядра OpenStack** укажите адрес хоста OpenStack (РУСТЭК) с префиксом протокола. Например, `https://myopenstackhost.ru/`. Поддерживаются протоколы HTTP и HTTPS. Вдобавок можно указать порт, например, `https://myopenstackhost.ru:12345` (по умолчанию используется порт 5000) или токен, например, `https://myopenstackhost.ru/identity`.
4. В поле **Домен** укажите домен с проектами, в которых находятся требуемые виртуальные машины.
5. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.
6. В выпадающем списке выберите сервер управления Кибер Бэкап, к которому будет подключен устанавливаемый агент. При этом, если сервер управления находится в одном домене Active Directory с хостом OpenStack (РУСТЭК), его можно выбрать по имени. В остальных случаях его необходимо выбрать по IP-адресу.
7. Укажите дополнительные параметры, щёлкнув **Далее** внизу справа. Появится список проектов в

указанном домене хоста. Ползунками отметьте необходимые. Для каждого из отмеченных проектов будет создано свое виртуальное устройство. Щёлкнув название проекта, можно выбрать параметры соответствующего виртуального устройства:

- **Имя**. Должно удовлетворять требованиям к именам виртуальных машин OpenStack (РУСТЭК).
- **Шаблон (Flavor)**. Необходимо минимум 4 ГБ ОЗУ, 2 ядра ЦП и 64 ГБ дискового пространства.
- **Группа безопасности**. Должна разрешать подключения к указанному серверу управления по протоколам TCP и ICMP.
- **Сеть**. Должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером OpenStack (РУСТЭК) через конечную точку (endpoint) `identity` (keystone). При необходимости можно снять флажок **Получить настройки с DHCP-сервера** и указать параметры сети вручную.
- **Зона доступности**. Выберите из списка зону доступности (Availability Zone), доступную для этого проекта OpenStack.
- **Ключевая пара**. Выберите из списка ключевую пару, доступную для этого проекта OpenStack.
- **Группа серверов**. Выберите из списка группу серверов, доступную для этого проекта OpenStack.

Например:



8. Указав необходимые параметры, нажмите **Развернуть**.

На указанном хосте будет создано виртуальное устройство, в которое будет установлен агент. При этом архив агента будет загружен с официального сайта Киберпротект. Если это невозможно, архив агента будет взят локально с машины, на которой установлен сервер управления: из директории `C:\ProgramData\Acronis\VaDeployer\va-images` на ОС Windows и из директории `/var/lib/Acronis/VaDeployer/va-images` на ОС Linux.

Запустившись автоматически, агент подключится к серверу управления, и виртуальные машины из выбранных проектов на хосте OpenStack (РУСТЭК) отобразятся в списке **Устройства** → **OpenStack**. После этого их можно будет добавлять к *планам защиты* обычным способом.

Примечание

В планах защиты таких виртуальных машин необходимо отключать функцию **Active Protection (Активная защита)**.

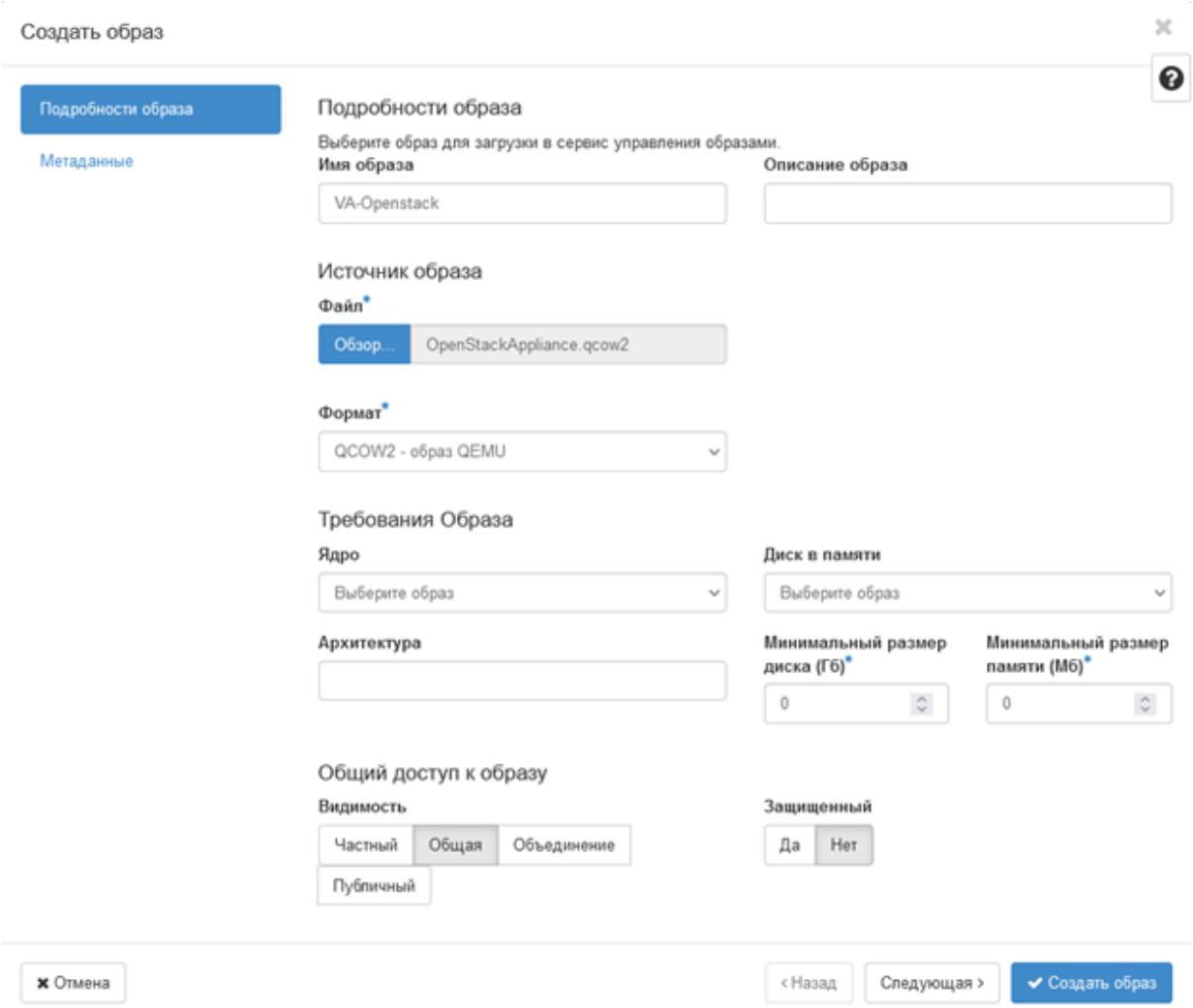
Установка агента для OpenStack вручную

Примечание

При установке агента для OpenStack в РУСТЭК вначале необходимо выполнить *подготовку хоста РУСТЭК*.

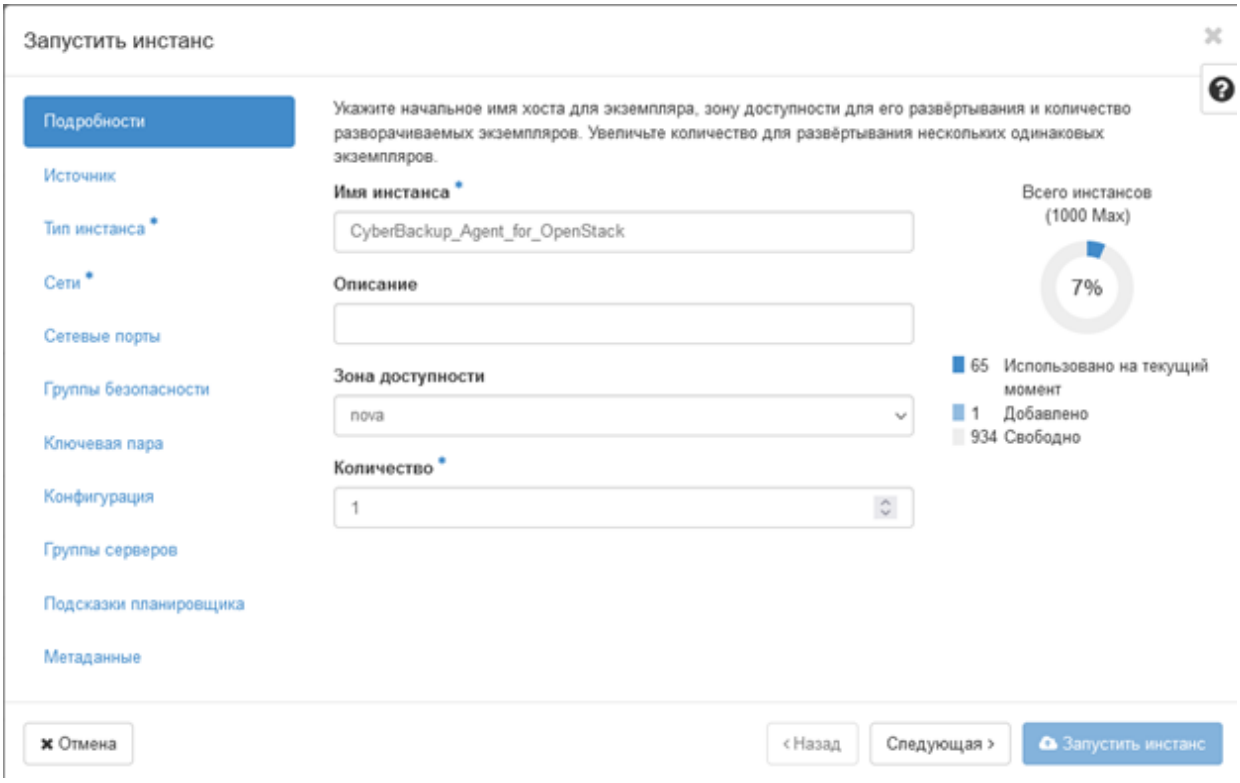
Чтобы установить агент для OpenStack вручную, выполните следующие шаги:

1. Загрузите **Пакет установки агента для OpenStack** с сайта Киберпротект.
2. Распакуйте образ виртуального устройства (например, `OpenStackAppliance.qcow2`).
3. В панели управления OpenStack перейдите на вкладку **Вычислительные ресурсы** → **Образы** и нажмите **Создать образ**.
4. В поле **Источник образа** укажите путь к распакованному образу виртуального устройства.



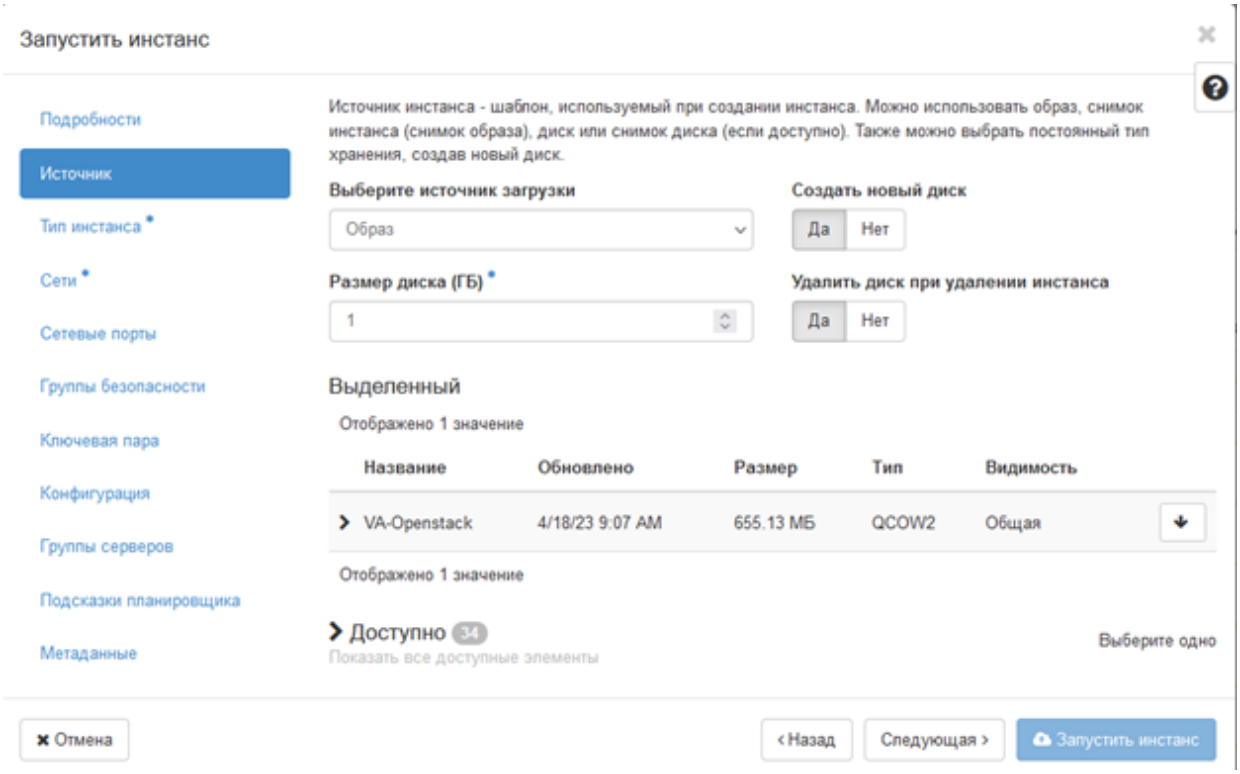
5. В поле **Формат** выберите **QCOW2 - образ QEMU**. По окончании ввода данных нажмите **Создать образ**.

6. Перейдите на вкладку **Вычислительные ресурсы** → **Инстансы** и выберите **Запустить инстанс**.

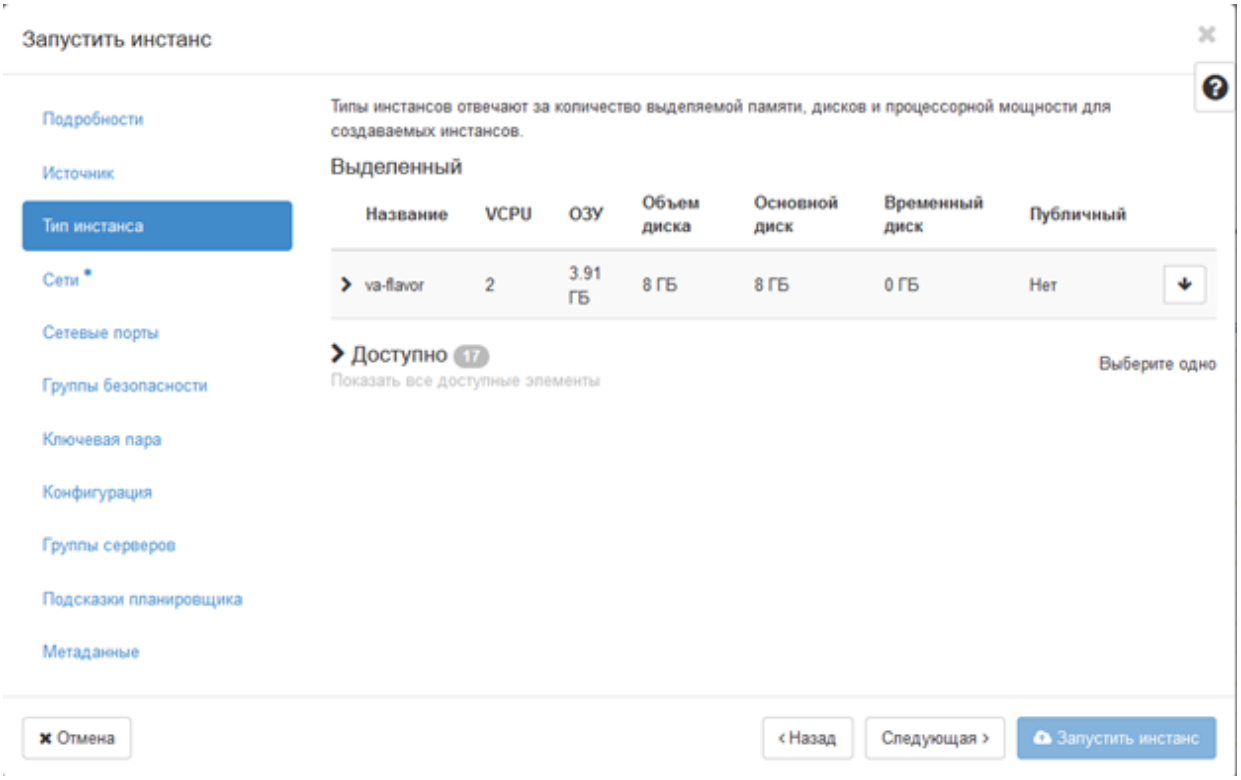


7. Укажите имя инстанса и зону доступности.

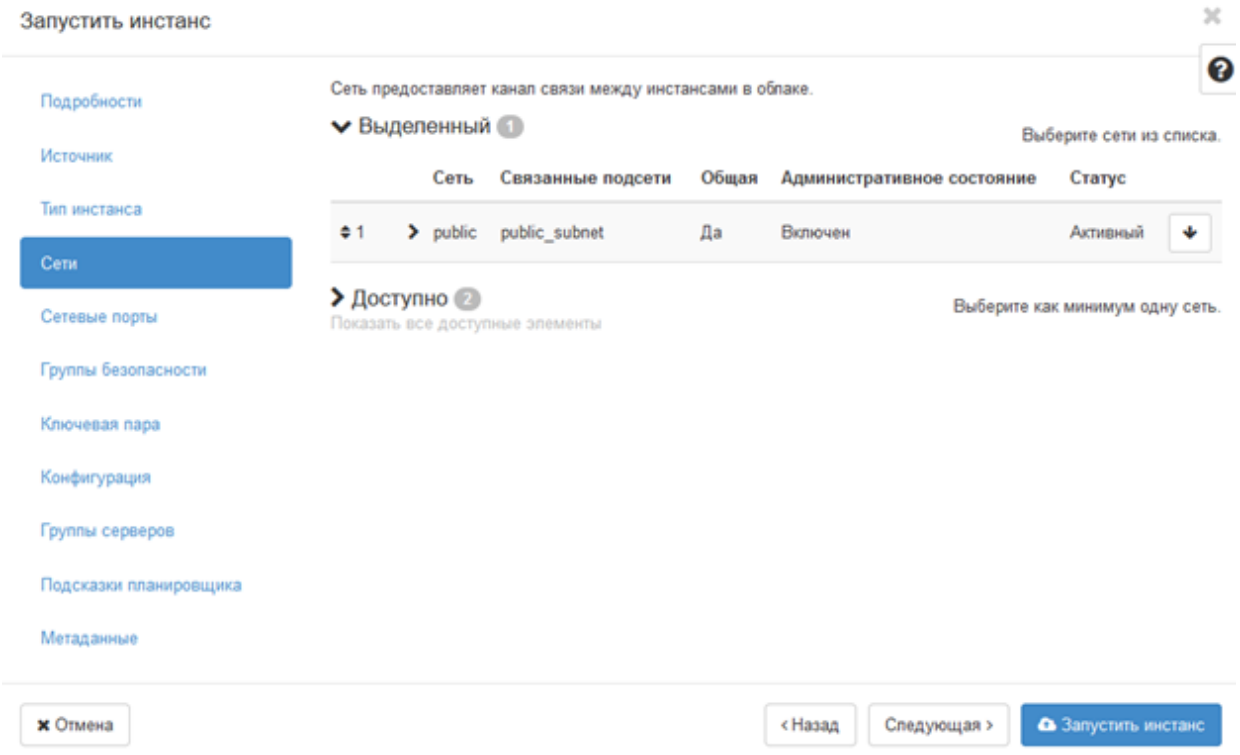
8. Выберите источник загрузки **Образ** и укажите образ виртуального устройства.



9. Укажите параметры виртуальной машины на вкладке **Тип инстанса**. Для промышленных сборок рекомендуется указывать не менее 2 ЦП и не менее 4 ГБ памяти.



10. На вкладке **Сети** укажите подходящие сеть и группу безопасности. Сеть должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером OpenStack через конечную точку (endpoint) `identity` (keystone). Группа должна разрешать подключения к серверу управления по протоколам TCP и ICMP.



11. По окончании ввода данных нажмите **Запустить инстанс**.
12. Перейдите на экран **Вычислительные ресурсы** → **Инстансы** и убедитесь, что имя машины с агентом появилось в списке виртуальных машин.
13. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:

    - **OpenStack**. Укажите адрес хоста-контроллера OpenStack с префиксом протокола. Например, `https://myopenstackhost.ru/`. Поддерживаются протоколы HTTP и HTTPS. Вдобавок можно указать порт, например, `https://myopenstackhost.ru:12345` (по умолчанию используется порт 5000) или токен, например, `https://myopenstackhost.ru/identity`.

      Кроме того, укажите домен с проектами, в которых находятся требуемые виртуальные машины. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.

    - **Management Server**. Укажите DNS-имя или IP-адрес сервера управления Кибер Бэкап, имя пользователя и пароль.
    - **Eth0**. Если необходимо, задайте параметры сетевого интерфейса, который будет использоваться агентом (IP-адрес, маску сети, шлюз, DNS-серверы и WINS-серверы). По умолчанию используется автоконфигурация посредством DHCP.
    - **Name**. Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.
    - **Time zone**. Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Выполненные действия должны привести к следующим результатам:

- В разделе **Настройки** → **Агенты** отобразится агент для OpenStack.
- В веб-консоли Кибер Бэкап в разделе **Устройства** появится подраздел **OpenStack**.

Подготовка хостов РУСТЭК к установке агента

Перед установкой агента на хост РУСТЭК необходимо добавить на этот хост политики для новой роли ”cyberbackup” и создать пользователя с этой ролью.

Выполните следующие шаги:

1. Загрузите архив cyberbackup-policy.tar.bz2 на один из узлов платформы РУСТЭК и распакуйте его:

```
# tar -xvf cyberbackup-policy.tar.bz2
```

2. Выполните сценарий Ansible из архива:

```
# ansible-playbook -i /var/lib/rustack-ansible/inventory.yml cyberbackup-policy/main.yml -vv
```

3. Примените новые политики, запустив конфигуратор РУСТЭК:

```
rustackctl
```

4. Выберите пункт меню **Изменить политики служб**.

5. После завершения процедуры вручную создайте пользователя ”cyberbackup” с новой ролью ”cyberbackup” в проекте ”cyberbackup”:

```
# openstack project create --os-cloud rustack_system --domain default cyberbackup
# openstack user create --os-cloud rustack_system --password <passwd> --enable --project¬
↪cyberbackup --domain default cyberbackup
# openstack role add --os-cloud rustack_system --user cyberbackup --project cyberbackup¬
↪cyberbackup
```

   где `<passwd>` — пароль для пользователя ”cyberbackup”.

6. При необходимости откройте этому пользователю полный доступ через портал:

```
# openstack role add --os-cloud rustack_system --user cyberbackup --user-domain default --
↪system all cyberbackup
# openstack role add --os-cloud rustack_system --user cyberbackup --user-domain default --
↪domain default cyberbackup
# openstack role add --os-cloud rustack_system --user cyberbackup --user-domain default --
↪domain default --inherited cyberbackup
```

Установка агента для OpenStack в РУСТЭК вручную

Чтобы установить агент для OpenStack в РУСТЭК вручную, выполните следующие шаги:

1. Загрузите **Пакет установки агента для OpenStack** с сайта Киберпротект.

2. Распакуйте образ виртуального устройства (например, `OpenStackAppliance.qcow2`).

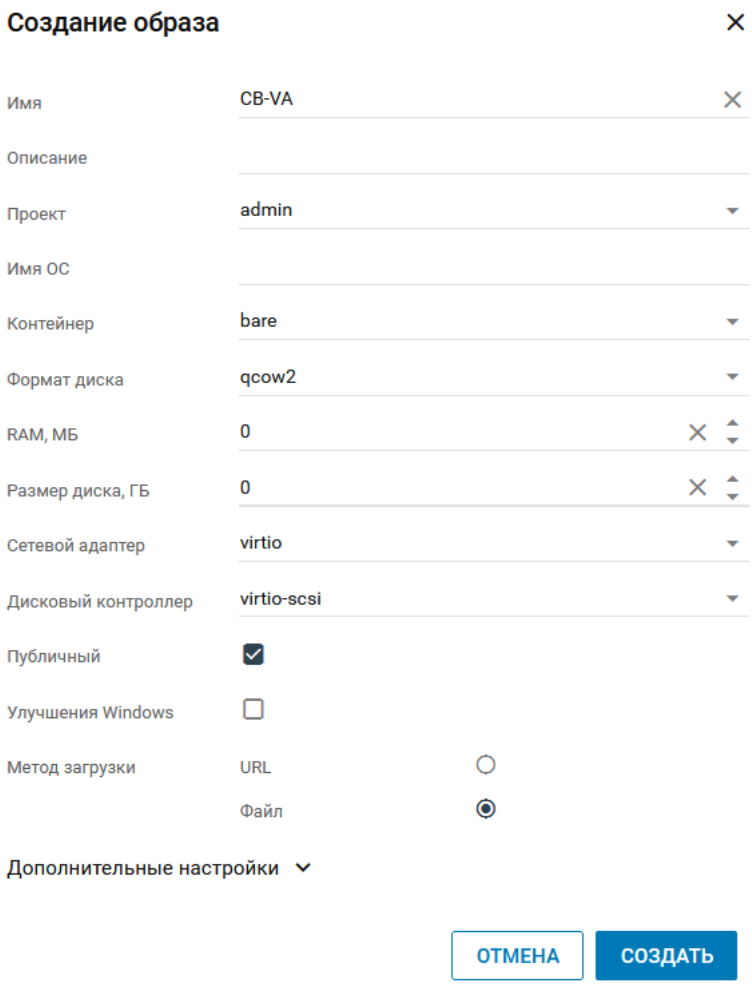
3. В панели управления РУСТЭК перейдите в раздел **Копии и образы** → **Образы** и нажмите **Создать**.

4. В окне **Создание образа** задайте параметры образа:

   - В поле **Имя** введите имя образа.
   - Убедитесь, что в поле **Формат диска** выбрано значение **qcow2**.

- В поле **Метод загрузки** выберите значение **Файл**.

По окончании ввода данных нажмите **Создать**.



5. В списке образов выберите созданный образ и нажмите **Загрузить образ**.
6. В окне **Загрузка образа** укажите путь к распакованному образу виртуального устройства и нажмите **Загрузить**.
7. Перейдите в раздел **Виртуальные машины** и нажмите **Создать**.
8. В окне **Создание виртуальной машины** задайте параметры виртуальной машины (ВМ):
    - В поле **Имя** введите имя ВМ.
    - В поле **ОС** укажите образ виртуального устройства.
    - В поле **Конфигурация** выберите конфигурацию ВМ. Для промышленных сред рекомендуется выбирать конфигурации, в которых указано не менее 4 ЦП и не менее 4 ГБ памяти.
    - В поле **Размер диска** укажите размер диска ВМ. Для промышленных сред рекомендуется указывать не менее 8 ГБ.

- В поле **Сети** выберите сеть, к которой будет подключена ВМ. Сеть должна обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером РУСТЭК через конечную точку (endpoint) `identity` (keystone).
- В поле **Профили безопасности** укажите профиль, разрешающий подключение ВМ к серверу управления по протоколам TCP и ICMP.

По окончании ввода данных нажмите **Создать**.



9. Перейдите в раздел **Виртуальные машины** и убедитесь, что имя ВМ с агентом появилось в списке виртуальных машин.

10. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:

    OpenStack

    Укажите адрес хоста-контроллера РУСТЭК с префиксом протокола. Например, `https://myrustackhost.ru/`. Поддерживаются протоколы HTTP и HTTPS. Вдобавок можно указать порт, например, `https://myrustackhost.ru:12345` (по умолчанию используется порт 5000) или токен, например, `https://myrustackhost.ru/identity`.

    Кроме того, укажите домен с проектами, в которых находятся требуемые виртуальные машины. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.

    Management Server

    Укажите DNS-имя или IP-адрес сервера управления Кибер Бэкап, имя пользователя и пароль.

    Eth0

    Если необходимо, задайте параметры сетевого интерфейса, который будет использоваться агентом (IP-адрес, маску сети, шлюз, DNS-серверы и WINS-серверы). По умолчанию используется автоконфигурация посредством DHCP.

    Name

    Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.

    Time zone

    Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

Выполненные действия должны привести к следующим результатам:

- В разделе **Настройки** → **Агенты** отобразится агент для OpenStack.
- В веб-консоли Кибер Бэкап в разделе **Устройства** появится подраздел **OpenStack**.

Ручная установка агента для VK Cloud

Для развертывания агента VK Cloud вам понадобятся установленные и настроенные системы:

- Платформа виртуализации VK Cloud (список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*);
- Решение Кибер Бэкап 17 или новее.

Перед установкой агента для VK Cloud требуется предварительная настройка пользователя VK Cloud в зависимости от типа облачной платформы.

Предварительная настройка VK Cloud

Настройка для публичной облачной платформы

В панели администратора VK Cloud убедитесь, что включен доступ к API у пользователя, который будет взаимодействовать с виртуальным устройством.

См. также документацию разработчика.

Настройка для частной облачной платформы

Выполните следующие действия:

1. Выполните авторизацию в OpenStack с помощью команды:

   ```
   source openrc.sh
   ```

2. Создайте нового пользователя, выполнив команду:

   ```
   openstack user create --password user_password user_name
   ```

   где `user_password` — пароль пользователя, `user_name` — имя пользователя.

   Запомните или запишите ID пользователя.

3. Отобразите список проектов с помощью команды:

   ```
   openstack project list
   ```

4. Найдите в списке нужный проект и получите информацию об этом проекте, выполнив команду:

   ```
   openstack project show project_name
   ```

   где `project_name` — название проекта.

5. Добавьте созданного пользователя в проект с правами `mcs_co_owner` с помощью команды:

   ```
   openstack role add --project project_ID --project-domain project_domain_ID --user user_ID¬
   ↪mcs_co_owner
   ```

   где `project_ID` — ID проекта, `user_ID` — ID пользователя.

   В зависимости от вашей конфигурации, в качестве `project_domain_ID` выберите ID домена проекта или укажите ID домена по умолчанию: `default`.

   См. также документацию разработчика.

Установка агента для VK Cloud

Для установки обратитесь к разделу *Установка агента для VK Cloud*.

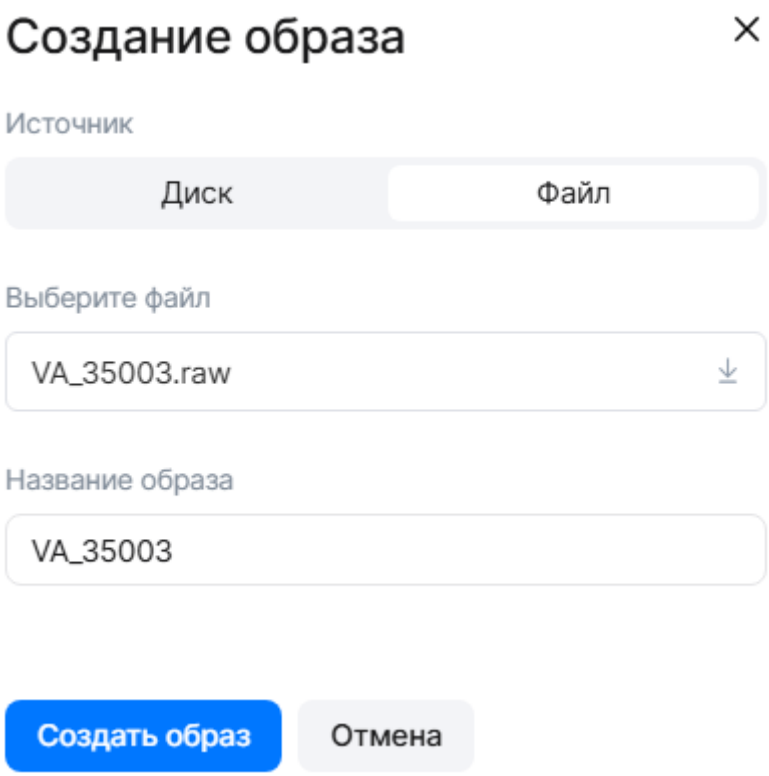
Установка агента для VK Cloud

Чтобы установить агент для VK Cloud вручную, выполните следующие шаги:

1. Загрузите пакет установки агента для OpenStack и распакуйте его.
2. Подготовьте образ виртуального устройства в формате RAW с помощью утилиты `qemu-img`:

   ```
   qemu-img convert -f qcow2 -O raw OpenStackAppliance.qcow2 OpenStackAppliance.raw
   ```

3. Войдите в личный кабинет VK Cloud.
4. Импортируйте подготовленный образ в VK Cloud:
   1. Перейдите в раздел **Облачные вычисления** → **Образы** и нажмите **Создать**.
   2. В окне **Создание образа** укажите параметры импортируемого образа:
      1. В поле **Источник** выберите **Файл**.
      2. В поле **Выберите файл** укажите путь к файлу образа в формате RAW.
      3. В поле **Название образа** введите имя образа.



3. Нажмите **Создать образ**.

5. Создайте ВМ на основе импортированного ранее образа:

    1. Перейдите в раздел **Облачные вычисления → Образы**, щёлкните значок многоточия рядом с образом и выберите **Создать ВМ из образа** в появившемся меню. Откроется мастер создания ВМ.

    2. На шаге **Конфигурация** укажите конфигурационные параметры ВМ:

        1. В поле **Имя виртуальной машины** введите имя ВМ.

        2. В поле **Тип виртуальной машины** выберите тип ВМ. Для промышленной среды рекомендуется использовать тип ВМ, в котором указано не менее 2 ЦП и не менее 4 ГБ памяти.

        3. В поле **Зона доступности** выберите необходимую зону.

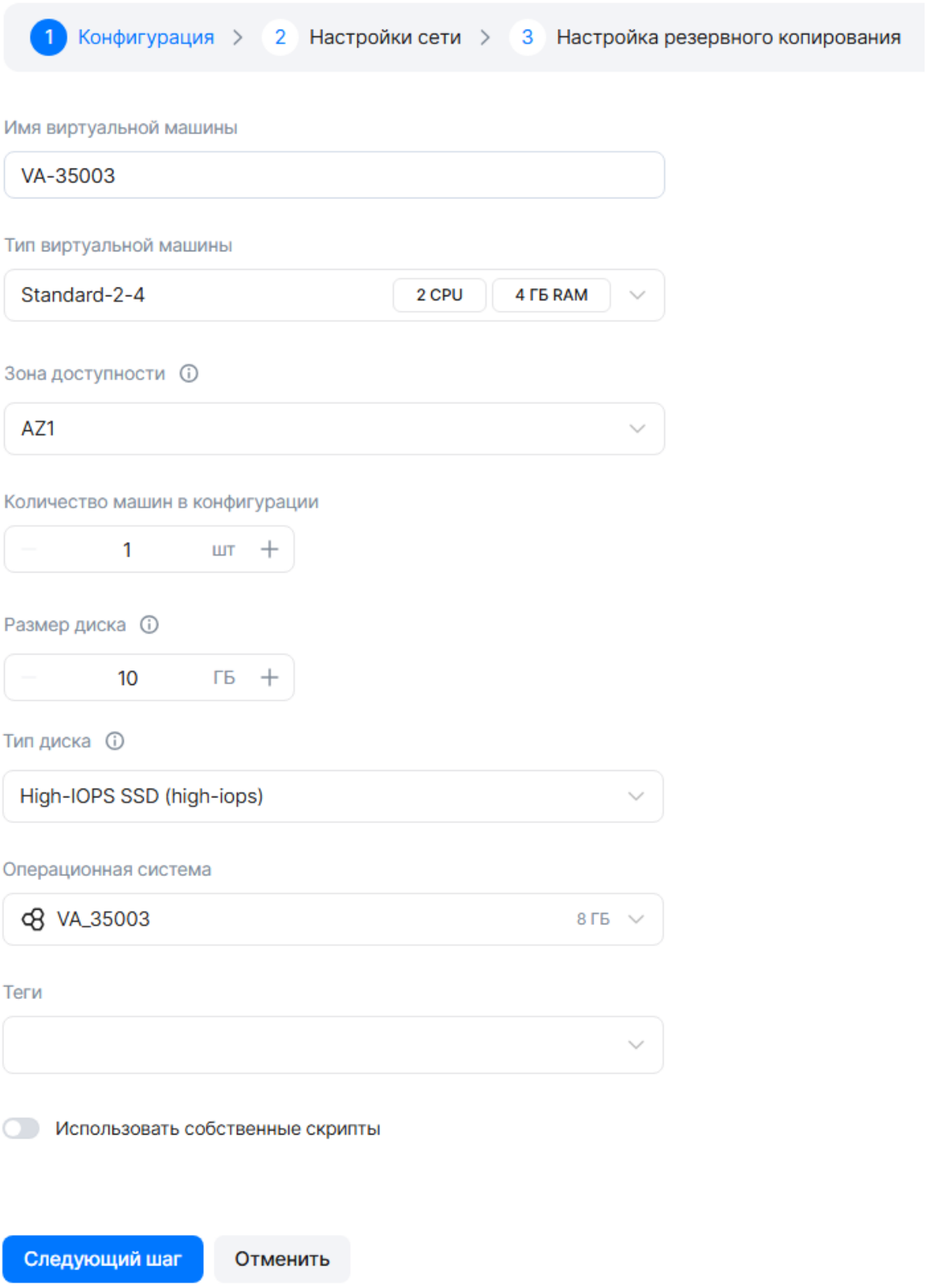
        4. В поле **Количество машин в конфигурации** укажите значение 1.

        5. В поле **Размер диска** задайте размер диска ВМ.

        6. В поле **Тип диска** выберите тип диска ВМ.

        7. Убедитесь, что в поле **Операционная система** выбран образ ВМ, который был импортирован ранее.

        По окончании ввода нажмите **Следующий шаг**.



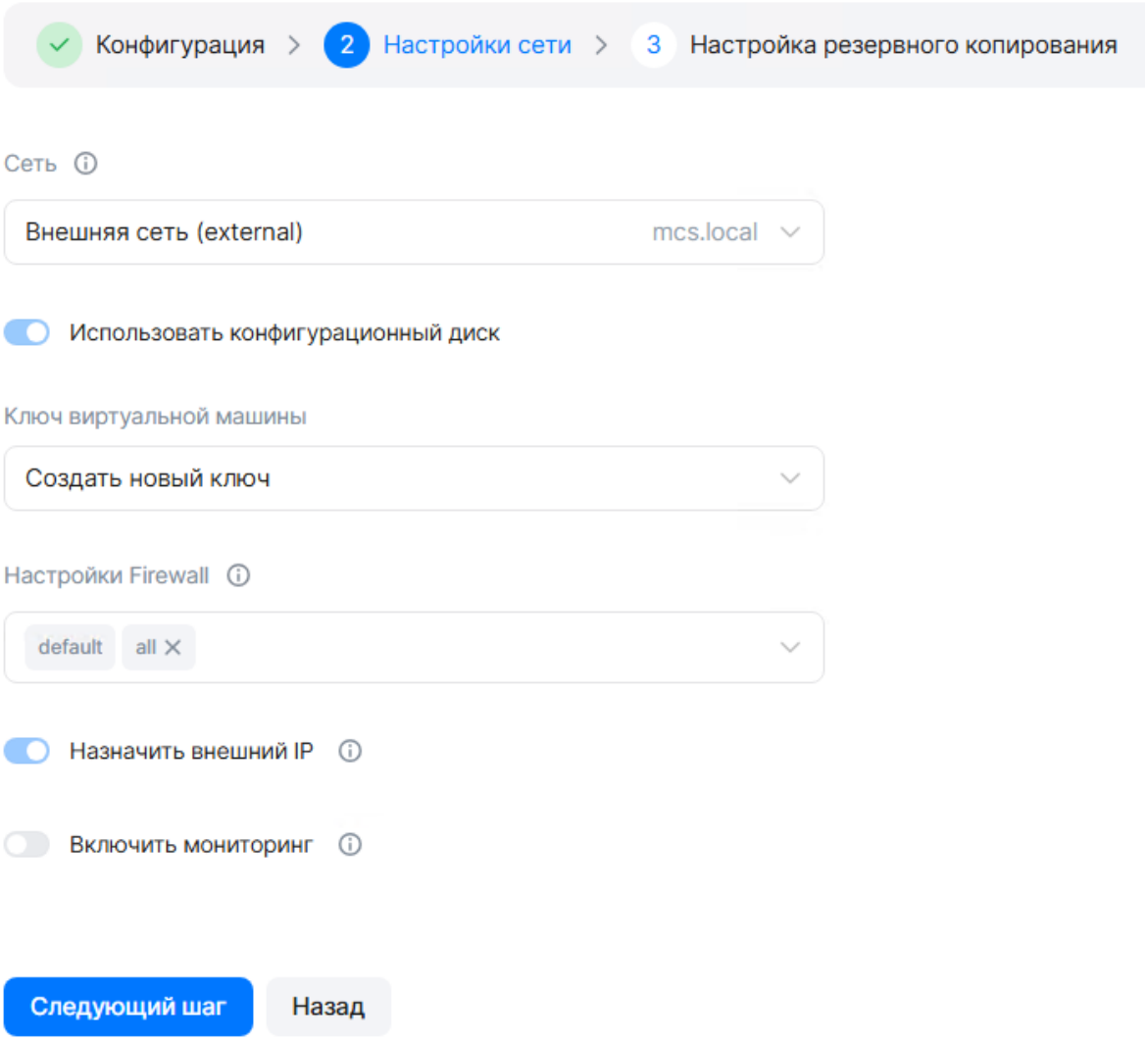
3. На шаге **Настройки сети** задайте сетевую конфигурацию ВМ:

    1. В поле **Сеть** выберите сеть, к которой будет подключена ВМ. Эта сеть должна

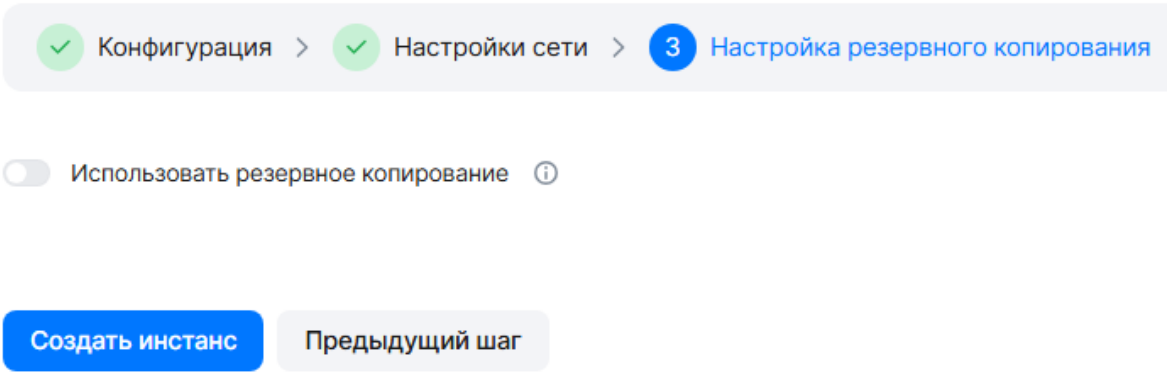
обеспечивать связь виртуального устройства с сервером управления Кибер Бэкап и с контроллером VK Cloud.

2. В поле **Ключ виртуальной машины** укажите SSH-ключ для доступа к ВМ.
3. В поле **Настройки Firewall** выберите группы безопасности.
4. При необходимости передвиньте переключатель **Назначить внешний IP** в положение ”вкл”.

По окончании ввода нажмите **Следующий шаг**.



4. На шаге **Настройка резервного копирования** нажмите **Создать инстанс**.



5. Перейдите в раздел **Облачные вычисления** → **Виртуальные машины** и убедитесь, что имя машины с агентом появилось в списке виртуальных машин.

6. Получите URL-адрес API для аутентификации, который будет использоваться виртуальным устройством для взаимодействия с VK Cloud:

   1. Щёлкните имя пользователя вверху справа и выберите **Настройки проекта**.
   2. Перейдите на вкладку **Доступ по API**.
   3. Запомните или запишите значение поля **Auth URL**.

7. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:

   OpenStack

   Укажите URL-адрес API для аутентификации. Кроме того, укажите домен с проектами, в которых находятся требуемые виртуальные машины. В соответствующих полях укажите имя пользователя и пароль администратора проектов с требуемыми виртуальными машинами.

   Management Server

   Укажите DNS-имя или IP-адрес сервера управления Кибер Бэкап, имя пользователя и пароль.

   eth0

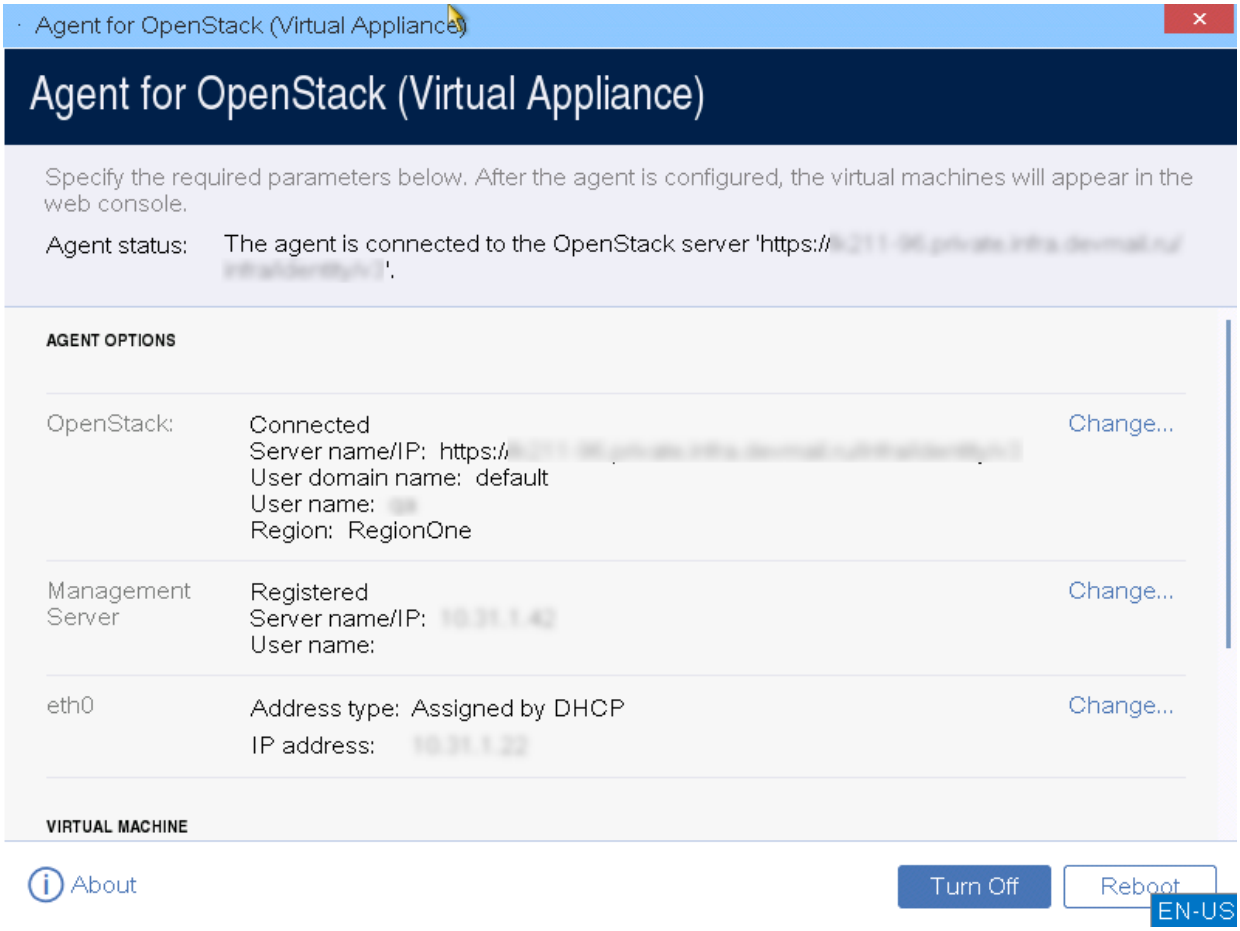
   Если необходимо, задайте параметры сетевого интерфейса, который будет использоваться агентом (IP-адрес, маску сети, шлюз, DNS-серверы и WINS-серверы). По умолчанию используется автоконфигурация посредством DHCP.

   Name

   Если необходимо, измените имя агента. Это имя отображается в списке агентов в веб-консоли Кибер Бэкап.

   Time zone

   Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.



Выполненные действия должны привести к следующим результатам:

- В разделе **Настройки** → **Агенты** отобразится агент для OpenStack (VK Cloud).
- В веб-консоли Кибер Бэкап в разделе **Устройства** появится подраздел **OpenStack (VK Cloud)**.

Установка агента для Basis DynamiX Enterprise

Общие сведения

1. Для резервного копирования данных Basis DynamiX Enterprise понадобятся установленные и настроенные продукты:
   - Кибер Бэкап версии 17 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. *Издания и лицензии Кибер Бэкап*);
   - Basis DynamiX Enterprise (список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*).
2. Для корректной работы Кибер Бэкап и Basis DynamiX Enterprise виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество центральных процессоров (CPU): 2;

- Объем ОЗУ: 4 ГБ;
- Объем диска: 8 ГБ.

Известные проблемы и ограничения

- Резервное копирование включённых ВМ поддерживается с версии 4.1.
- Не поддерживается подключение более 9 дисков к ВМ Basis DynamiX Enterprise 3.8.8 – 4.0.0 из-за ограничений платформы.
- Не поддерживается подключение более 8 сетевых адаптеров к ВМ Basis DynamiX Enterprise 3.8.8 – 4.0.0 из-за ограничений платформы.
- При развертывании агента не отслеживается прогресс передачи диска.
- После создания мгновенного снимка невозможно отключить вновь присоединенные или созданные диски от ВМ.
- Резервное копирование дисков с данными объемом более 100 ГБ может завершаться с ошибкой.
- Не поддерживается резервное копирование виртуальной машины, если к ней подключены диски из разных пулов.
- Не поддерживается резервное копирование виртуальной машины, если диски ВМ подключены к разным SEP.
- Автоматическая установка агента может завершаться с ошибкой, связанной с загрузкой диска виртуального устройства на сервер виртуализации. Ошибка возникает из-за того, что Basis DynamiX Enterprise версии 4.4 или более ранней не поддерживает разреженные образы виртуальных машин (sparse VM images). Например, разреженный образ, физический и логический размеры которого составляют 800 МБ и 64 ГБ соответственно, будет загружаться как обычный образ размером 64 ГБ, что может занять большее время, чем допускается настройками платформы виртуализации. Ожидается, что поддержка разреженных образов будет добавлена в Basis DynamiX Enterprise версии 4.7.

  При возникновении ошибки выполните одно из двух следующих действий:

  - Установите агент для Basis DynamiX Enterprise вручную, использовав пакет установки агента для текущей версии Кибер Бэкап.
  - Установите агент для Basis DynamiX Enterprise вручную, использовав пакет установки агента для Кибер Бэкап версии 18.0, а затем обновите его до текущей версии.

Автоматическая установка агента для Basis DynamiX Enterprise

Установка Basis DynamiX Enterprise включает в себя следующие шаги:

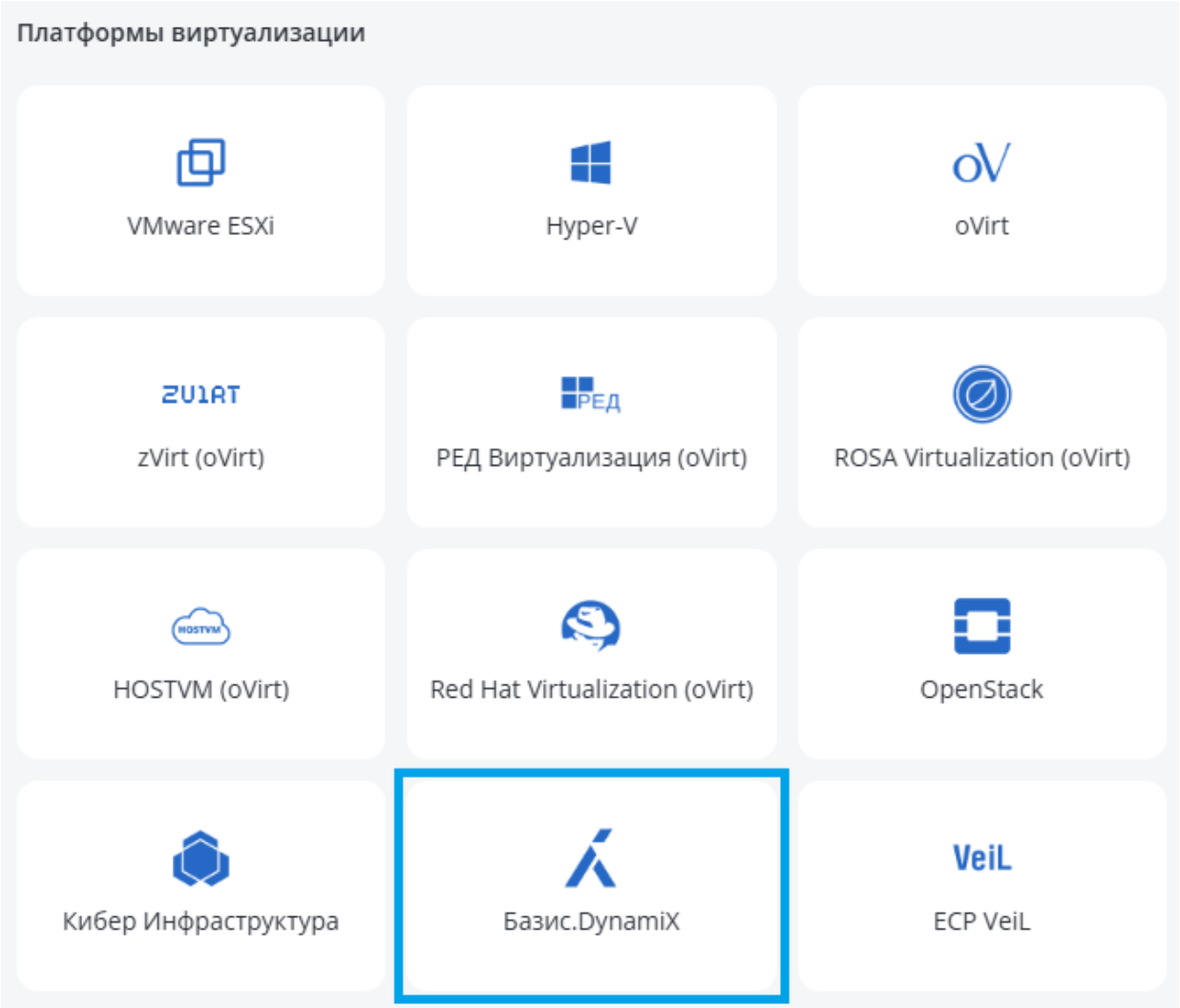
1. Установка сервера управления Кибер Бэкап.
2. Подключение виртуального устройства Basis DynamiX Enterprise к серверу управления Кибер Бэкап.

Установка сервера управления Кибер Бэкап

Для установки сервера управления Кибер Бэкап обратитесь к разделу *Установка сервера управления*.

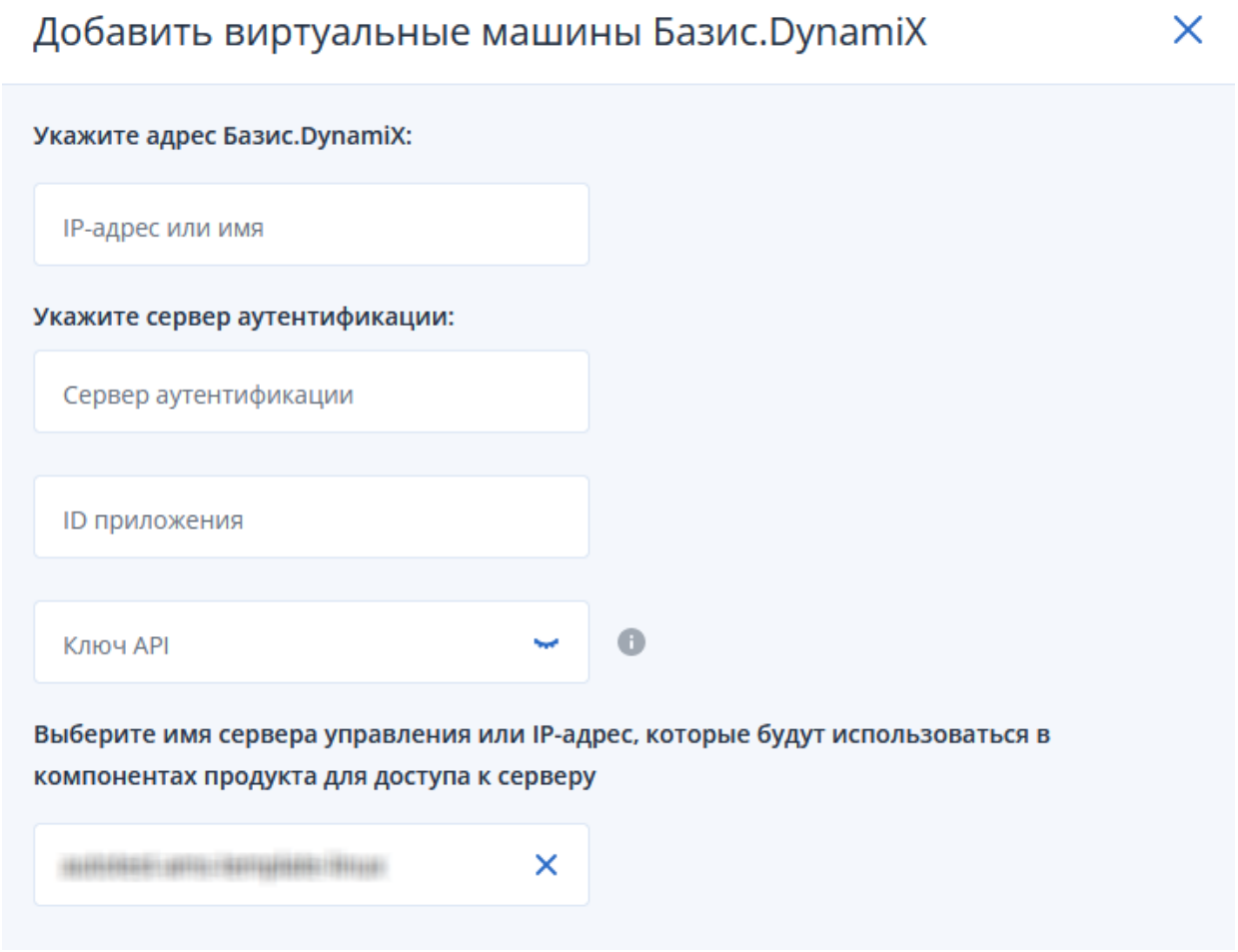
Подключение виртуального устройства Basis DynamiX Enterprise к серверу управления Кибер Бэкап

1. На вкладке **Устройства** → **Физические и виртуальные машины** щёлкните **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **Платформы виртуализации** выберите **Базис.DynamiX**.



Откроется окно **Добавить виртуальные машины Базис.DynamiX**.

3. Укажите IP-адрес или имя для Basis DynamiX Enterprise, данные сервера аутентификации и укажите данные для доступа к серверу управления.

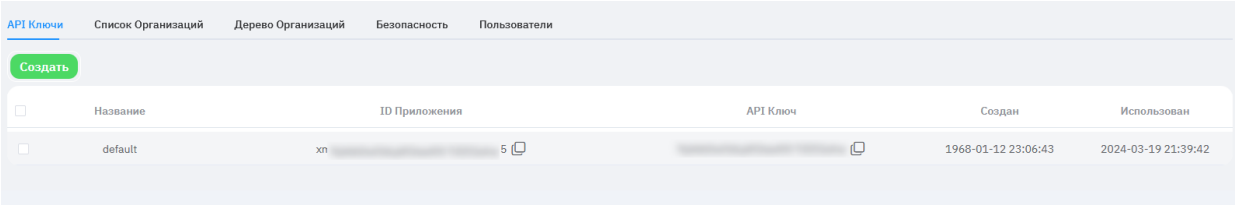


Для получения ID приложения и ключа API выполните следующие действия:

1. Перейдите на портал управления авторизацией SSO, например: `sso.your_domain_name.domain`.
2. Авторизуйтесь под именем пользователя, от имени которого будут выполняться запросы к REST API платформы (посредством токена JWT).

> **Примечание**
>
> Пользователь должен иметь права **Admin** в учетной записи Basis DynamiX Enterprise.

3. Перейдите на вкладку **API Ключи** и нажмите **Создать**.
4. Введите название ключа и нажмите `Ввод`.
5. Введите ID приложения и API ключ с экрана в соответствующие строки.



После заполнения полей нажмите **Далее** и дождитесь окончания подключения.

4. Перейдите в **Устройства** → **Basis DynamiX Enterprise** и убедитесь, что подключенное устройство отображается корректно.
5. Перейдите в **Настройки** → **Агенты** и убедитесь, что в списке агентов появился агент для резервного копирования.

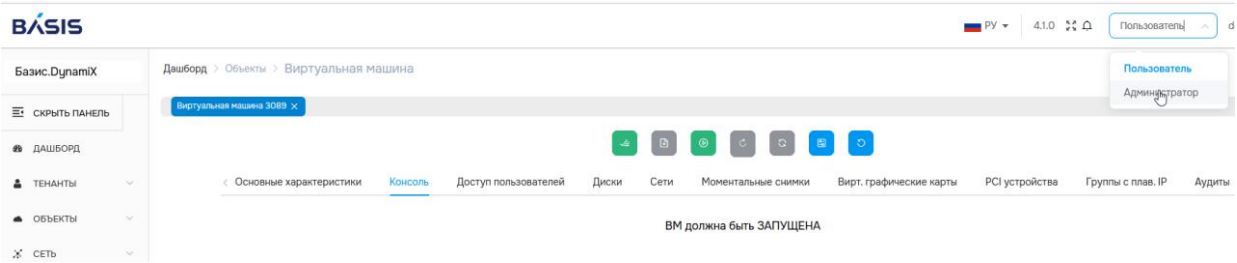
   Если операция подключения завершилась с ошибкой, проверьте сетевые настройки, соединение с сервером управления и настройки подключения к платформе Basis DynamiX Enterprise.

> **Примечание**
>
> Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

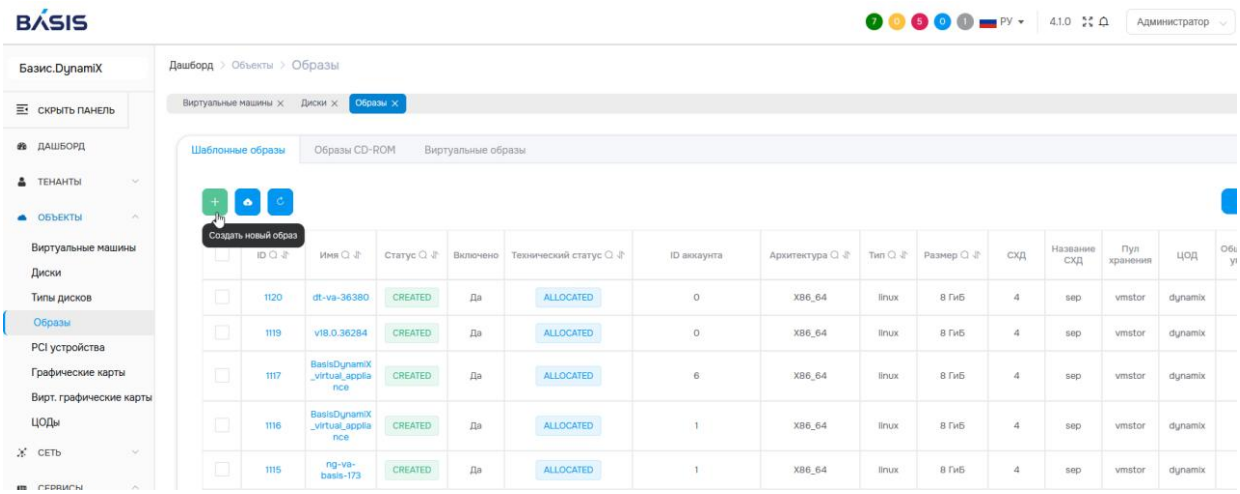
Установка агента для Basis DynamiX Enterprise вручную

Для установки вручную агента для Basis DynamiX выполните следующие действия:

1. Скачайте пакет установки агента Basis DynamiX с сайта компании (файл формата .qcow2; например, `BasisDynamixAppliance.qcow2`).
2. В панели управления системой виртуализации Basis DynamiX перейдите в режим администратора.

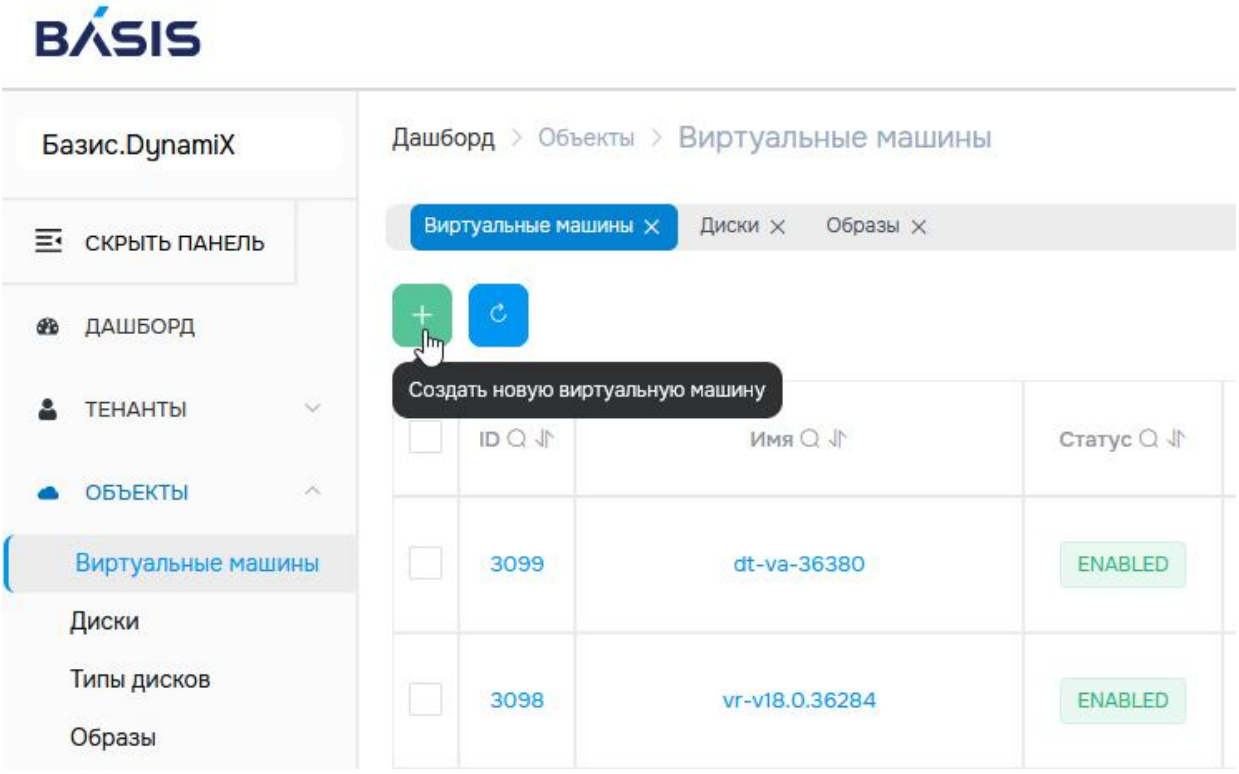


3. Перейдите в раздел **Объекты** → **Образы** и нажмите **Создать новый образ**.

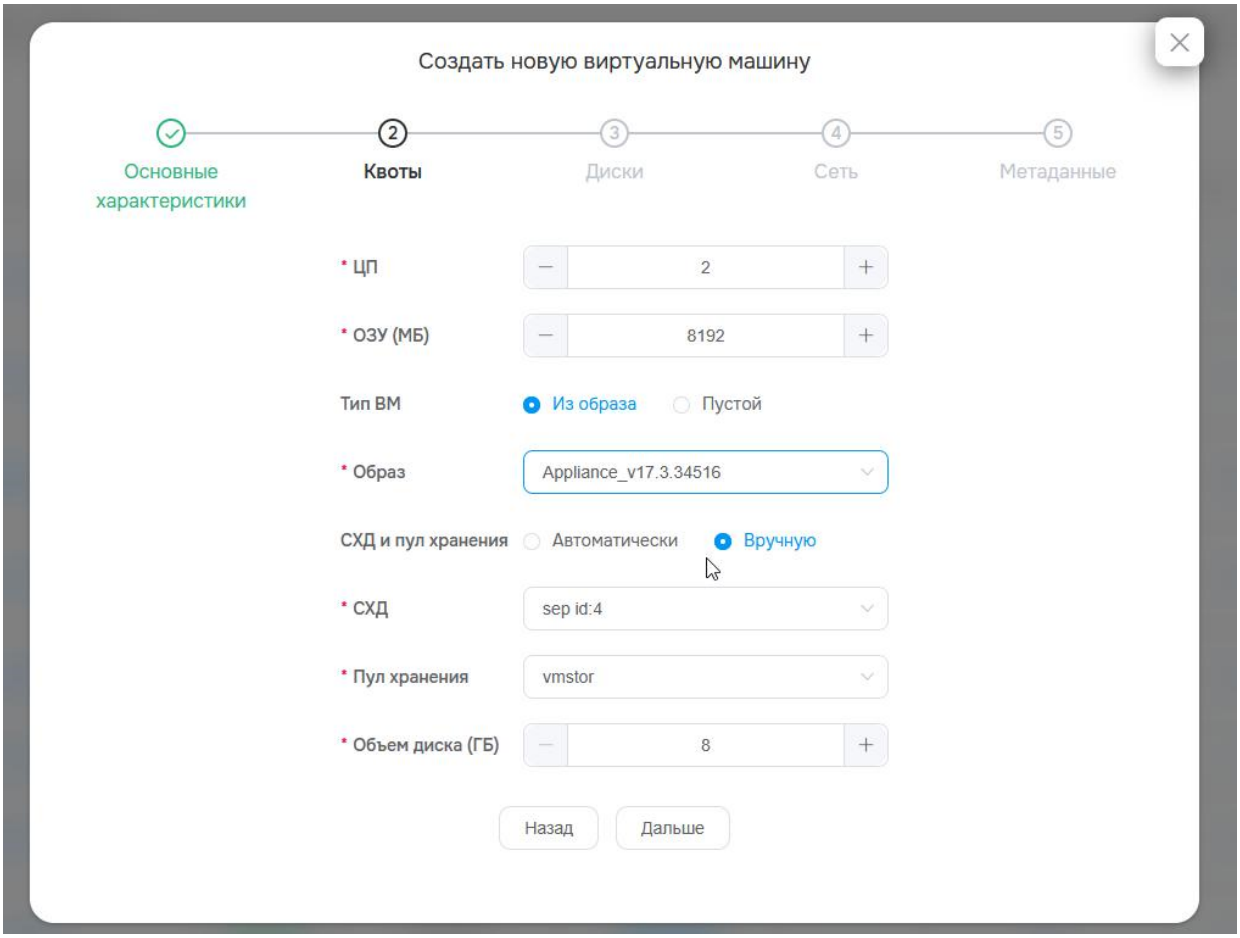


4. В окне создания образа укажите путь к пакету установки агента Basis DynamiX (подробнее см. в документации Basis DynamiX).

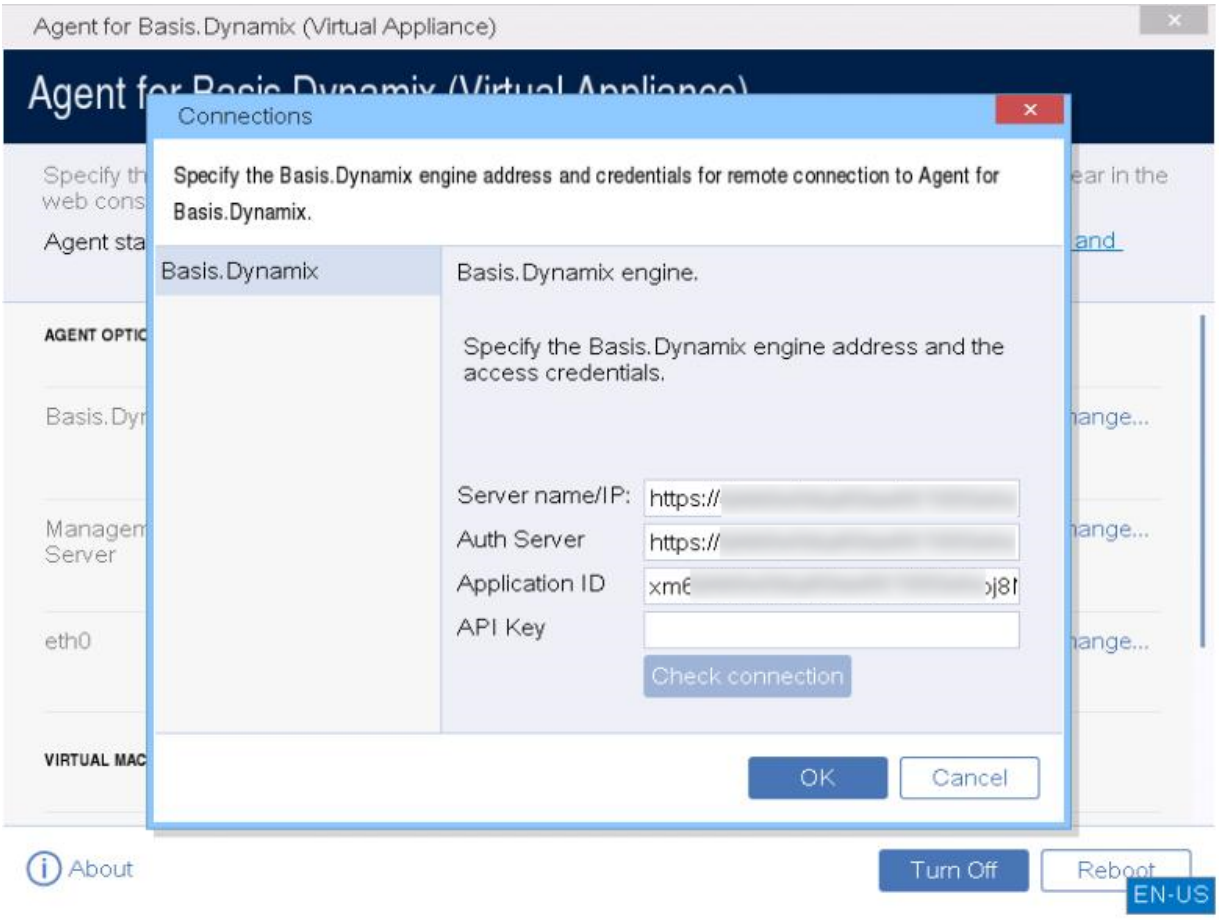
5. Перейдите в раздел **Виртуальные машины** и нажмите **Создать новую виртуальную машину**.



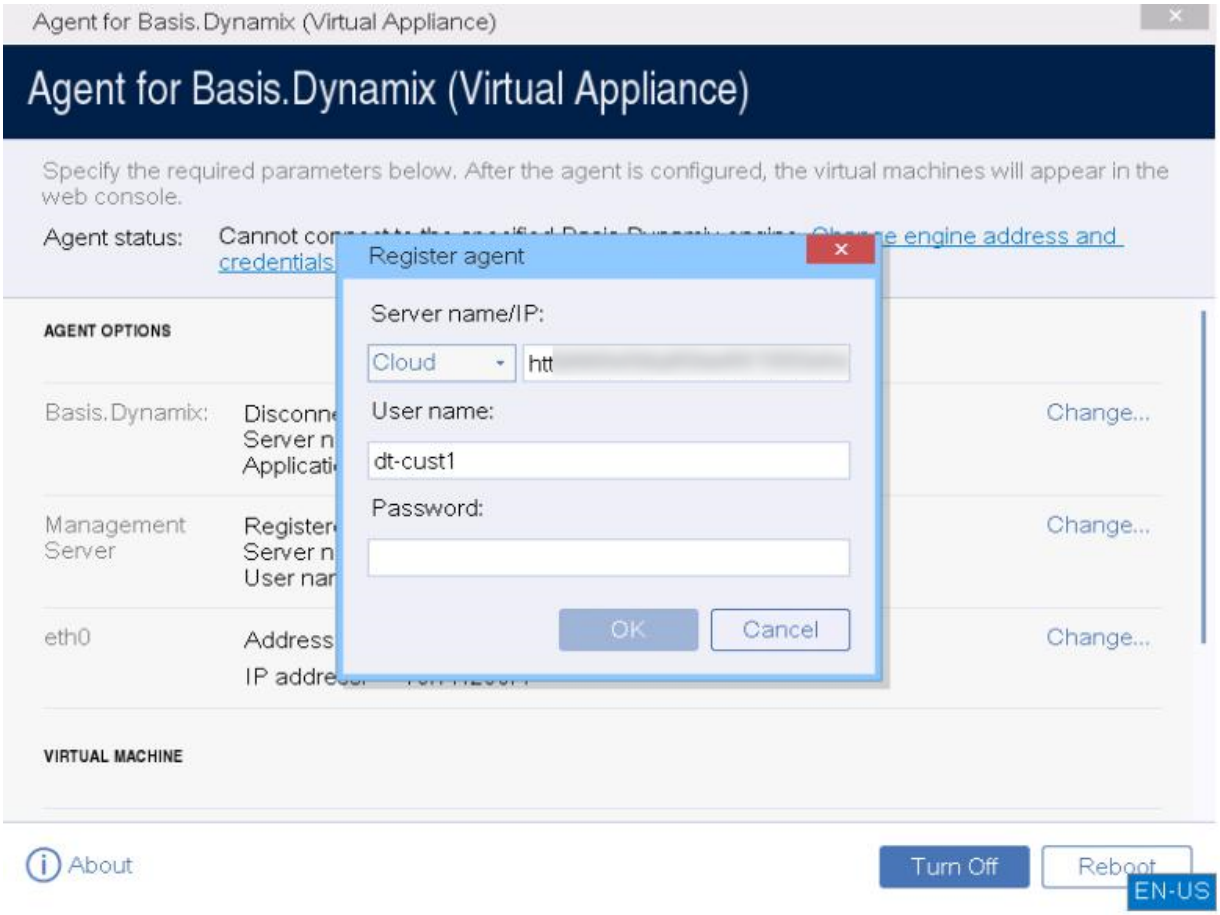
6. В окне создания виртуальной машины на шаге **Квоты** укажите созданный ранее образ ВМ.



7. Укажите остальные настройки для создания шаблона на основе образа виртуального устройства согласно документации Basis DynamiX.
8. Подключитесь к консоли виртуальной машины.
9. В разделе **Basis.Dynamix** нажмите **Change** и укажите IP-адрес сервера платформы виртуализации, ID приложения и ключ API (информацию о получении ID приложения и ключа API см. в разделе *Автоматическая установка Basis DynamiX Enterprise*).



10. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учетные данные для подключения к нему.



11. Перезапустите виртуальную машину.
12. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап отображаются устройства Basis DynamiX.

Установка агента для OpenNebula

Предварительные требования

1. Для развёртывания агента OpenNebula вам понадобятся установленные и настроенные системы:
   - Решение Кибер Бэкап версии 17.2 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. *Издания и лицензии Кибер Бэкап*);
   - Система управления виртуализацией (например, ПК СВ ”Брест”).
2. Поддерживаются следующие системы управления виртуализацией:
   - OpenNebula;
   - ПК СВ ”Брест”;
   - Альт Виртуализация;

- Система группового управления ”Горизонт-ВС”.

Список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*.

3. Для корректной работы Кибер Бэкап и OpenNebula виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество процессоров (vCPU): 2;
   - Объём ОЗУ: 4 ГБ;
   - Объём диска: 64 ГБ.

Процедура установки

Вы можете установить агент двумя способами:

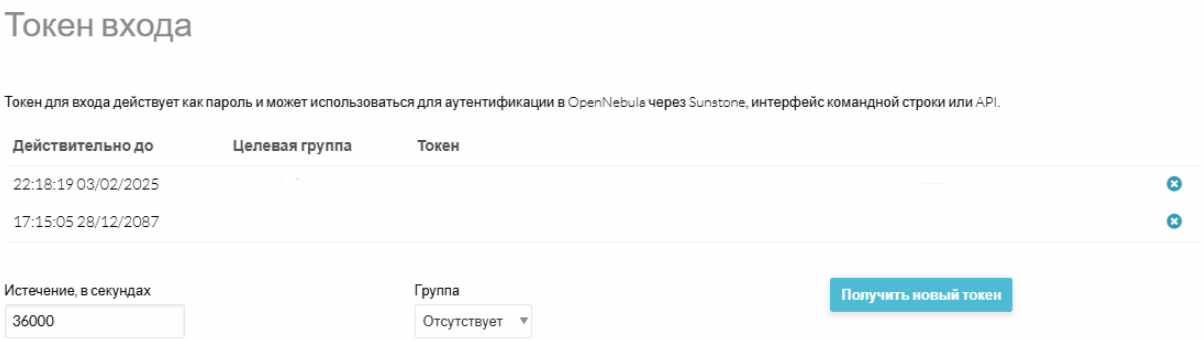
- Автоматически из интерфейса Кибер Бэкап (см. *Автоматическая установка агента для OpenNebula*).
- Вручную, используя установочный файл агента OpenNebula (см. *Установка агента для OpenNebula вручную*).

После установки агента *создайте план защиты ваших виртуальных устройств*.

Настройка токена входа

По умолчанию срок жизни нового токена входа для пользователя составляет 36 000 секунд (10 часов). Чтобы изменить срок жизни токена входа, выполните следующие действия:

1. В панели управления системой виртуализации перейдите в раздел **Система** → **Пользователи**.
2. Выберите пользователя, с помощью которого Кибер Бэкап будет подключаться к системе виртуализации.
3. Перейдите в раздел **Аутентификация** и выберите **Управление токенами входа**.
4. В поле **Истечение, в секундах** укажите необходимое значение и нажмите **Получить новый токен**.



Используйте токен при установке агента.

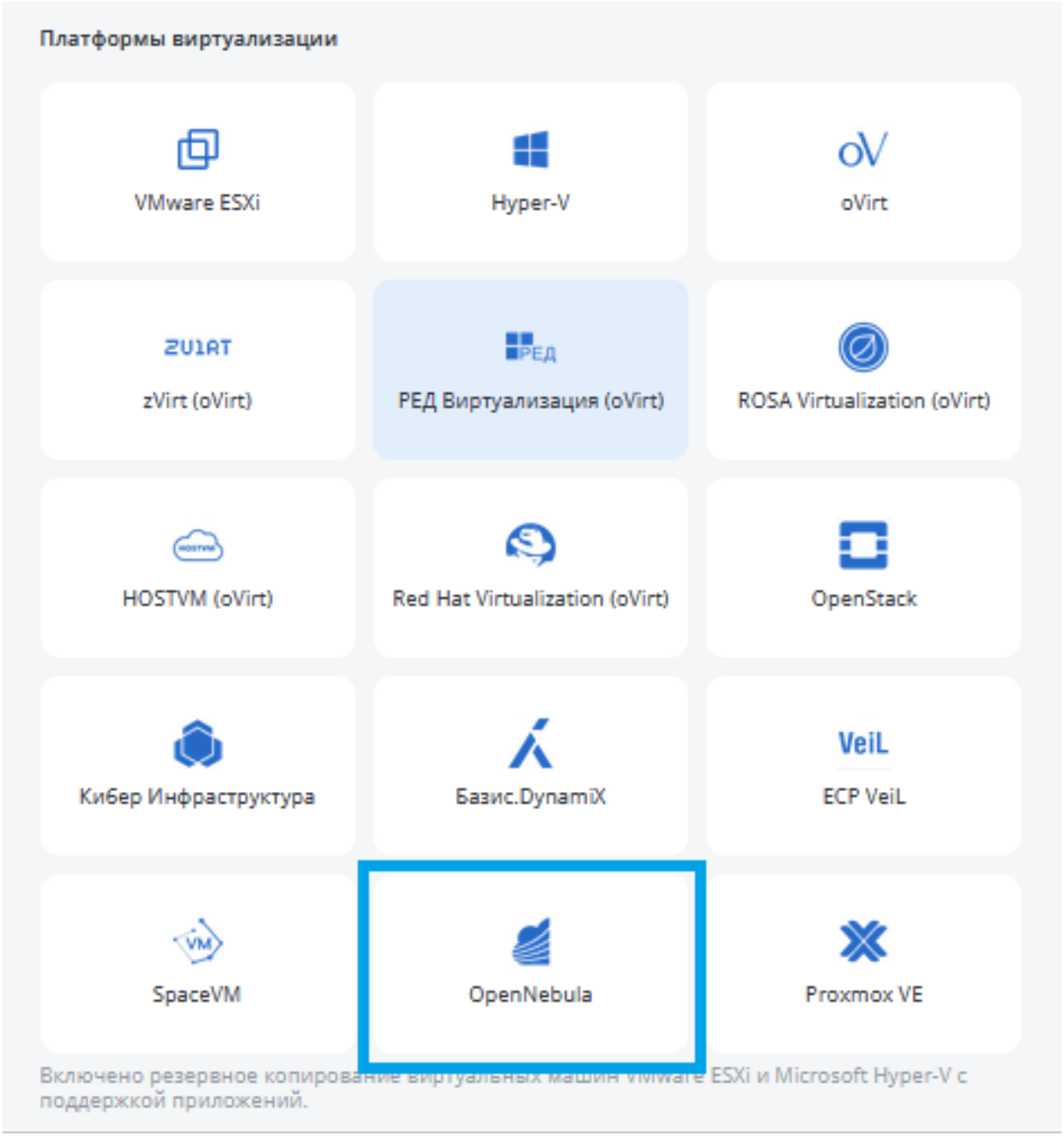
Известные проблемы и ограничения

- Не поддерживается резервное копирование RAW-дисков.
- Диски в системных хранилищах (System_DS) LVM_LVM обрабатываются как RAW-диски. Из-за ограничений платформы у таких хранилищ не поддерживается создание моментальных снимков диска и создание ”тонких” дисков.
- Из-за ограничений платформы создание моментальных снимков диска в хранилищах BREST_LVM не поддерживается. Резервное копирование виртуальных машин в таких хранилищах также не поддерживается.
- Резервное копирование в LVM-хранилищах на платформе OpenNebula версии 6.0.0.2 и ниже (например, ПК СВ ”Брест”, основанный на OpenNebula версии 6.0.0.2 и ниже) не гарантируется из-за ограничения самой платформы: размещение виртуального устройства в LVM-хранилище может приводить к сбоям в дисковых операциях.
- Не поддерживается резервное копирование временных дисков.
- Не поддерживаются CD/DVD-диски.
- Не поддерживается восстановление дисков, использующих интерфейс SATA. Из-за ограничений платформы SATA-диски обрабатываются как SCSI-диски.
- Не поддерживается восстановление ВМ с дисками VirtIO. Диски VirtIO обрабатываются как SCSI-диски.
- Из-за ограничений платформы виртуальное устройство с агентом запускается как служебная ВМ. По этой причине дискреционный режим работы платформы виртуализации характеризуется следующими особенностями:
  - ВМ запускается от имени системного пользователя `Oneadmin`;
  - Необходимо разворачивать виртуальное устройство путем ручной загрузки образа, если нет возможности использовать в системе запуск виртуального устройства как служебной ВМ;
  - Не работает отложенный запуск ВМ.

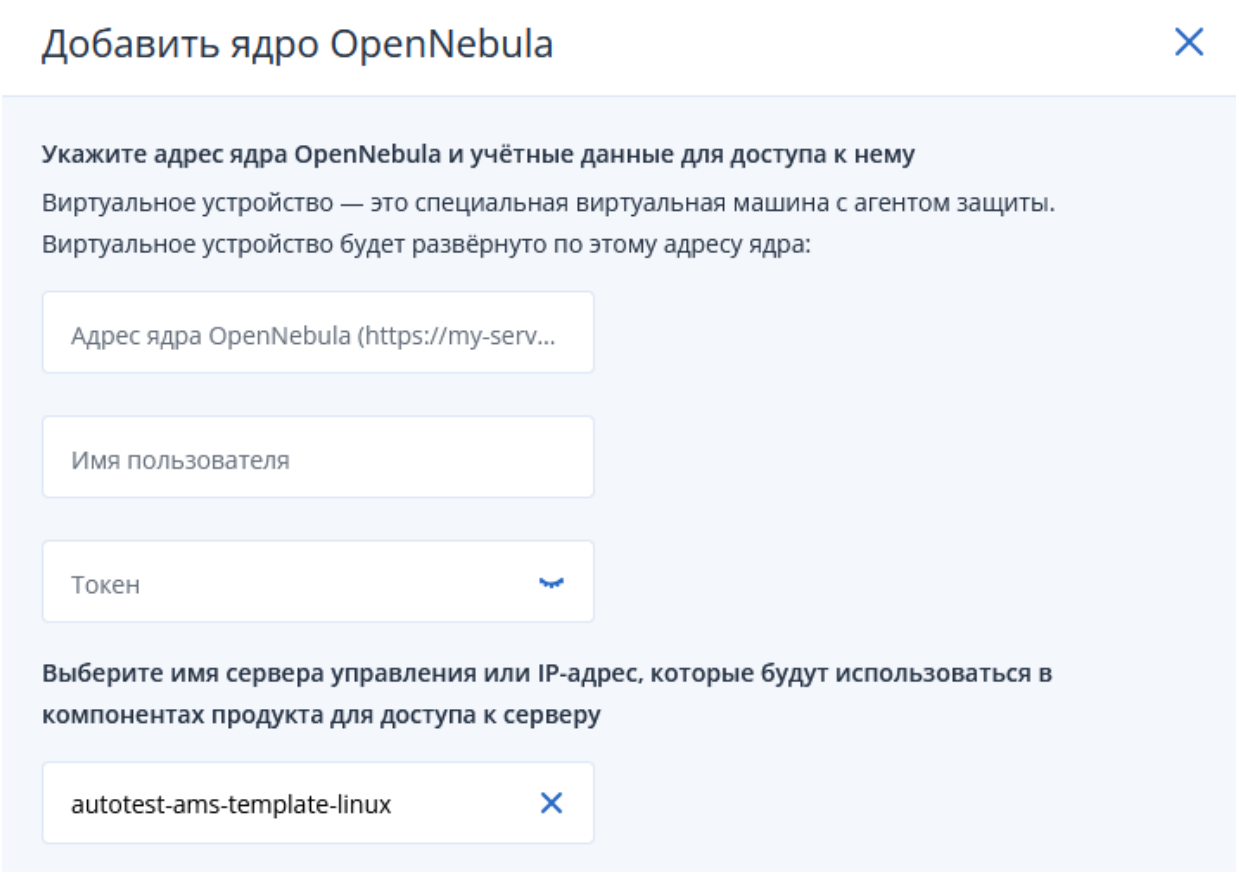
Автоматическая установка агента для OpenNebula

Для автоматической установки агента для OpenNebula выполните следующие действия:

1. В консоли Кибер Бэкап в разделе **Устройства** щёлкните **Добавить** и выберите OpenNebula.



2. Укажите адрес платформы, данные пользователя и сетевые настройки.



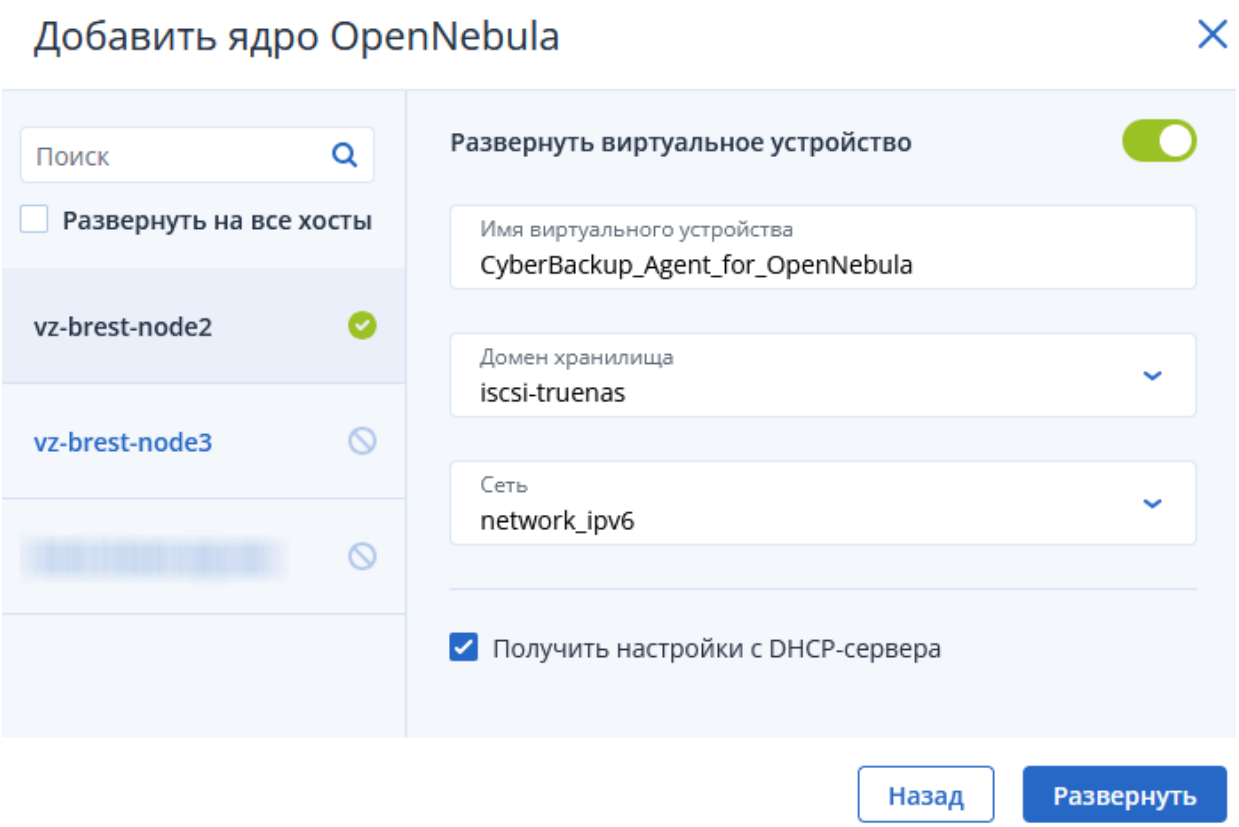
- В поле **Адрес ядра OpenNebula** укажите URL-адрес для доступа к серверу платформы виртуализации. В качестве этого адреса в OpenNebula используется конечная точка (например, для платформы ПК СВ ”Брест” для получения точки доступа перейдите в **Инфраструктура** → **Зоны**).

  Примечание

  Убедитесь, что в конфигурационном файле OpenNebula `oned.conf` адрес прослушивания для порта открыт в диапазоне с 127.0.0.0 до 0.0.0.0 или укажите конкретный IP-адрес.

- В поле **Имя пользователя** укажите имя пользователя (логин), с помощью которого Кибер Бэкап будет подключаться к системе виртуализации.
- В поле **Токен** укажите токен входа (см. *Настройка токена входа*).
- В нижнем поле укажите доменное имя или IP-адрес сервера управления Кибер Бэкап.

3. Нажмите **Далее** и укажите дополнительные параметры.



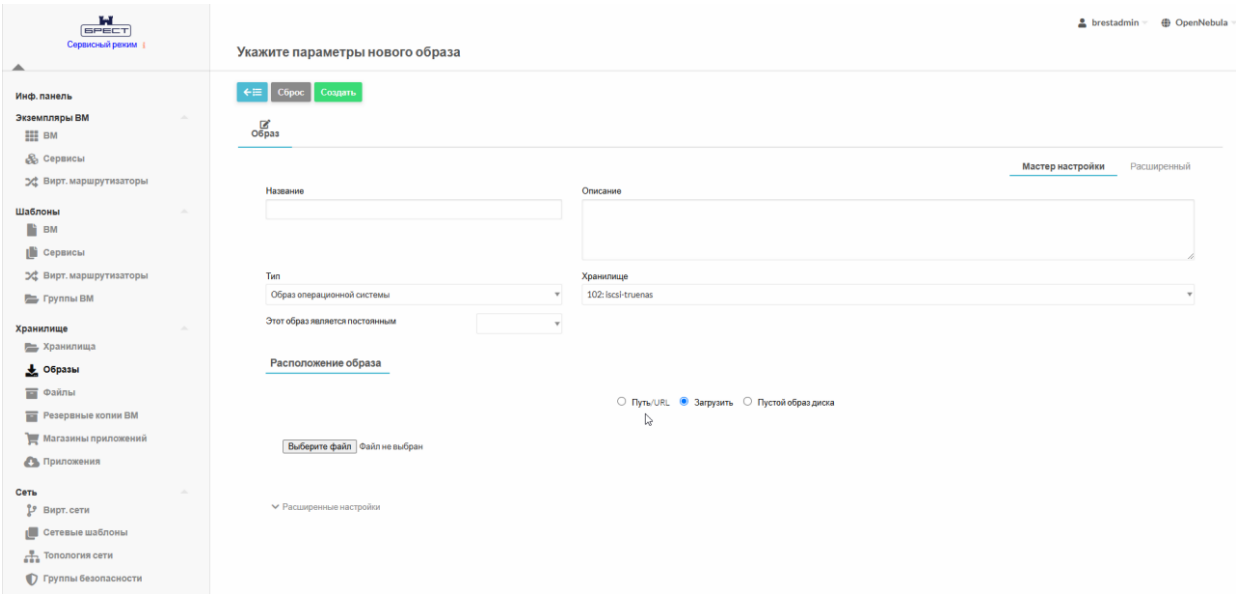
Задайте имя виртуального устройства, выберите кластер, домен и сеть, с которыми будет взаимодействовать виртуальное устройство. Если необходимо, укажите сетевые настройки вручную, сняв флажок **Получить настройки с DHCP-сервера**.

4. Нажмите **Развернуть** и дождитесь завершения процедуры развертывания. Убедитесь, что виртуальное устройство с агентом появилось в интерфейсе платформы виртуализации в списке виртуальных машин.

Установка агента для OpenNebula вручную

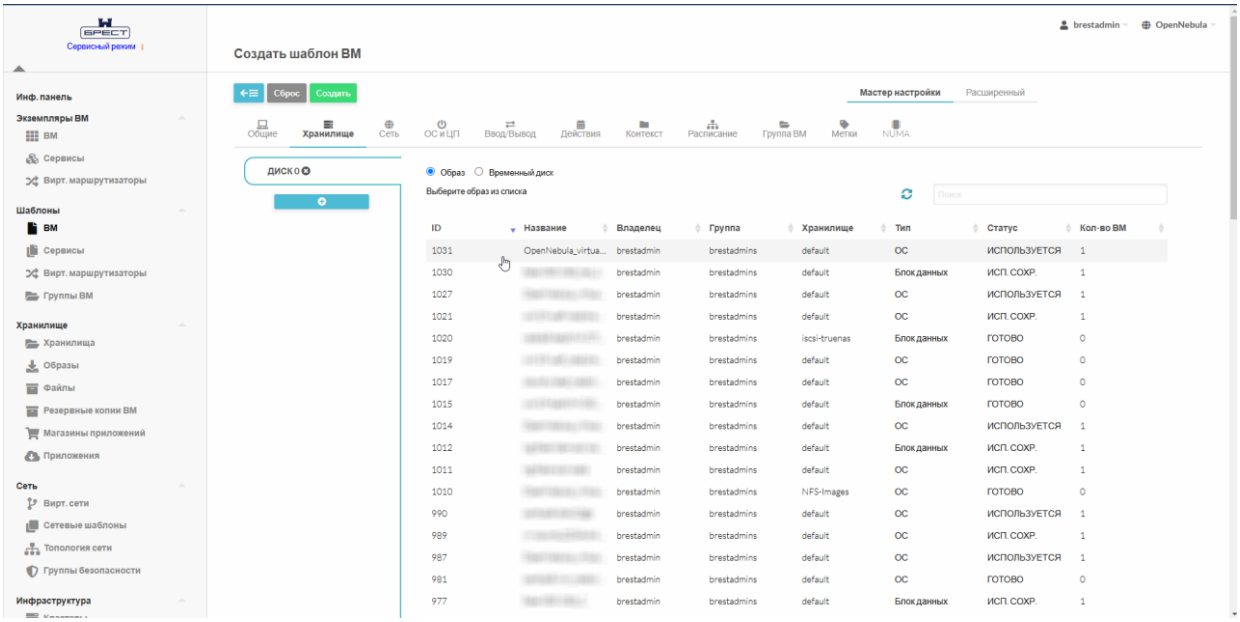
Для установки вручную агента для OpenNebula выполните следующие действия:

1. Скачайте пакет установки агента OpenNebula (файл формата `.qcow2`, например: `OpenNebulaAppliance.qcow2`).
2. Распакуйте образ виртуального устройства.
3. В панели управления системой виртуализации (например, ПК СВ ”Брест”) перейдите в раздел **Хранилище** → **Образы**.
4. Отметьте флажок **Загрузить** и далее щёлкните **Выберите файл**.



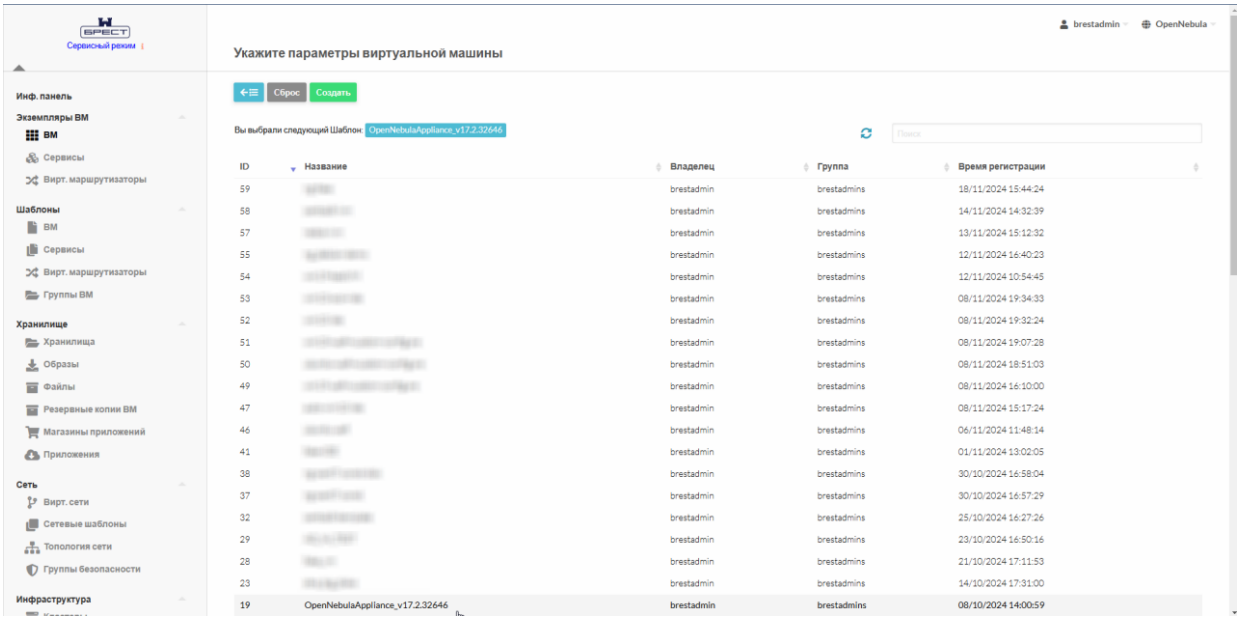
5. Укажите скачанный файл образа виртуального устройства и подтвердите загрузку.

6. Перейдите в раздел **Шаблоны** → **ВМ** и нажмите **Создать**.



7. Выберите из списка появившееся виртуальное устройство и укажите необходимые настройки для создания шаблона на основе образа виртуального устройства.

8. Перейдите в список виртуальных машин **Экземпляры ВМ** → **ВМ** и отметьте в списке появившийся там шаблон.

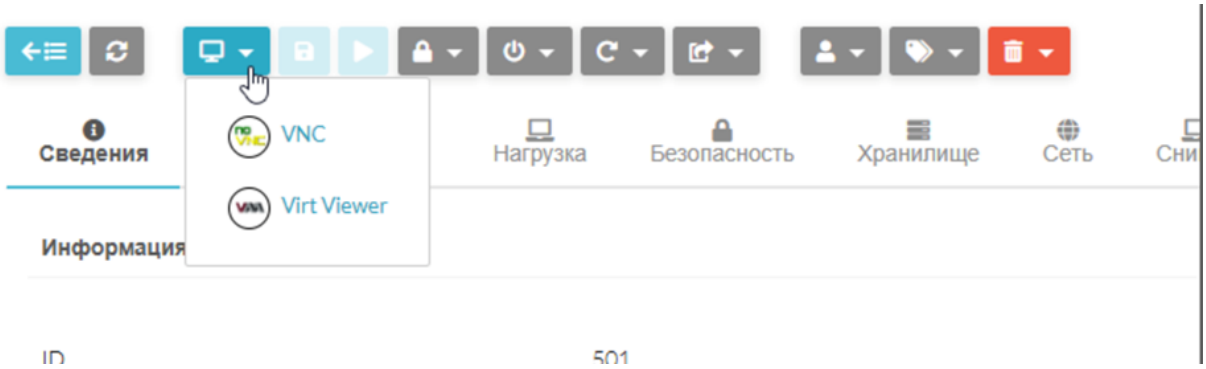


9. Щёлкните **Создать** и подтвердите создание ВМ на основе выбранного шаблона и укажите необходимые настройки, в том числе:

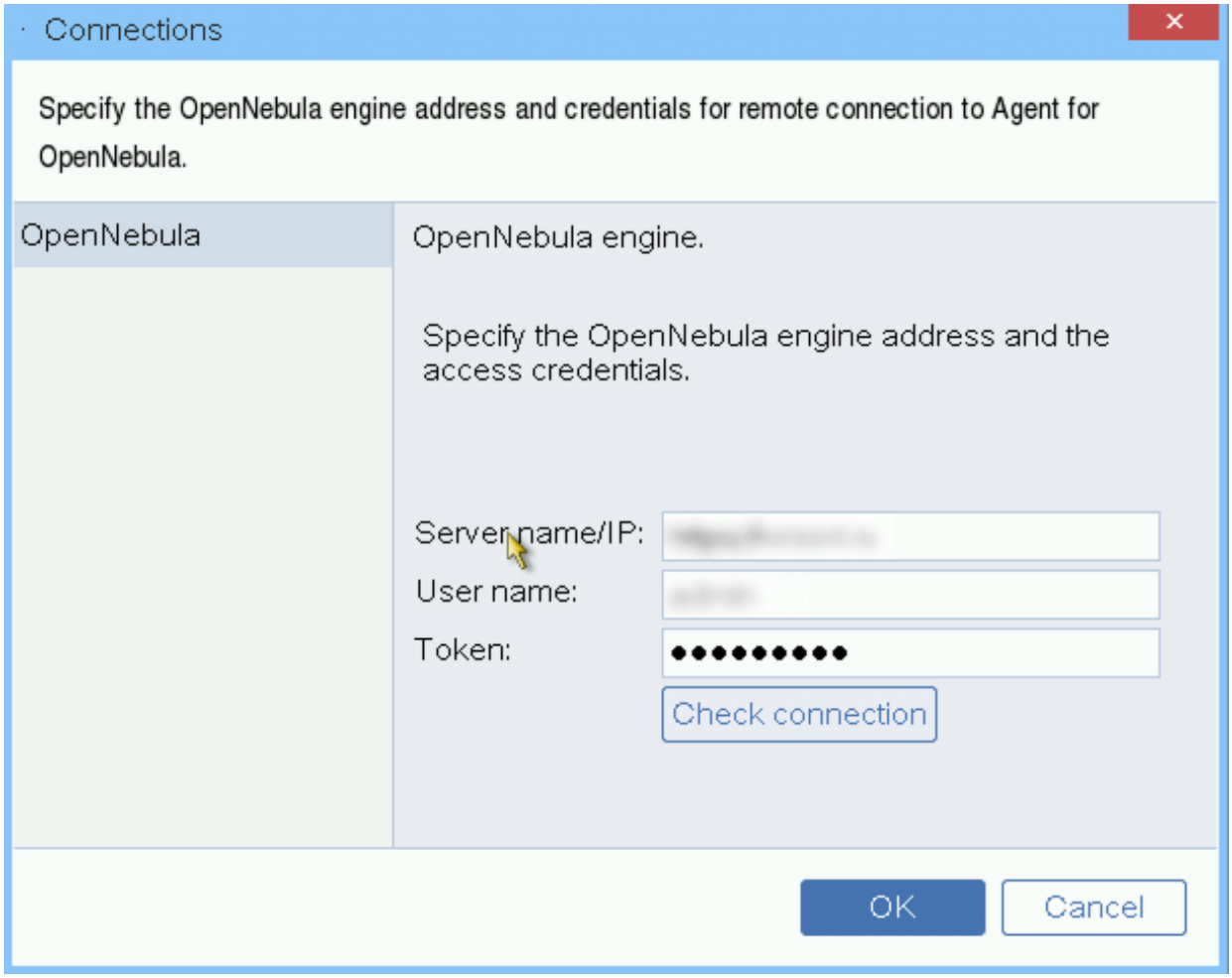
    - Количество процессоров CPU: не менее 2;
    - Количество памяти RAM: не менее 4 Гб;
    - Объем жесткого диска: не менее 8 Гб.

10. Убедитесь, что виртуальное устройство с агентом Кибер Бэкап для OpenNebula появилось в списках ВМ.

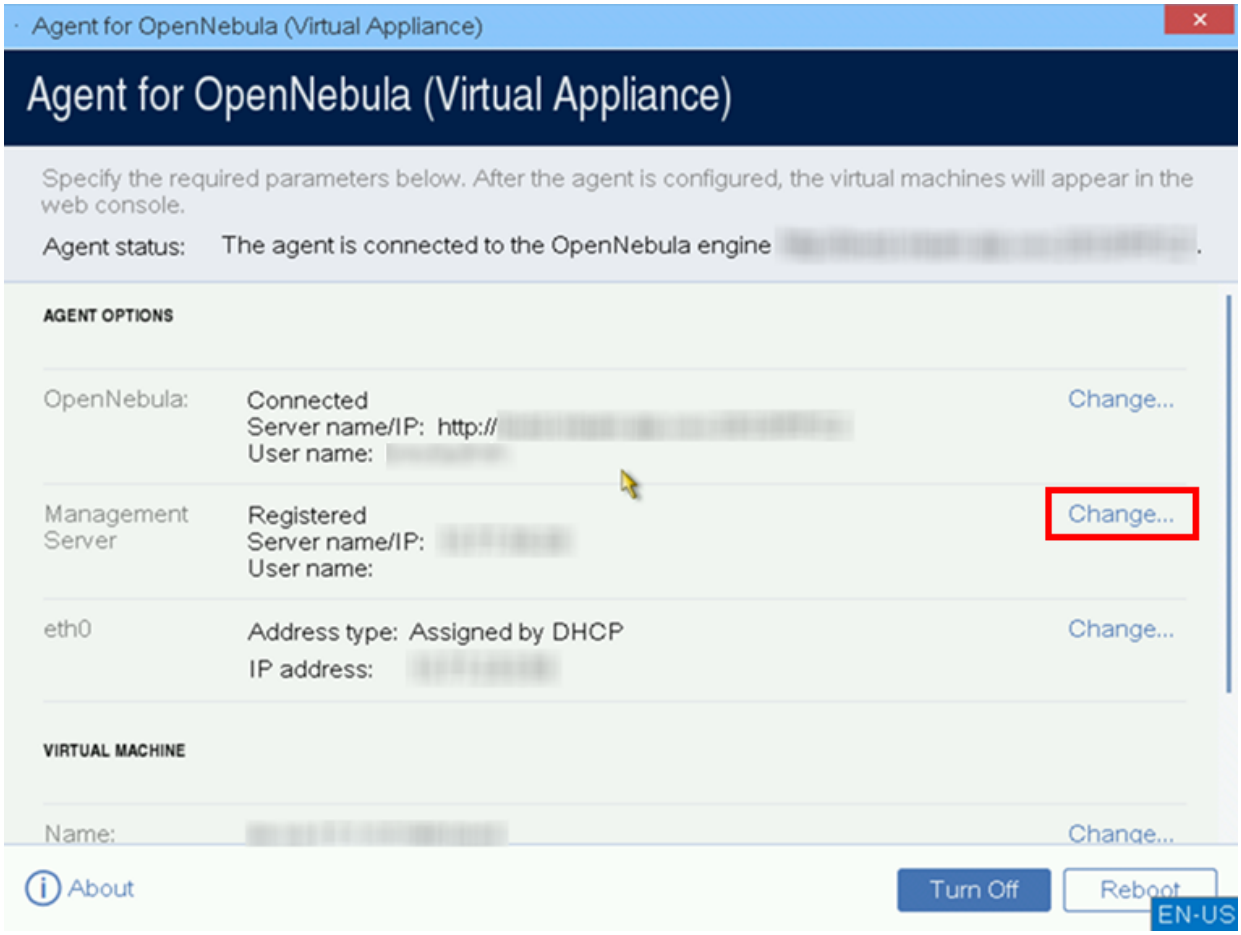
11. Подключитесь к консоли виртуальной машины: в панели управления ВМ нажмите **VNC**. Отобразится меню интеграции с OpenNebula.



12. В разделе **OpenNebula** нажмите **Change** и укажите URL-адрес сервера платформы виртуализации в формате `http://<IP-адрес>:2633/RPC2`, имя пользователя и токен входа (см. *Настройка токена входа*).



13. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учетные данные для подключения к нему.



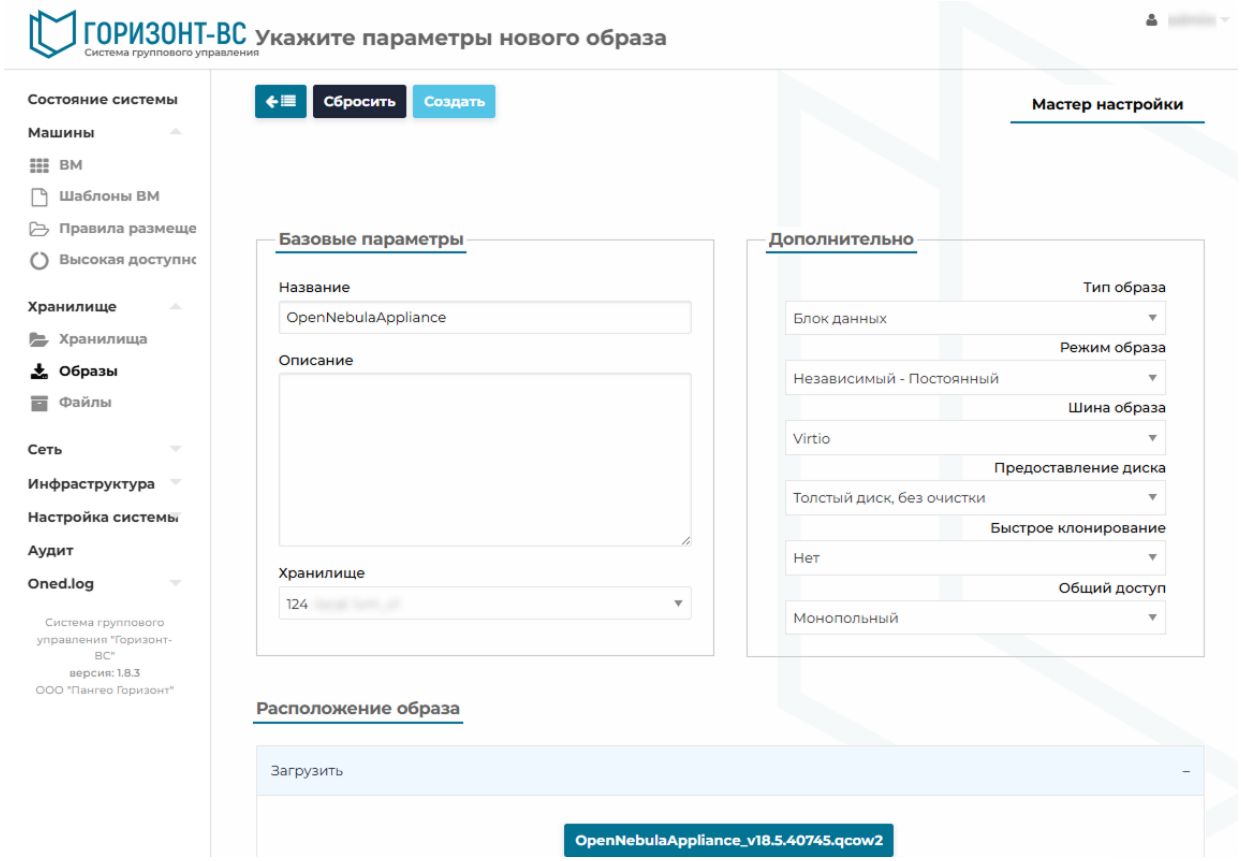
14. Перезапустите виртуальную машину.
15. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап отображаются устройства OpenNebula.

Установка агента для OpenNebula вручную в СГУ ”Горизонт-ВС”

Для установки вручную агента для OpenNebula в Системе группового управления ”Горизонт-ВС” выполните следующие действия:

1. Скачайте пакет установки агента OpenNebula (файл формата `.qcow2`, например: `OpenNebulaAppliance.qcow2`).
2. В панели управления Системы группового управления ”Горизонт-ВС” перейдите в раздел **Хранилище** → **Образы**.
3. Щёлкните значок плюса в верхнем меню и заполните поля в появившейся форме. При этом в блоке **Дополнительно** для параметра **Тип образа** выберите значение **Блок данных**.
4. В блоке **Расположение образа** нажмите **Загрузить файл** и выберите скачанный на шаге 1 файл с пакетом установки агента OpenNebula. В результате название выбранного файла будет отображено в области кнопки **Загрузить файл**.

5. Щёлкните **Создать** в верхнем меню.



6. Подключитесь по SSH к машине с Системой группового управления ”Горизонт-ВС” и выполните команду:

```
bhcs
```

7. Создайте файл с шаблоном виртуальной машины:

```
mcedit <имя_файла_с_шаблоном>
```

Где:

- `<имя_файла_с_шаблоном>` — имя создаваемого файла с шаблоном виртуальной машины (например, `template`).

8. В созданном файле укажите текст конфигурации:

```
NAME = <имя_файла_с_шаблоном>
AUTOSTART = ”0”
CONTEXT = [
  NETWORK = ”YES”,
  SSH_PUBLIC_KEY = ”$USER[SSH_PUBLIC_KEY]” ]
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
CPU = ”1”
DISK = [
  CACHE = ”none”,
  IMAGE = ”<имя_загруженного_с_сайта_файла>”,
  IMAGE_UNAME = ”admin” ]
FEATURES = [
  GUEST_AGENT = ”yes” ]
GRAPHICS = [
  LISTEN = ”0.0.0.0”,
  TYPE = ”VNC” ]
INPUT = [
  BUS = ”usb”,
  TYPE = ”tablet” ]
LOGO = ”images/logos/redos.svg”
MEMORY = ”4096”
NIC = [
  MODEL = ”virtio”,
  NETWORK = ”Public”,
  NETWORK_UNAME = ”admin” ]
OS = [
  ARCH = ”x86_64”,
  AUTOSTART = ”NO”,
  BIOS = ”LEGACY”,
  BOOTMENU = ”NO”,
  HA = ”NO”,
  SMBIOS_MODE = ”sysinfo” ]
SYSINFO=[
  VENDOR_INFO=”yes”,
  VM_INFO=”yes”
]
USB_CONTROLLER = ”XHCI”
VCPU = ”2”
VGA_ADAPTER = [
  ACCEL3D = ”no”,
  HEADS = ”1”,
  MODEL = ”qxl”,
  RENDERNODE = ”” ]
```

В тексте конфигурации замените значения параметров `NAME` и `IMAGE`, где:

- `<имя_файла_с_шаблоном>` — имя создаваемого на шаге 7 файла с шаблоном виртуальной

машины (например, `template`);

- `<имя_загруженного_с_сайта_файла>` — имя файла с пакетом установки агента OpenNebula, загруженного на шаге 1 (например, `OpenNebulaAppliance`).

9. Завершите создание шабона, выполнив команду:

```
onetemplate create <имя_файла_с_шаблоном>
```

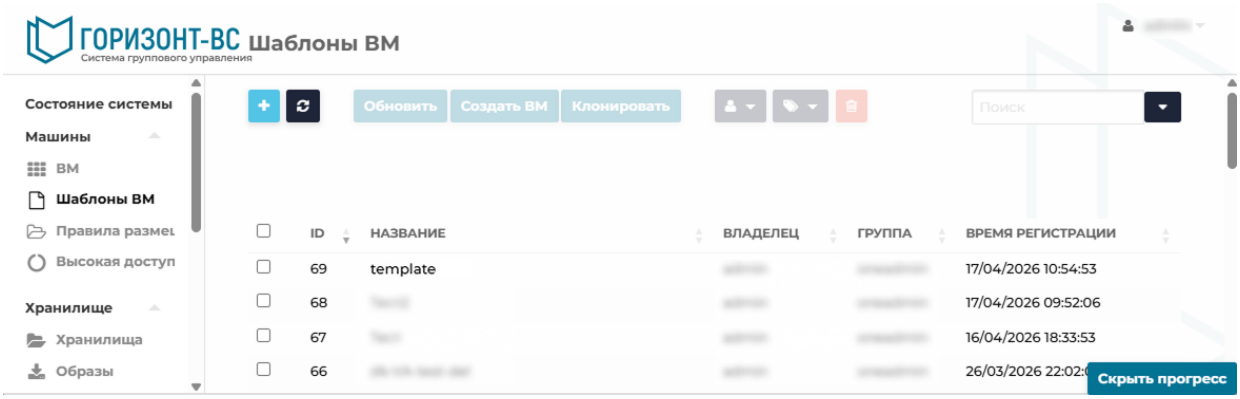
Где:

- `<имя_файла_с_шаблоном>` — имя создаваемого файла с шаблоном виртуальной машины (например, `template`).

Убедитесь в отображении номера созданного шаблона в ответе команды (например, `ID: 69`).

10. В панели управления Системы группового управления ”Горизонт-ВС” перейдите в раздел **Машины** → **Шаблоны ВМ**.

11. Убедитесь в отображении созданного шаблона в списке. Для поиска воспользуйтесь номером созданного шабона из предыдущего шага.



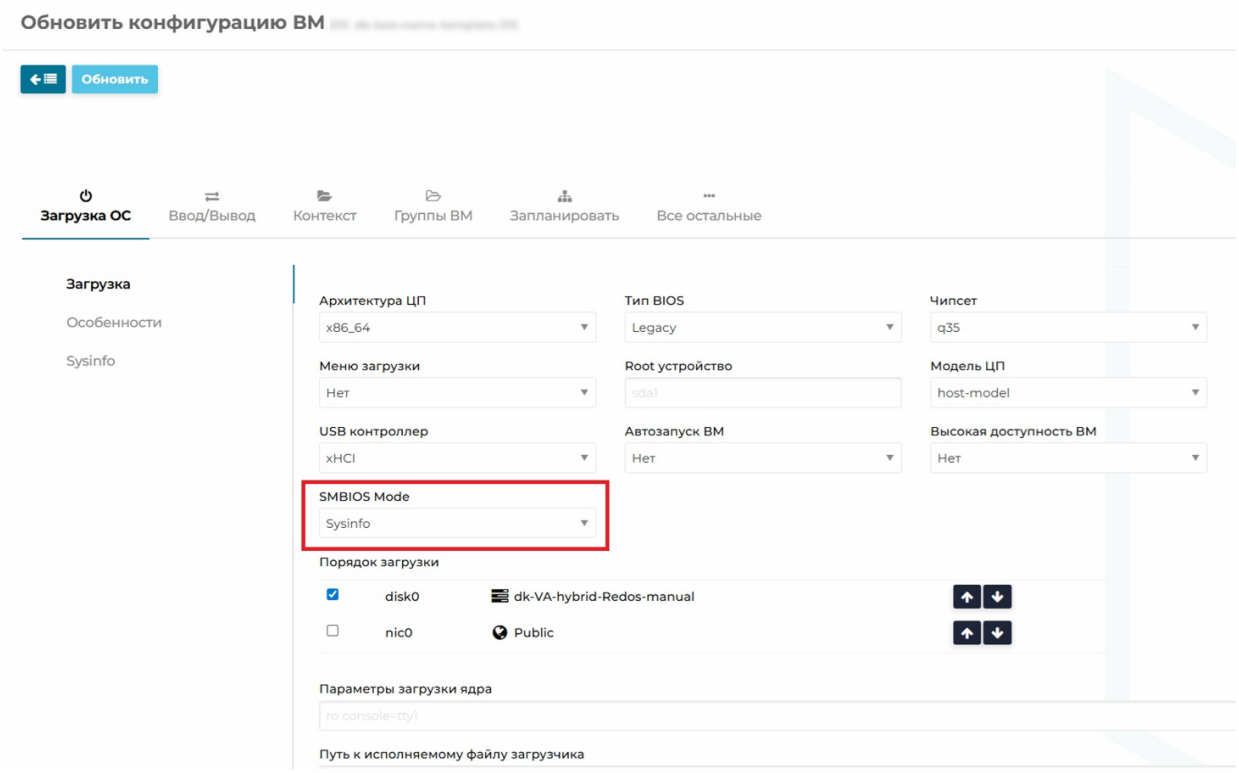
12. Перейдите в раздел **Машины** → **ВМ**.

13. Щёлкните значок плюса в верхнем меню, выберите созданный шаблон и нажмите **Создать**. Дождитесь окончания процесса создания виртуальной машины и отображения её в списке виртуальных машин со статусом **Запущено**.

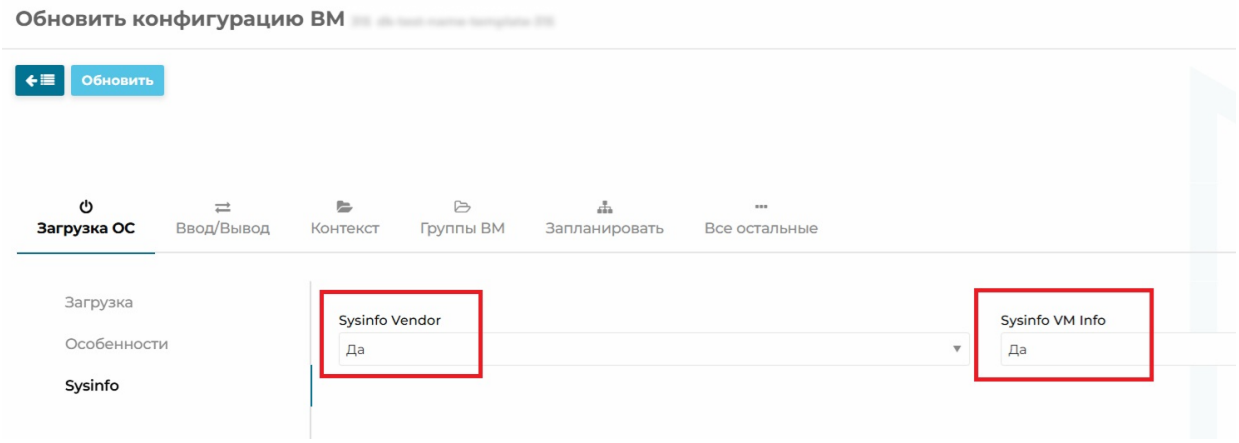
14. Выберите созданную вирутуальную машину в списке и отключите её питание.

15. После отключения питания виртуальной машины в верхнем меню перейдите в раздел **Конфигурация** и щёлкните **Обновить конфигурацию**.

16. В верхнем меню перейдите в раздел **Загрузка ОС**, на панели слева выберите **Загрузка**. После этого для параметра **SMBIOS Mode** установите значение **Sysinfo**.

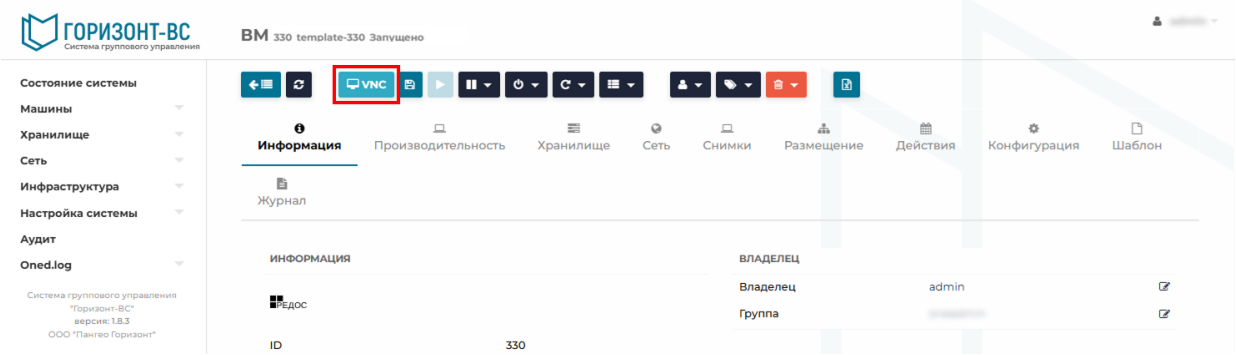


17. На панели слева выберите **Sysinfo** и установите для параметров **Sysinfo Vendor** и **Sysinfo VM Info** значение **Да**. Затем щёлкните **Обновить**.

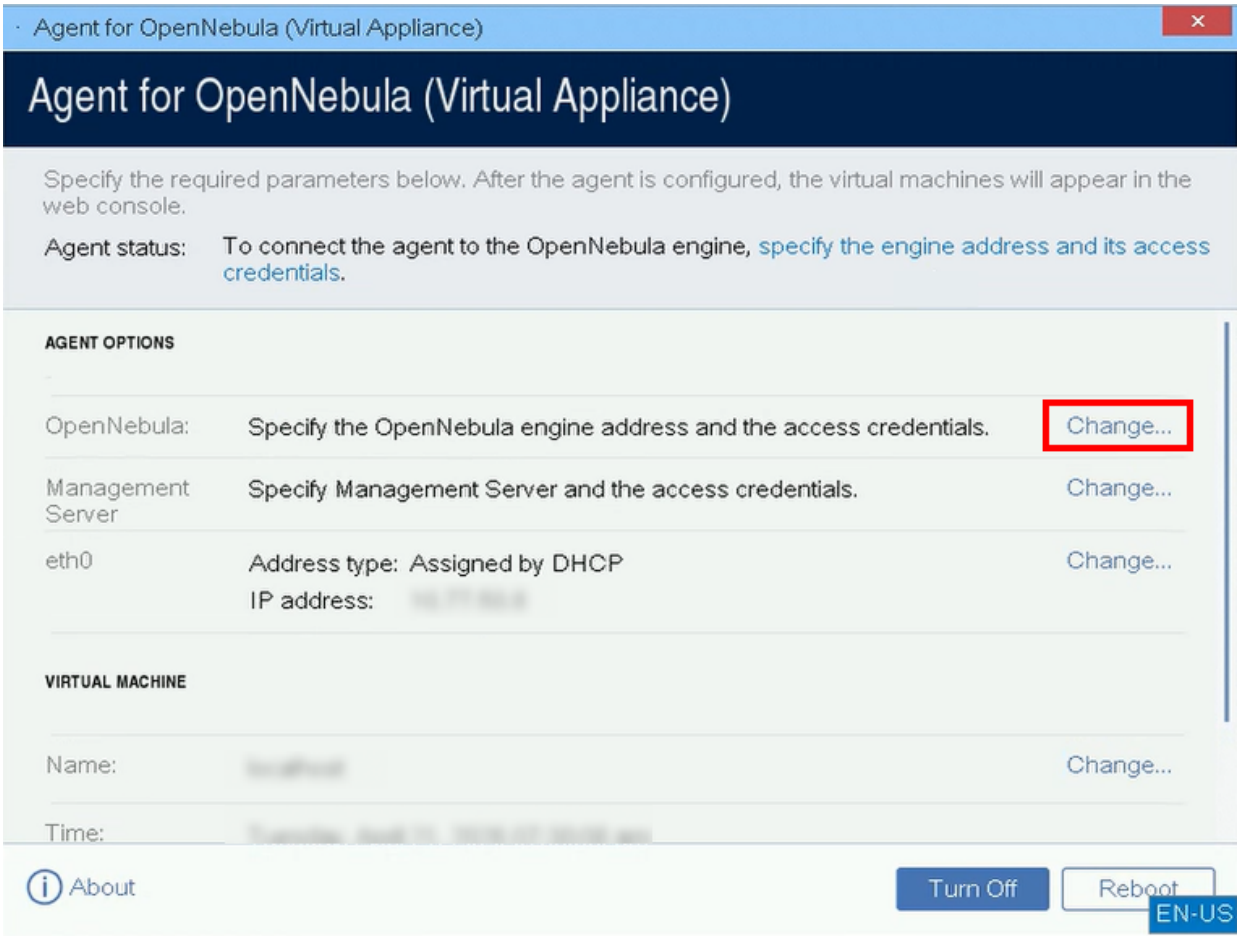


18. Запустите виртуальную машину.

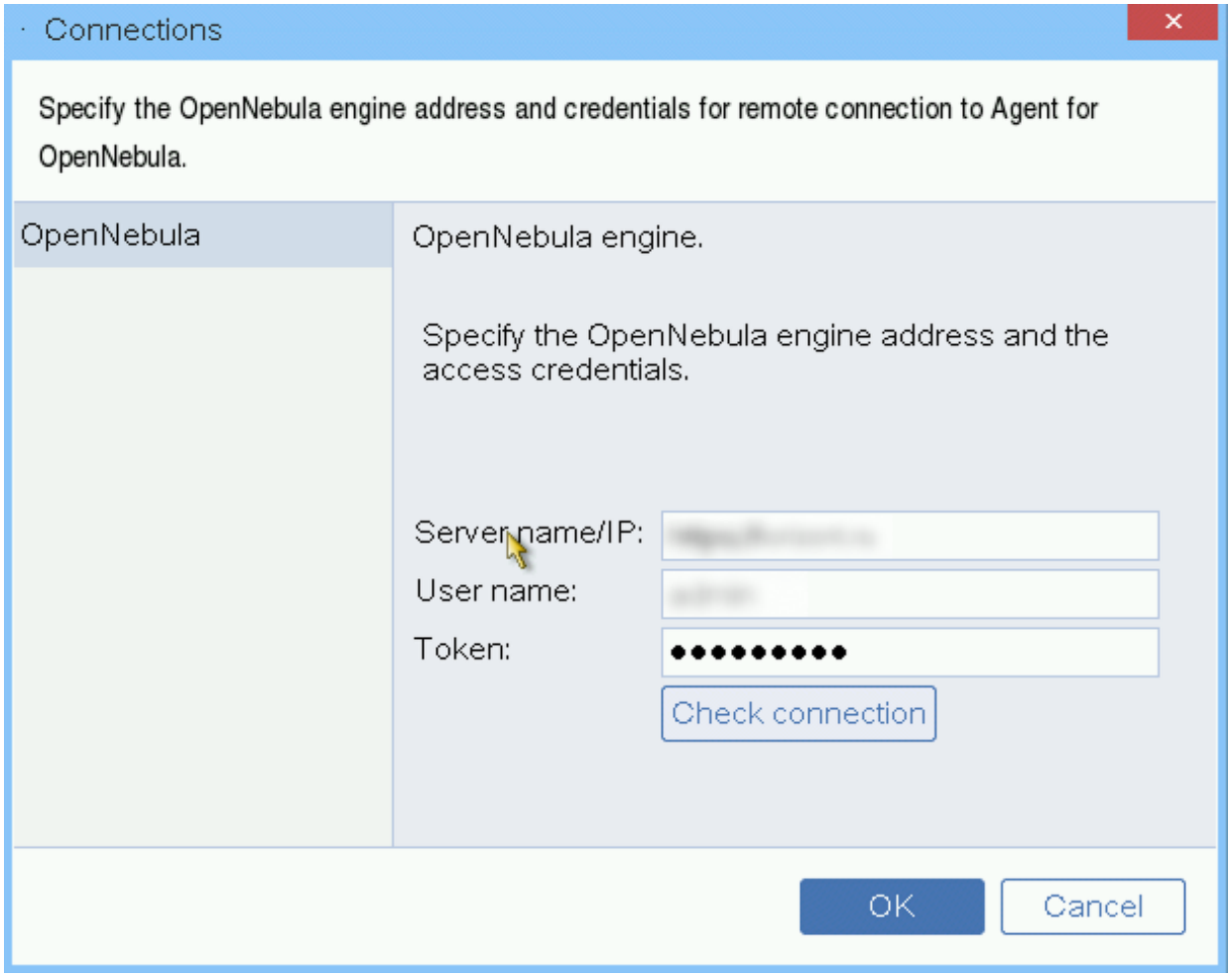
19. Подключитесь к консоли виртуальной машины, щёлкнув **VNC** в верхнем меню.



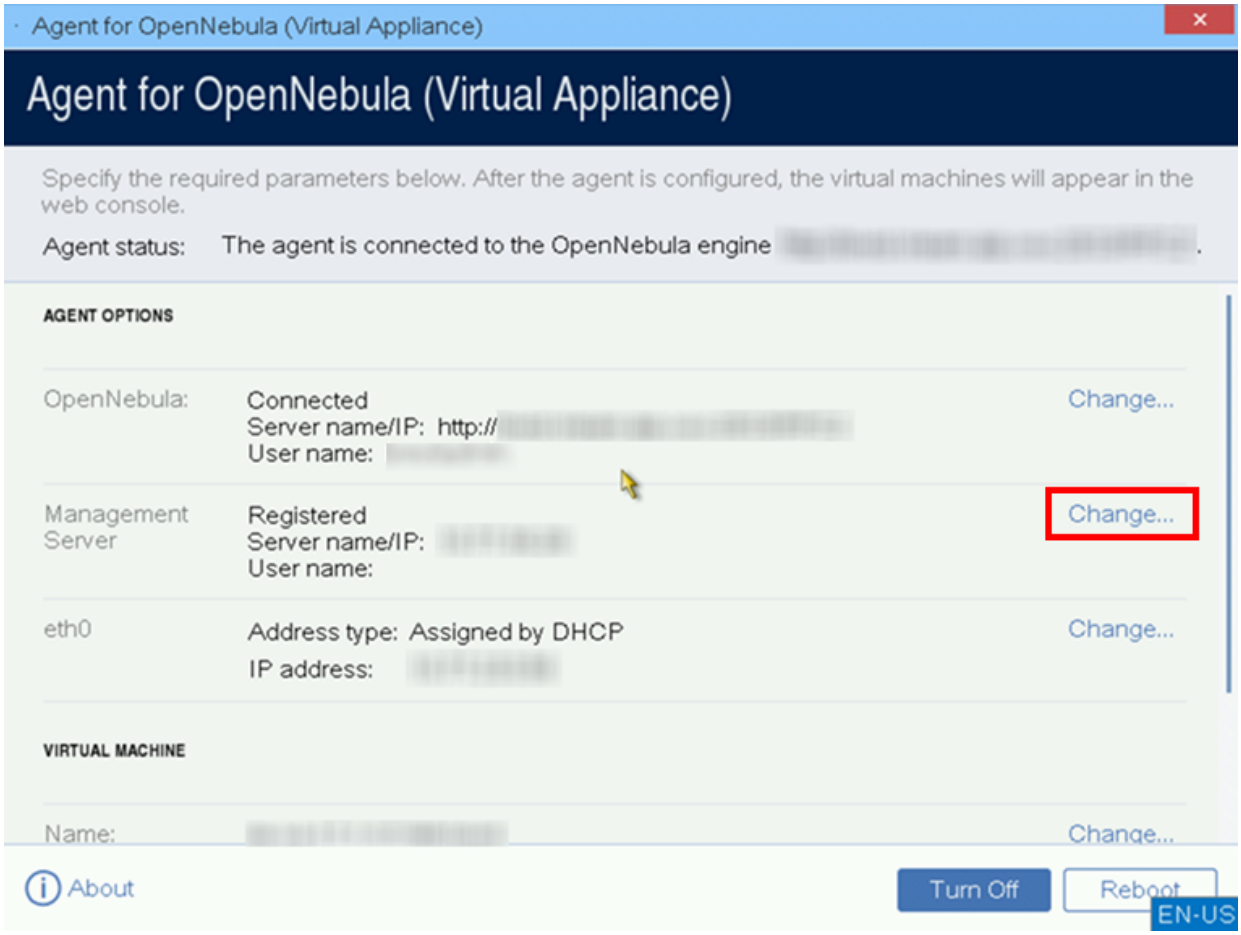
20. В разделе **OpenNebula** нажмите **Change**.



21. В появившемся окне укажите IP-адрес сервера Системы группового управления ”Горизонт-ВС”, имя пользователя и токен входа (см. *Настройка токена входа*).



22. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учётные данные для подключения к нему.



23. Убедитесь, что в разделе **Настройки** → **Агенты** веб-консоли Кибер Бэкап отображается созданное виртуальное устройство.

Установка агента для Proxmox

Для работы с виртуальными машинами на хосте Proxmox необходимо развернуть виртуальное устройство — виртуальную машину с агентом Кибер Бэкап.

Общие сведения

1. Для резервного копирования и восстановления данных Proxmox VE понадобятся установленные и настроенные продукты:
   - Кибер Бэкап версии 18 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. *Издания и лицензии Кибер Бэкап*);
   - Система управления виртуализацией.
2. Поддерживаются следующие системы управления виртуализацией:
   - Proxmox Virtual Environment;

- Альт Виртуализация редакции PVE.

Подробнее о поддерживаемых версиях вышеуказанных продуктов см. раздел *Поддерживаемые платформы виртуализации*.

3. Для корректной работы Кибер Бэкап и Proxmox VE виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество центральных процессоров (CPU): 2;
   - Объем ОЗУ: 4 ГБ;
   - Объем диска: 8 ГБ.

Планирование количества агентов для Proxmox

Агент для Proxmox контролирует виртуальные машины только на том сервере Proxmox, на котором он установлен. Для резервного копирования всех виртуальных машин в кластере необходимо развернуть агенты на каждом сервере Proxmox.

Известные проблемы и ограничения

- Из-за ограничений системы Proxmox VE при восстановлении виртуальной машины в *новую ВМ* необходимо в настройках новой ВМ указывать не более четырех виртуальных процессоров. Для увеличения производительности ВМ в консоли Proxmox VE можно увеличить количество ядер для данной ВМ.
- Виртуальное устройство поддерживает следующие типы контроллеров: VirtiO SCSI, VirtiO SCSI Single, LSI 53C895A, VMware PVSCSI.
- Для аутентификации пользователя на виртуальном устройстве доступны следующие методы: LDAP и Linux PAM Standard Authentication. Подробнее см. в документации Proxmox VE.
- В ряде случаев Proxmox дублирует UUID-идентификаторы SMBIOS в виртуальных машинах. Такие ВМ не отображаются в списках в Кибер Бэкап. В таких случаях необходимо вручную изменить идентификаторы на уникальные.
- Хранилища iSCSI/kernel, iSCSI/libiscsi и Ceph/RBD не поддерживаются.
- Совместимость продукта Кибер Бэкап с хранилищами CephFS, Proxmox Backup и BTRFS не проверялась.

Установка агента для Proxmox вручную

Чтобы установить вручную агент для Proxmox, выполните следующие действия:

1. Загрузите пакет установки агента Proxmox с сайта компании (файл формата .qcow2; например, `ProxmoxAppliance.qcow2`).
2. Войдите как администратор в панель управления системы виртуализации Proxmox VE.
3. Создайте виртуальную машину без подключенных дисков:
    1. В верхнем левом углу панели управления нажмите **Create VM**.
    2. Укажите следующие данные в окне создания ВМ:
        1. На вкладке **General** задайте имя ВМ.
        2. На вкладке **OS** выберите пункт **Do not use any media**.
        3. На вкладке **System** в поле **SCSI Controller** выберите один из поддерживаемых контроллеров: VirtIO SCSI, VirtIO SCSI Single, LSI 53C895A, VMware PVSCSI.
        4. На вкладке **Disks** удалите диск, который предлагается создать вместе с ВМ.
        5. На вкладке **CPU** в поле **Cores** укажите минимум 2 ядра процессора.
        6. На вкладке **Memory** укажите минимум 4 ГБ оперативной памяти.

    Укажите остальные настройки согласно документации Proxmox VE (ссылка на документацию находится в правом верхнем углу панели управления).
4. Загрузите диск установки агента на сервер системы виртуализации Proxmox VE. Например, выполните команду:

    ```
    cd /mnt/pve/nfsproxmox/template
    wget адрес_архива/ProxmoxAppliance.qcow2
    ```

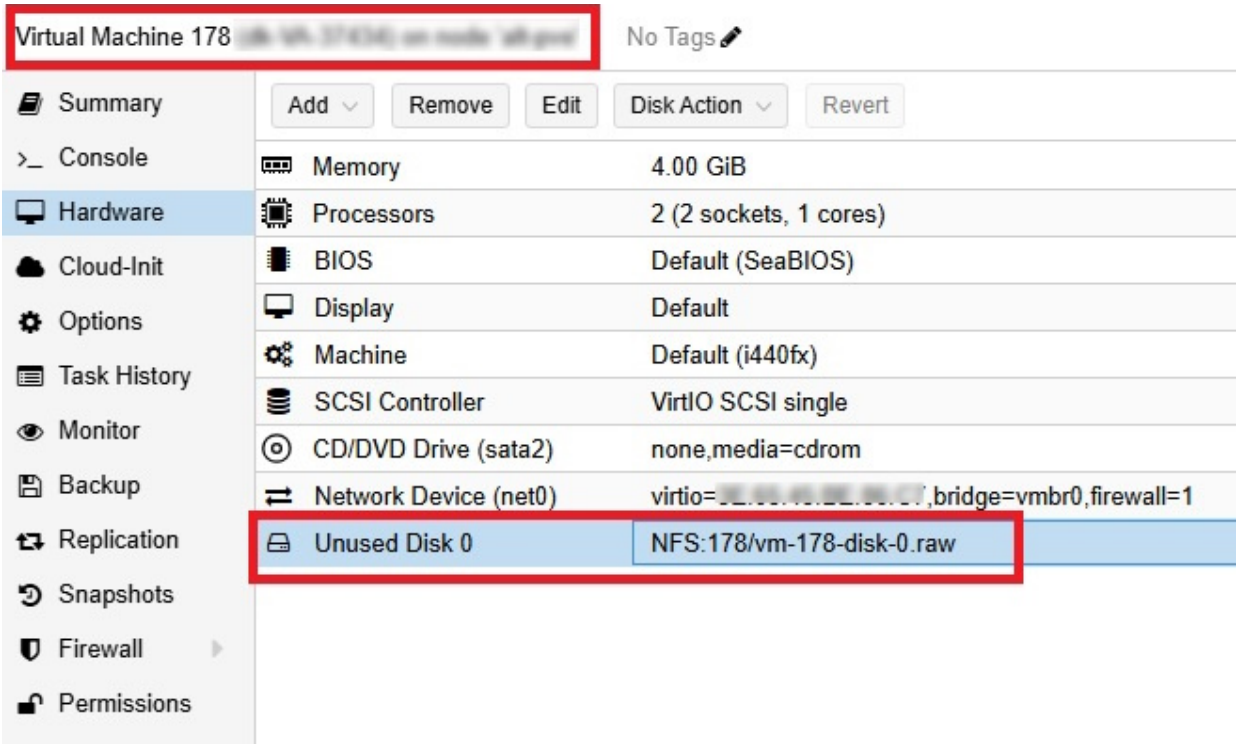
5. Подключите диск агента для ранее созданной ВМ. Например, выполните команду:

    ```
    qm importdisk 178 ProxmoxAppliance.qcow2 NFS
    ```

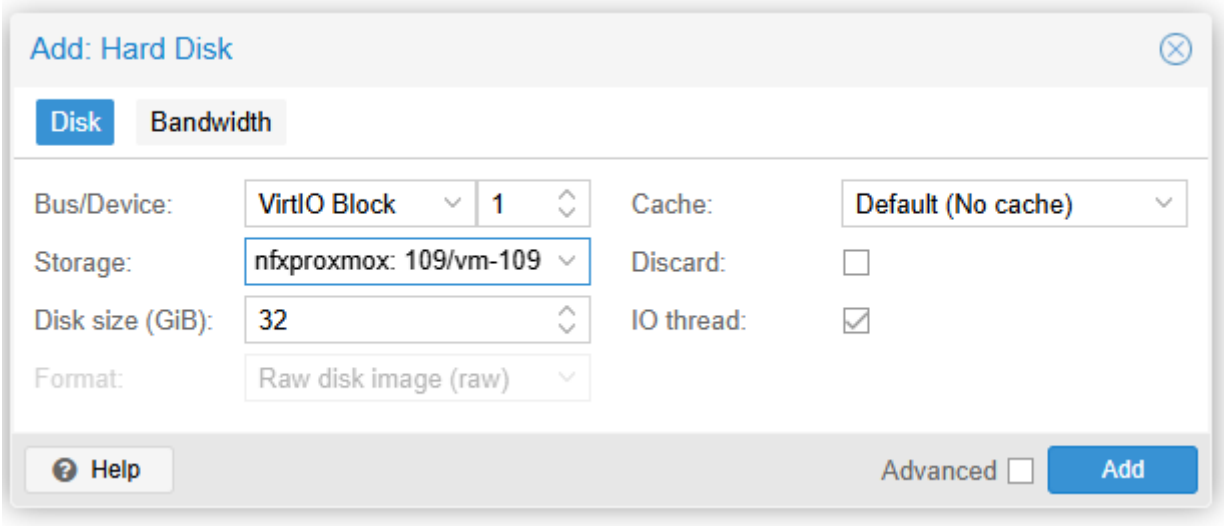
    Где:

    - `178` — ID виртуальной машины, созданной на шаге 3 данной инструкции;
    - `ProxmoxAppliance.qcow2` — имя пакета установки агента;
    - `NFS` — имя хранилища в Proxmox, куда будет помещён диск.
6. Выберите в списке созданную виртуальную машину и перейдите в раздел **Hardware**.

7. Откройте подключенный диск с именем **Unused Disk 0**.



8. В поле **Bus/Device** выберите **VirtIO Block**.



9. Установите для нового диска первый приоритет в порядке загрузки:
    1. Выберите в списке виртуальную машину и нажмите **Options**.
    2. Выберите **Boot Order** и нажмите **Edit**.
    3. Перенесите диск, импортированный из пакета установки, на первое место в списке и поставьте для него галочку **Enabled**.
10. Подключитесь к консоли виртуальной машины.

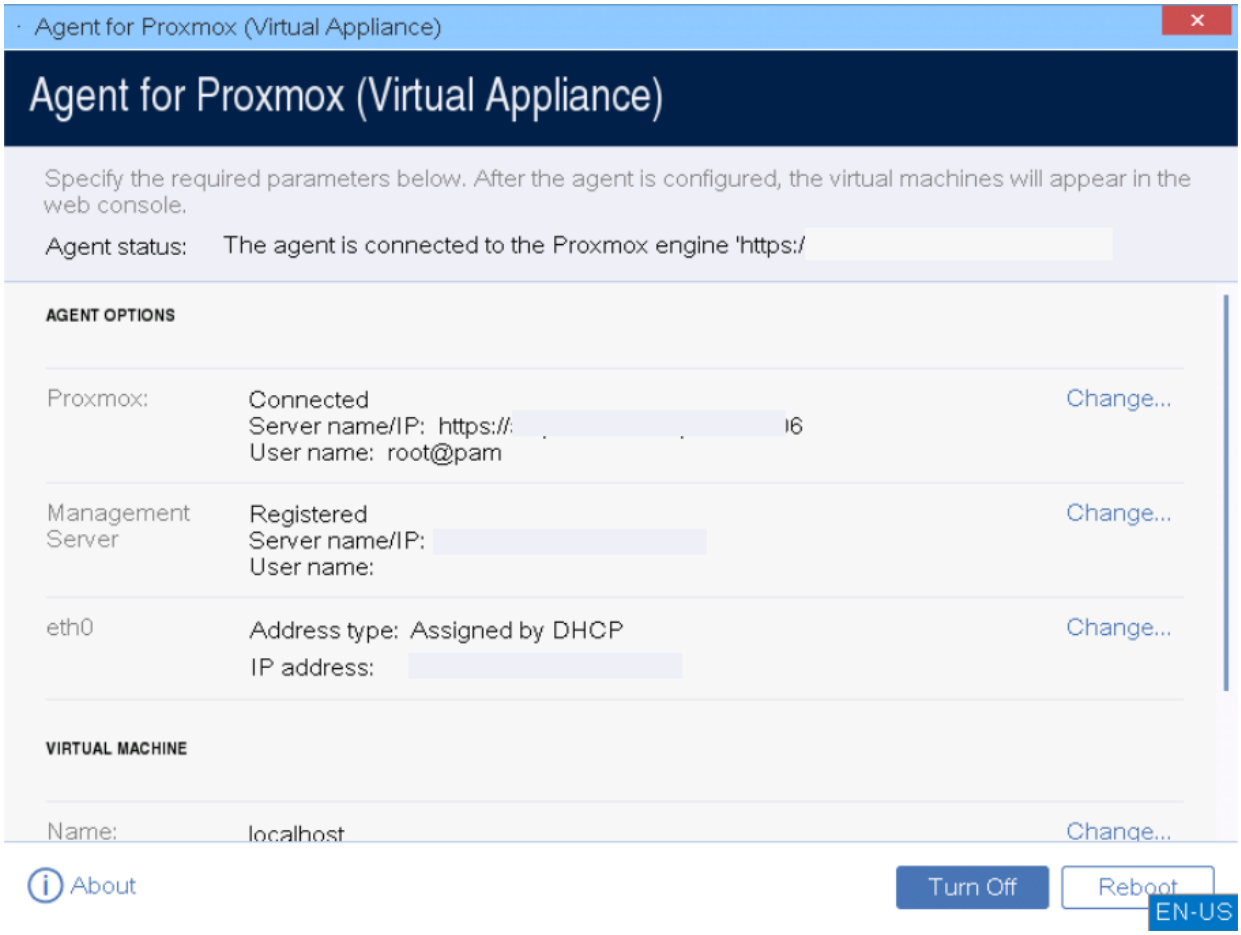
11. В разделе **Proxmox** нажмите **Change** и укажите:

    - URL-адрес системы виртуализации Proxmox VE в формате `https://<IP-адрес>:8006`

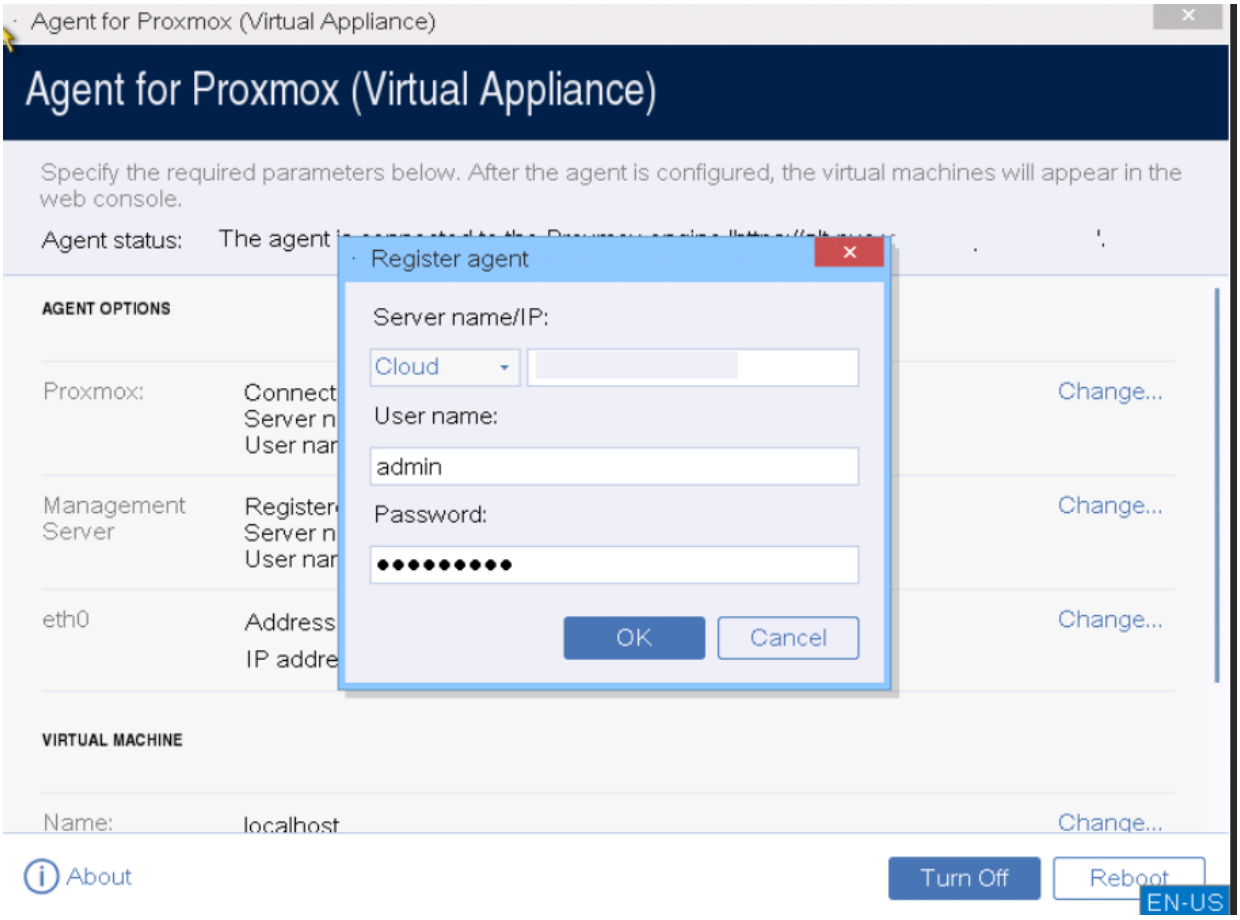
      Где:

      - `<IP-адрес>` — IP-адрес системы виртуализации Proxmox VE;
      - `8006` — порт подключения.

    - имя пользователя и пароль администратора.



12. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап и учетные данные для подключения к нему.



13. Перезапустите виртуальную машину.
14. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап отображаются устройства Proxmox VE.

Установка агента для VMmanager

Общие сведения

1. Для резервного копирования данных VMmanager понадобятся установленные и настроенные продукты:
   - Кибер Бэкап версии 19 или выше с лицензией Кибер Бэкап Расширенная редакция для платформы виртуализации (подробнее о лицензиях см. в разделе *Издания и лицензии Кибер Бэкап*);
   - VMmanager (список поддерживаемых версий приведён в разделе *Поддерживаемые платформы виртуализации*).
2. Для корректной работы Кибер Бэкап и VMmanager виртуальное устройство должно отвечать следующим минимальным требованиям:

- количество ядер центрального процессора: 2;
- объем ОЗУ: 4 ГБ;
- объем диска: 8 ГБ.

Известные проблемы и ограничения

- Виртуальному устройству (агенту для VMmanager) доступны виртуальные машины и ресурсы только того узла, на котором оно расположено.

Автоматическая установка агента для VMmanager

Установка агента для VMmanager включает в себя следующие шаги:

1. установка сервера управления Кибер Бэкап;
2. установка виртуального устройства VMmanager и его подключение к серверу управления Кибер Бэкап и платформе виртуализации VMmanager.

Установка сервера управления Кибер Бэкап

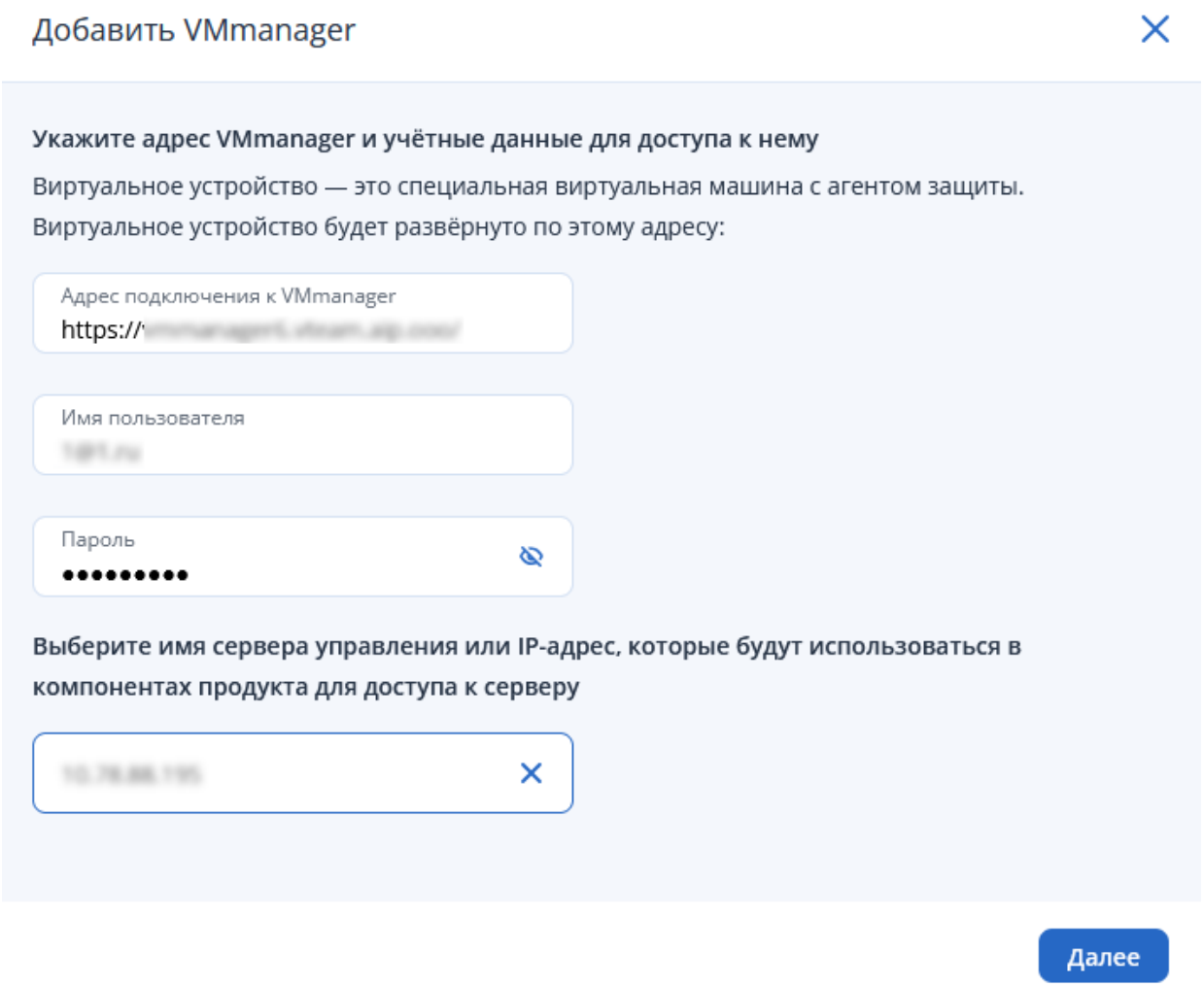
Для установки сервера управления Кибер Бэкап обратитесь к разделу *Установка сервера управления*.

Установка виртуального устройства VMmanager и его подключение к серверу управления Кибер Бэкап и платформе виртуализации VMmanager

Для установки виртуального устройства и его подключения выполните следующие действия:

1. Перейдите в раздел **Устройства** и нажмите **Добавить**. Появится окно **Добавить устройства**.
2. В разделе **Платформы виртуализации** щелкните **VMmanager**. Откроется окно **Добавить VMmanager**.
3. Укажите URL-адрес и учетные данные пользователя для подключения к VMmanager. В VMmanager пользователю должна быть назначена роль **Администратор**.

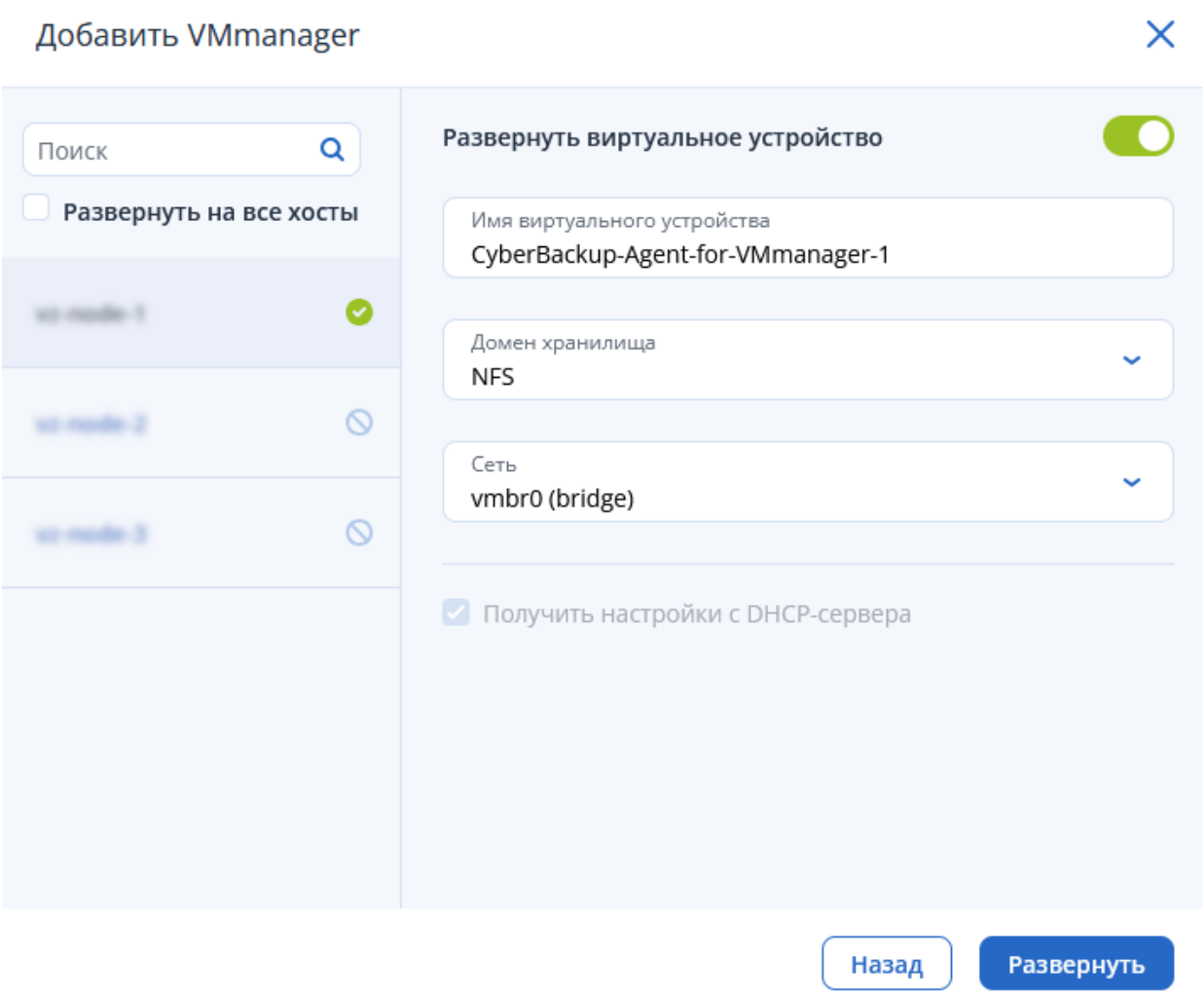
   При необходимости выберите, какое DNS-имя или какой IP-адрес сервера управления Кибер Бэкап будет указан в настройках виртуального устройства.



Нажмите **Далее** и дождитесь окончания операции создания агента и его подключения к Кибер Бэкап и VMmanager.

Если операция завершилась с ошибкой, проверьте сетевые настройки, соединение с сервером управления и настройки подключения к VMmanager.

4. Выберите узлы, на которых будут развернуты виртуальные устройства. Для каждого виртуального устройства задайте имя, домен хранилища и настройки сети.



Нажмите **Развернуть** и дождитесь окончания операции.

5. Перейдите в раздел **Устройства** → **VMmanager** и убедитесь, что после получения сведений из VMmanager в нем отображаются требуемые кластеры, узлы и виртуальные машины.
6. Перейдите в раздел **Настройки** → **Агенты** и убедитесь, что в списке агентов появились требуемые агенты для резервного копирования.

Примечание

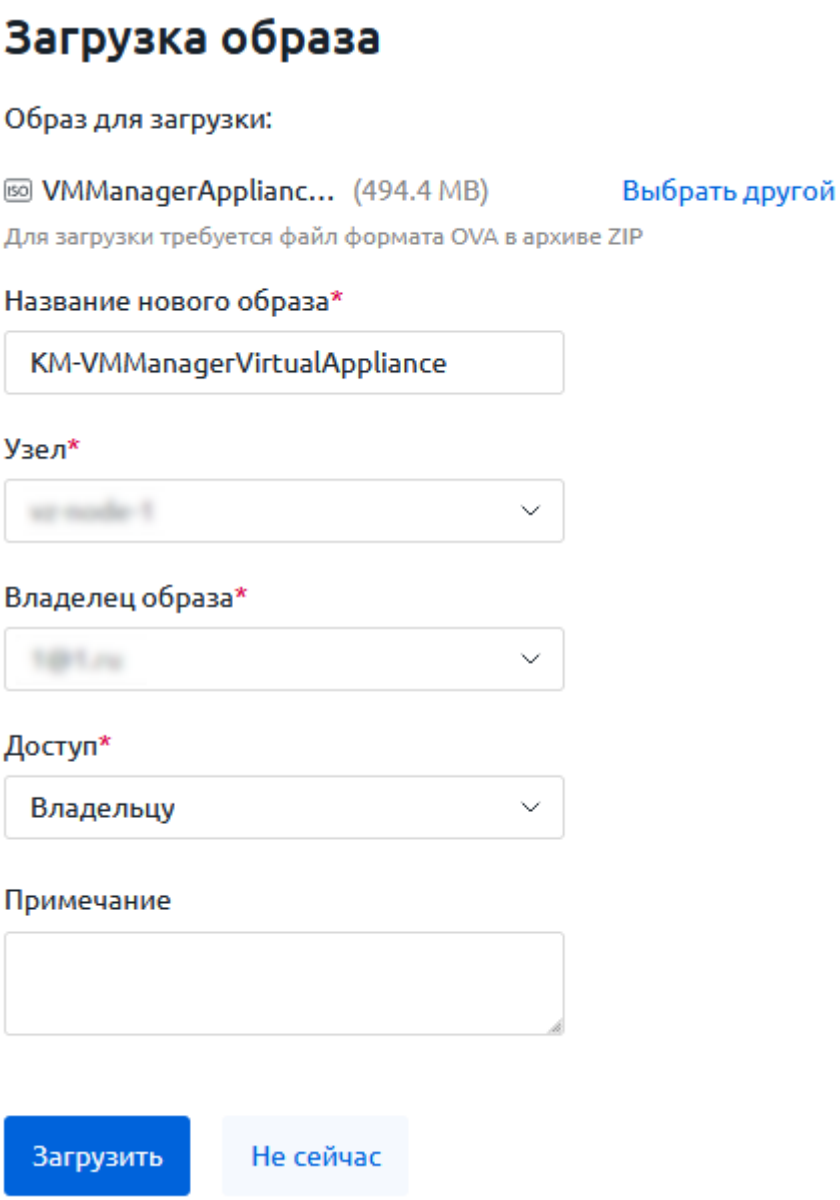
Убедитесь, что на каждом виртуальном устройстве установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить виртуальное устройство.

Установка агента для VMmanager вручную

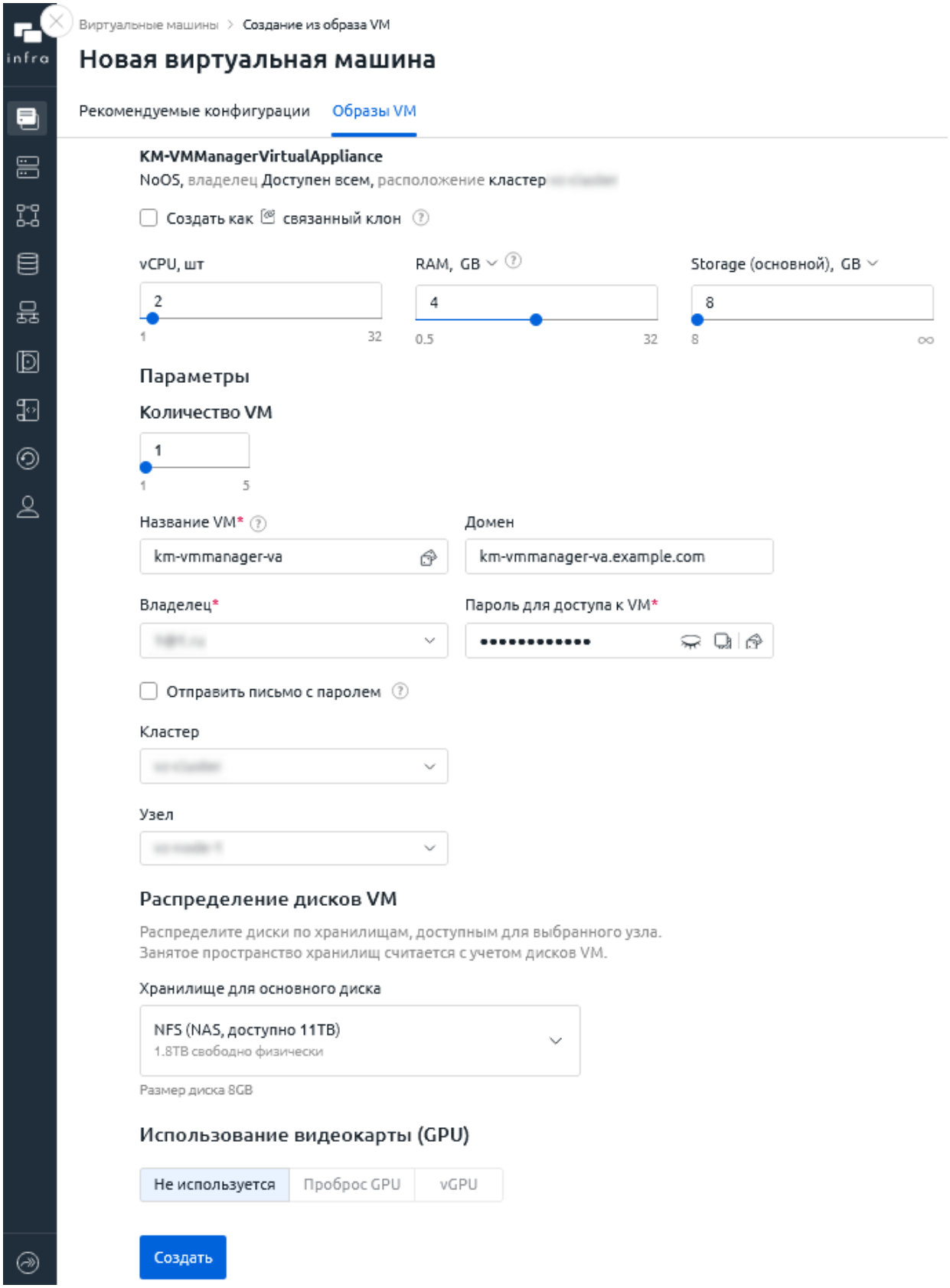
Для установки вручную агента для VMmanager выполните следующие действия:

1. Скачайте пакет установки агента для VMmanager с сайта компании (файл формата ZIP; например, `VMManagerAppliance_v*.*.*.zip`).
2. Войдите в панель управления платформы виртуализации VMmanager, использовав учетные данные пользователя с ролью **Администратор**.
3. Перейдите в раздел **Шаблоны** → **Образы VM**, нажмите **Создать образ** и выберите пункт меню **Загрузить**.
4. В окне создания образа укажите путь к пакету установки агента для VMmanager, название образа, узел, на который будет загружен образ, и остальные необходимые параметры. Подробные сведения о загрузке образов см. в документации VMmanager.

   Нажмите **Загрузить** и дождитесь завершения процесса загрузки.



5. Перейдите в раздел **Виртуальные машины** → **Виртуальные машины**, нажмите **Создать VM** и переключитесь на вкладку **Образы VM**.
6. В списке образов щелкните по имени добавленного раннее образа.
7. В окне создания виртуальной машины укажите ее параметры. Убедитесь, что выделено необходимое количество ресурсов. Подробные сведения о создании виртуальных машин см. в документации VMmanager.

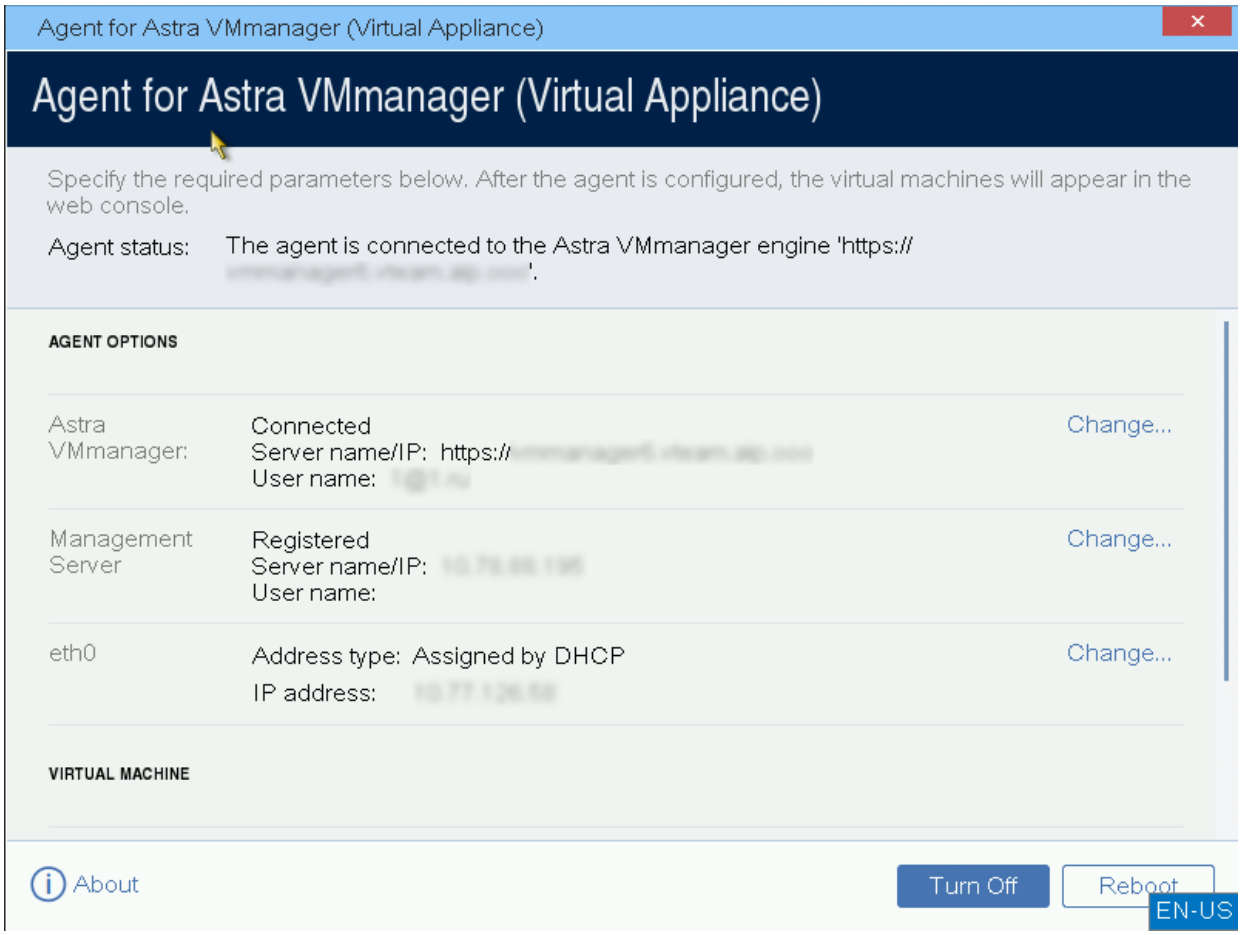


Нажмите **Создать** и дождитесь завершения процесса создания.

8. Отключите функцию ”Антиспуфинг” у созданной виртуальной машины:

1. В списке виртуальных машин щелкните по имени машины и нажмите **Параметры**.
2. Перейдите в раздел **Тонкие настройки** и в блоке **Антиспуфинг** снимите соответствующий флажок.
3. Нажмите **Применить и перезагрузить** и дождитесь завершения перезагрузки.

9. Подключитесь к консоли виртуальной машины и настройте агент для VMmanager:
   1. В разделе **Astra VMmanager** нажмите **Change** и укажите URL-адрес платформы виртуализации и учетные данные пользователя для подключения к ней. В VMmanager пользователю должна быть назначена роль **Администратор**.
   2. В разделе **Management Server** нажмите **Change** и укажите URL-адрес сервера управления Кибер Бэкап и учетные данные пользователя для подключения к нему.



10. Перейдите в раздел **Устройства** → **VMmanager** и убедитесь, что после получения сведений из VMmanager в нем отображаются требуемые кластеры, узлы и виртуальные машины.
11. Перейдите в раздел **Настройки** → **Агенты** и убедитесь, что в списке агентов появился требуемый агент для резервного копирования.

Примечание

Убедитесь, что на виртуальном устройстве установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить виртуальное устройство.

Автоматическая установка или автоматическое удаление

Автоматическая установка или автоматическое удаление в Windows

В этом разделе показано, как установить или удалить Кибер Бэкап в автоматическом режиме на машине с Windows, используя установщик Windows (программа `msiexec`). В домене Active Directory можно также выполнять автоматическую установку с помощью групповой политики: см. раздел *Развертывание агентов с использованием групповой политики*.

При установке можно использовать файл, называемый **преобразованием** (MST-файл). Преобразование — это файл с параметрами установки. В качестве альтернативного варианта можно указать параметры прямо в командной строке.

Предварительные требования

В этом режиме установки требуется распространяемый компонент Microsoft Visual C++ 2022 версии не ниже 14.42.34438. Проверьте наличие этого компонента на машине или установите его перед выполнением установки Кибер Бэкап. После установки пакета может потребоваться перезагрузка. Распространяемый пакет Microsoft Visual C++ можно скачать по ссылке https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Создание MST-преобразования и извлечение пакетов установки

1. Войдите как администратор и запустите программу установки.
2. Щёлкните **Создать MST- и MSI-файлы для автоматической установки**.
3. В разделе **Устанавливаемые компоненты** выберите компоненты, которые требуется установить. Пакеты установки для этих компонентов будут извлечены из программы установки.
4. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл.
5. Нажмите кнопку **Создать**.

В результате создается MST-файл, а установочные MSI-пакеты и CAB-пакеты извлекаются в указанную папку.

Установка или удаление продукта с использованием преобразования MST

Чтобы установить продукт, выполните следующую команду:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Чтобы удалить продукт, выполните следующую команду:

```
msiexec /x <package name> TRANSFORMS=<transform name>
```

В этих командах:

- `<имя пакета>` — это имя MSI-файла. Этот файл имеет имя **AB_AIP64.msi**.
- `<имя преобразования>` — это имя преобразования. Этот файл имеет имя **AB_AIP64.msi.mst**.

Примеры:

- Установка продукта с использованием преобразования MST.

  ```
  msiexec /i AB_AIP64.msi TRANSFORMS=AB_AIP64.msi.mst
  ```

- Удаление продукта с использованием преобразования MST.

  ```
  msiexec /x AB_AIP64.msi TRANSFORMS=AB_AIP64.msi.mst
  ```

Установка или удаление продукта с указанием параметров вручную

Выполните следующую команду:

```
msiexec /i <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

`<имя пакета>` — это имя MSI-файла. Этот файл имеет имя **AB_AIP64.msi**.

Доступные параметры и их значения описаны в разделе *Параметры автоматической установки или автоматического удаления*.

Примеры:

- Установка сервера управления и компонентов для удаленной установки.

  ```
  msiexec.exe /i AB_AIP64.msi /l*v my_log.txt /qn ADDLOCAL=AcronisCentralizedManagementServer,
  ↪WebConsole,ComponentRegisterFeature TARGETDIR="C:\Program Files\Acronis"¬
  ↪REBOOT=ReallySuppress CURRENT_LANGUAGE=en CMS_USE_SYSTEM_ACCOUNT=1
  ```

- Установка агента для Windows, программы командной строки и программы Мониторинг Защиты

Данных. Регистрация машины с агентом на ранее установленном сервере управления.

```
msiexec.exe /i AB_AIP64.msi /l*v my_log.txt /qn ADDLOCAL=AgentsCoreComponents,
↪BackupAndRecoveryAgent,CommandLineTool,TrayMonitor TARGETDIR="C:\Program Files\Acronis"¬
↪REBOOT=ReallySuppress CURRENT_LANGUAGE=en MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.
↪10.1.1
```

- Удаление всех компонентов продукта и их настроек.

```
msiexec.exe /i AB_AIP64.msi /l*v my_log.txt /qn TARGETDIR="C:\Program Files\Acronis"¬
↪REMOVE=ALL DELETE_ALL_SETTINGS=1
```

Параметры автоматической установки или автоматического удаления

В этом разделе описаны параметры, которые используются при автоматической установке или автоматическом удалении в Windows.

Кроме этих параметров можно использовать другие параметры `msiexec`, как описано по ссылке.

Параметры установки

Стандартные параметры

`ADDLOCAL=<список компонентов>`

Компоненты для установки, разделенные запятыми без символов пробела. Все указанные компоненты необходимо извлечь из программы установки до установки.

Полный список компонентов указан ниже. Все компоненты являются 64-разрядными.

Компонент	Необходимо установить вместе с	Имя / описание компонента
AcronisCentralizedManagementServer	WebConsole	Сервер управления
WebConsole	AcronisCentralizedManagementServer	Веб-консоль
ComponentRegisterFeature	AcronisCentralizedManagementServer	Компоненты для удаленной установки
AgentsCoreComponents		Компоненты Core для агентов
BackupAndRecoveryAgent	AgentsCoreComponents	Агент для Windows
ArxAgentFeature	BackupAndRecoveryAgent	Агент для Exchange
ArsAgentFeature	BackupAndRecoveryAgent	Агент для SQL

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Компонент	Необходимо установить вместе с	Имя / описание компонента
ARADAgentFeature	BackupAndRecoveryAgent	Агент для Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	Агент для Oracle
AcronisESXSupport	AgentsCoreComponents	Агент для VMware (Windows)
HyperVAgent	AgentsCoreComponents	Агент для Hyper-V
ESXVirtualAppliance		Агент для VMware (виртуальное устройство)
CommandLineTool		Программа командной строки
TrayMonitor	BackupAndRecoveryAgent	Мониторинг Защиты Данных
BackupAndRecovery-BootableComponents		Мастер создания загрузочных носителей
PXEServer		PXE-сервер
StorageServer	BackupAndRecoveryAgent	Узел хранения
CommunigateAgentFeature	BackupAndRecoveryAgent	Агент для CommuniGate Pro
PostgreSqlAgentFeature	BackupAndRecoveryAgent	Агент для PostgreSQL
WorkmailAgentFeature	BackupAndRecoveryAgent	Агент для VK WorkMail

`TARGETDIR=<путь>`

Папка, в которую будет установлен продукт.

`REBOOT=ReallySuppress`

Если данный параметр указан, перезапуск машины запрещен.

`CURRENT_LANGUAGE=<ИД языка>`

Язык продукта. Доступные значения: `ru`, `en`, `en_GB`.

`REGISTRATION_ADDRESS=<имя или IP-адрес хоста>:<порт>`

Имя хоста или IP-адрес машины, на которой установлен сервер управления. Агенты и узел хранения, указанные в параметре `ADDLOCAL`, будут зарегистрированы на этом сервере управления. Порт должен быть обязательно указан, если он отличается от установленного по умолчанию (9877).

Необходимо указать параметр REGISTRATION_TOKEN или параметры REGISTRATION_LOGIN и REGISTRATION_PASSWORD.

REGISTRATION_TOKEN=<маркер>

Маркер регистрации, сгенерированный в веб-консоли Кибер Бэкап, как описано в разделе *Развертывание агентов с использованием групповой политики*.

REGISTRATION_LOGIN=<имя пользователя> и REGISTRATION_PASSWORD=<пароль>

Имя пользователя и пароль администратора сервера управления.

REGISTRATION_TENANT=<идентификатор отдела>

Отдел в организации. Агенты и узел хранения, указанные в параметре ADDLOCAL, будут добавлены в этот отдел.

Чтобы узнать идентификатор отдела, в веб-консоли Кибер Бэкап щёлкните **Настройки** → **Учетные записи**, выберите нужный отдел и щёлкните **Подробнее**.

Этот параметр не работает без параметра REGISTRATION_TOKEN или параметров REGISTRATION_LOGIN и REGISTRATION_PASSWORD. В этом случае компоненты будут добавлены в организацию.

Если данный параметр не указан, компоненты будут добавлены в организацию.

REGISTRATION_REQUIRED={0,1}

Результат установки при сбое регистрации. Если значение равно 1, установка завершится сбоем. Если значение равно 0, установка завершается успешно, даже если компонент не зарегистрирован.

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<значение открытого ключа>

Эти взаимоисключающие параметры определяют метод проверки сертификата сервера управления при регистрации. Проверьте сертификат, и таким образом вы проверите подлинность сервера управления для предотвращения атак MITM.

Если значение равно 1, для проверки подлинности используется системный центр сертификации или пакет центра сертификации, который прилагается к продукту. Если указан закрепленный открытый ключ, он используется для проверки подлинности. Если значение равно 0 или параметры не указаны, проверка сертификатов не выполняется, но трафик регистрации остается зашифрованным.

/l*v <файл журнала>

Если данный параметр указан, журнал установки в режиме подробного протоколирования сохраняется в указанный файл. Файл журнала можно использовать для анализа проблем с установкой.

Параметры установки сервера управления

WEB_SERVER_PORT=<номер порта>

Порт, который будет использоваться в веб-браузере для доступа к серверу управления. По умолчанию это порт 9877.

ZMQ_PORT=<номер порта>

Порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию это порт 7780.

SQL_INSTANCE=<экземпляр>

База данных, которая должна использоваться сервером управления. Можно выбрать любую версию Microsoft SQL Server 2012, Microsoft SQL Server 2014 или Microsoft SQL Server 2016. Выбранный экземпляр может использоваться и другими программами.

Без этого параметра будет использоваться встроенная база данных SQLite.

SQL_USER_NAME=<имя пользователя> и SQL_PASSWORD=<пароль>

Учетные данные учетной записи для входа на Microsoft SQL Server. Сервер управления использует эти учетные данные для подключения к выбранному экземпляру SQL Server. Если эти параметры не выбраны, сервер управления будет использовать учетные данные учетной записи службы сервера управления (**CMS User**).

Учетная запись, под которой запущена служба сервера управления

Укажите один из следующих параметров:

CMS_USE_SYSTEM_ACCOUNT={0,1}

Если задано значение `1`, будет использоваться системная учетная запись.

`CMS_CREATE_NEW_ACCOUNT={0,1}` Если задано значение `1`, будет создана новая учетная запись.

`CMS_SERVICE_USERNAME=<имя пользователя>` и `CMS_SERVICE_PASSWORD=<пароль>` Будет использоваться указанная учетная запись.

Параметры установки агента

HTTP_PROXY_ADDRESS=<IP-адрес> и HTTP_PROXY_PORT=<порт>

Прокси-сервер HTTP, который будет использоваться агентом. Если эти параметры не заданы, не будет использовано ни одного прокси-сервера.

HTTP_PROXY_LOGIN=<имя входа> и HTTP_PROXY_PASSWORD=<пароль>

Учетные данные для прокси-сервера HTTP. Используйте эти параметры, если сервер требует проверки подлинности.

HTTP_PROXY_ONLINE_BACKUP={0,1}, SET_ESX_SERVER={0,1}

Если задано значение `0`, устанавливаемый агент для VMware не будет подключаться к vCenter Server или хосту ESXi. После установки продолжайте действия, как указано в разделе *Настройка уже зарегистрированного агента для VMware*.

Если задано значение `1`, укажите следующие параметры:

ESX_HOST=<имя хоста или IP-адрес>

Имя хоста или IP-адрес vCenter Server или хоста ESXi.

ESX_USER=<имя пользователя> И ESX_PASSWORD=<пароль>

Учетные данные для доступа к vCenter Server или хосту ESXi.

Учетная запись, с которой будет запускаться служба агента

Укажите один из следующих параметров:

MMS_USE_SYSTEM_ACCOUNT={0,1}

Если задано значение `1`, будет использоваться системная учетная запись.

MMS_CREATE_NEW_ACCOUNT={0,1}

Если задано значение `1`, будет создана новая учетная запись.

MMS_SERVICE_USERNAME=<имя пользователя> И MMS_SERVICE_PASSWORD=<пароль>

Будет использоваться указанная учетная запись.

Параметры установки узла хранения

Учетная запись, с которой будет запускаться служба узла агента

Укажите один из следующих параметров:

CSN_USE_SYSTEM_ACCOUNT={0,1}

Если задано значение `1`, будет использоваться системная учетная запись.

CSN_CREATE_NEW_ACCOUNT={0,1}

Если задано значение `1`, будет создана новая учетная запись.

CSN_SERVICE_USERNAME=<имя пользователя> И CSN_SERVICE_PASSWORD=<пароль>

Будет использоваться указанная учетная запись.

Параметры удаления

REMOVE={<список компонентов>|ALL}

Компоненты для удаления, разделенные запятыми без символов пробела.

Доступные компоненты описаны ранее в этом разделе.

Если задано значение `ALL`, все компоненты продукта будут удалены. Кроме того, можно указать следующий параметр:

DELETE_ALL_SETTINGS={0,1}

Если задано значение `1`, журналы продукта, задачи и настройки конфигурации будут удалены.

Автоматическая установка или автоматическое удаление в Linux

В этом разделе описан порядок установки или удаления Кибер Бэкап в автоматическом режиме на машинах под управлением Linux с использованием командной строки.

Порядок установки или удаления продукта

1. Откройте приложение терминала.
2. Выполните следующую команду:

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   Здесь `<имя пакета>` — это имя пакета установки (файла .i686 или .x86_64).
3. [Только при установке агента для Linux] Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните пароль, который следует использовать (пароль привилегированного пользователя). Во время перезапуска системы выберите управление ключом владельца машины (MOK), выберите **Зарегистрировать MOK** и зарегистрируйте ключ, используя рекомендуемый пароль.

Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 3. В противном случае последующие операции резервного копирования завершатся сбоем.

Параметры установки

Стандартные параметры

`{-a|--auto}`

Установить или удалить компоненты продукта без участия пользователя. Чтобы использовать этот параметр при установке агента, необходимо также указать учетную запись, под которой агент будет

зарегистрирован в службе Cyber Protect. Для этого можно использовать параметр `--token` или параметры `--login` и `--password`.

`{-i |--id=}<список компонентов>`

Компоненты для установки, разделенные запятыми без символов пробела.

Для установки доступны указанные ниже компоненты:

Компонент	**Необходимо установить вместе с**	**Описание компонента**
AcronisCentralizedManagementServer		Сервер управления
BackupAndRecoveryAgent		Агент для Linux
BackupAndRecoveryBootableComponents;		Мастер создания загрузочных носителей
CommunigateAgentFeature	BackupAndRecoveryAgent	Агент для CommuniGate Pro
K8sAgentFeature	BackupAndRecoveryAgent	Агент для Kubernetes
PostgreSqlAgentFeature	BackupAndRecoveryAgent	Агент для PostgreSQL
WorkmailAgentFeature	BackupAndRecoveryAgent	Агент для VK WorkMail

Если данный параметр не указан, устанавливаются все перечисленные выше компоненты.

`--language=<ИД языка>`

Язык продукта. Доступные значения: `ru`, `en`, `en_GB`, `de`.

`{-d|--debug}`

Если данный параметр указан, журнал установки записывается в режиме подробного протоколирования. Журнал расположен в файле `/var/log/trueimage-setup.log`.

`{-t|--strict}`

Если данный параметр указан, любое предупреждение при установке приведет к сбою установки. Если данный параметр не указан, установка успешно выполняется, даже при наличии предупреждений.

`{-n|--nodeps}`

Если параметр указан, отсутствие требуемых пакетов Linux не будет принято во внимание при установке.

Параметры установки сервера управления

{-W |--web-server-port=}<номер порта>

Порт, который будет использоваться в веб-браузере для доступа к серверу управления. По умолчанию это порт 9877.

--ams-tcp-port=<номер порта>

Порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию это порт 7780.

{-P | --force-postgres}

Если параметр указан, то для установки будет использована СУБД PostgreSQL вместо встроенной СУБД SQLite. Перед установкой сервера управления PostgreSQL необходимо подготовить, как описано в разделе *Установка в Linux*.

Используйте следующие параметры, чтобы указать сведения для подключения к PostgreSQL:

--postgres-user=<имя пользователя>

Имя пользователя для подключения к PostgreSQL. Необходимо указать имя пользователя, который был создан при подготовке PostgreSQL.

--postgres-password=<пароль пользователя>

Пароль пользователя для подключения к PostgreSQL. Необходимо указать пароль пользователя, который был создан при подготовке PostgreSQL.

--postgres-host=<IP-адрес или DNS-имя>

IP-адрес или DNS-имя машины с PostgreSQL.

--postgres-port=<номер порта>

Порт для подключения к PostgreSQL.

Параметры установки агента

Укажите один из следующих параметров:

--skip-registration

Не регистрировать агент на сервере управления.

{-C |--ams=}<имя хоста или IP-адрес>

Имя хоста или IP-адрес машины, на которой установлен сервер управления. Агент будет зарегистрирован на этом сервере управления.

Если установить агент и сервер управления одной командой, агент будет зарегистрирован на этом сервере управления независимо от значения параметра `-C`.

Необходимо указать параметр `token` parameter или параметры `login` и `password`.

--token=<маркер>

Маркер регистрации, сгенерированный в веб-консоли Кибер Бэкап, как описано в разделе *Развертывание агентов с использованием групповой политики*.

{-g |--login=}<имя пользователя> и {-w |--password=}<пароль>

Учетные данные администратора сервера управления.

--unit=<идентификатор отдела>

Отдел в организации. Агент будет добавлен в этот отдел.

Чтобы узнать идентификатор отдела, в веб-консоли Кибер Бэкап щёлкните **Настройки** → **Учетные записи**, выберите нужный отдел и щёлкните **Подробнее**.

Если данный параметр не указан, агент будет добавлен в организацию.

--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}

Метод проверки сертификата сервера управления при регистрации. Проверьте сертификат, и таким образом вы проверите подлинность сервера управления для предотвращения атак MITM.

Если задано значение `https`, или параметр не указан, проверка сертификата не выполняется, но трафик регистрации остается зашифрованным. Если задано значение, *отличное от*`https`, для проверки подлинности используется системный центр сертификации или пакет центра сертификации, который прилагается к продукту или закрепленному открытому ключу соответственно.

--reg-transport-pinned-public-key=<значение открытого ключа>

Значение закрепленного открытого ключа. Этот параметр должен быть указан вместе с параметром `--reg-transport=https-pinned-public-key` или вместо него.

--http-proxy-host=<IP-адрес> и --http-proxy-port=<порт>, --http-proxy-login=<имя входа> и --http-proxy-password=<пароль>

Учетные данные для прокси-сервера HTTP. Используйте эти параметры, если сервер требует проверки подлинности.

--no-proxy-to-ams

Агент защиты подключится к серверу управления без использования прокси-сервера, который указан параметрами `--http-proxy-host` и `--http-proxy-port`.

Параметры удаления

{-u|--uninstall}

Удаляет продукт.

--purge

Удаляет журналы продукта, задачи и настройки конфигурации.

Параметры информации

{-?|--help}

Показано описание параметров.

--usage

Показывает краткое описание использования команды.

{-v|--version}

Показывает версию пакета установки.

--product-info

Показывает имя продукта и версию пакета установки.

--components-list

Показывает список компонент продукта, включенных в пакет установки.

--snapapi-list

Показывает список версий модуля Snap API, включенных в пакет установки. Данный модуль обеспечивает создание моментальных снимков тома.

Примеры

- Установка сервера управления.

```
./CyberBackup_17_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Установка сервера управления, указание нестандартных портов.

```
./CyberBackup_17_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --web-server-port
↪6543 --ams-tcp-port 8123
```

- Установка сервера управления с использованием СУБД PostgreSQL.

```
./CyberBackup_17_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --force-postgres --
↪postgres-user=cyberbackup --postgres-password=69c64fee29d24024b219578ecd9f5d88 --postgres-
↪host=127.0.0.1 --postgres-port=5432
```

- Установка агента для Linux и его регистрация на указанном сервере управления.

```
./CyberBackup_17_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 --login root --
↪password 123456
```

- Установка агента для Linux и его регистрация на указанном сервере управления в указанном отделе.

```
./CyberBackup_17_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 --login root --
↪password 123456 –unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

- Удаление Кибер Бэкап.

```
./CyberBackup_17_64-bit.x86_64 -a -u
```

Развертывание агентов с использованием групповой политики

Агент для Windows можно централизованно устанавливать (или развертывать) на машинах в составе домена Active Directory с помощью групповой политики.

В этом разделе описывается настройка объекта групповой политики для развертывания агентов на машинах во всем домене или в его организационной единице.

Каждый раз при входе машины в домен результирующий объект групповой политики проверяет, установлен и зарегистрирован ли на ней агент.

Предварительные требования

Перед развертыванием агента убедитесь в том, что выполнены перечисленные ниже условия.

- Имеется домен Active Directory, контроллер которого работает под управлением Microsoft Windows Server.
- Вы входите в состав группы **Администраторы домена**.
- Вы загрузили программу установки **Все агенты для установки в Windows**. Ссылка для скачивания доступна на странице **Добавить устройства** в веб-консоли Кибер Бэкап.
- Выполнены предварительные условия для автоматической установки агента в среде Windows (см. *Автоматическая установка или автоматическое удаление в Windows*).

Шаг 1. Формирование маркера регистрации

Маркер регистрации передает ваше удостоверение в программу установки, не сохраняя имя входа и пароль для веб-консоли Кибер Бэкап. Это позволяет зарегистрировать любое количество машин в учетной записи. Чтобы обеспечить более высокий уровень безопасности, маркер имеет ограниченный срок действия.

Формирование маркера регистрации

1. Войдите в веб-консоль Кибер Бэкап с учетными данными той учетной записи, для которой необходимо назначить машины.
2. Щёлкните **Физические и виртуальные машины** → **Добавить**.
3. Прокрутите вниз до поля **Маркер регистрации** и нажмите кнопку **Создать**.
4. Укажите срок действия маркера и нажмите кнопку **Создать маркер**.
5. Скопируйте маркер или запишите его. Сохраните маркер, если он понадобится в будущем.

   Для просмотра уже сформированных маркеров и управления ими можно щёлкнуть **Управление активными маркерами**. Имейте в виду, что из соображений безопасности в этой таблице не отображаются полные значения маркеров.

Шаг 2. Создание MST-преобразования и извлечение пакета установки

1. Войдите как администратор на любую машину в домене.
2. Создайте общую папку, в которой будут находиться пакеты установки. Убедитесь, что у пользователей домена есть доступ к этой папке (для этого можно, например, оставить значение параметра общего доступа по умолчанию для категории **Все**).
3. Запустите программу установки.
4. Щёлкните **Создать MST- и MSI-файлы для автоматической установки**.
5. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл. Указывая способ подключения к серверу управления, выберите **Используйте маркер регистрации** и введите сгенерированный маркер.
6. Щёлкните **Продолжить**.
7. В поле **Сохранить файлы в** укажите путь к созданной папке.
8. Нажмите кнопку **Создать**.

В результате будет сформировано MST-преобразование, а установочные MSI-пакеты и CAB-пакеты будут извлечены в созданную вами папку.

Шаг 3. Настройка объектов групповой политики

1. Войдите на контроллер домена с правами администратора домена. Если в домене больше одного контроллера, это можно сделать на любом из них.
2. Если вы планируете развернуть агент в рамках организационной единицы, она должна быть

создана до начала установки. В противном случае пропустите этот шаг.

3. В меню **Пуск** выберите пункт **Администрирование**, а затем щёлкните **Управление групповой политикой**.
4. Правой кнопкой мыши щёлкните имя домена или организационной единицы, а затем щёлкните **Создать объект GPO в этом домене и связать его**.
5. Назовите новый объект групповой политики **Агент для Windows**.
6. Откройте объект групповой политики **Агент для Windows** для изменения. Чтобы сделать это, в разделе **Объекты групповой политики** щёлкните правой кнопкой мыши объект групповой политики, а затем щёлкните **Изменить**.
7. В оснастке ”Редактор объектов групповой политики” разверните узел **Конфигурация компьютера**.
8. Разверните узел **Политики** → **Конфигурация программ**.
9. Щёлкните правой кнопкой мыши узел **Установка программ**, выберите пункт **Создать**, затем щёлкните **Пакет**.
10. Выберите MSI-пакет установки агента в созданной ранее общей папке и нажмите кнопку **Открыть**.
11. В диалоговом окне **Развертывание программ** выберите **особый**, затем нажмите кнопку **ОК**.
12. На вкладке **Изменения** нажмите кнопку **Добавить** и выберите созданное ранее MST-преобразование.
13. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Развертывание программ**.

Регистрация агента вручную

Помимо регистрации машины на сервере управления Кибер Бэкап при установке агента, можно также зарегистрировать ее в интерфейсе командной строки. Это может понадобиться, например, когда агент установлен, но при этом не удалось выполнить автоматическую регистрацию, или необходимо зарегистрировать существующую машину под новой учетной записью.

Перед регистрацией в Windows убедитесь, что были выполнены предварительные условия для автоматической установки (см. *Автоматическая установка или автоматическое удаление в Windows*).

Порядок регистрации агента

В командной строке машины, на которой установлен агент, выполните одну из следующих команд:

- Регистрация агента по учетной записи администратора

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> -u <имя_
↪пользователя> -p <пароль>
```

<имя_пользователя> и <пароль> — учетные данные учетной записи администратора, для которой будет зарегистрирован агент.

- Регистрация агента в отделе по идентификатору отдела

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> -u <имя_
↪пользователя> -p <пароль> --tenant <идентификатор_отдела>
```

Чтобы узнать идентификатор отдела, в веб-консоли Кибер Бэкап щёлкните **Настройки** → **Учетные записи**, выберите нужный отдел и щёлкните **Сведения**.

Администраторы могут регистрировать агентов только на своём уровне в иерархии организации. Администраторы отдела могут регистрировать агентов в собственных отделах и их подотделах. Администраторы организации могут регистрировать агентов во всех отделах. Дополнительную информацию о разных учетных записях администратора см. в разделе *Управление учетными записями пользователей и отделами организации*.

- Регистрация агента по маркеру регистрации

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> --token
↪<маркер_регистрации>
```

Маркер регистрации — это последовательность из 12 символов, разделенных дефисами на три части. Дополнительную информацию о создании маркера регистрации см. в разделе *Развертывание агентов с использованием групповой политики*.

Отмена регистрации агента

В командной строке машины, на которой установлен агент, выполните следующую команду:

```
<путь_к_программе_регистрации> -o unregister
```

Примеры

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a https://10.250.144.
↪179:9877 -u johndoe -p johnspasswd
```

```
”%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe” -o register -a https://10.250.144.
↪179:9877 -u johndoe -p johnspasswd --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
”%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe” -o register -a https://10.250.144.
↪179:9877 --token 3B4C-E967-4FBD
```

```
”%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe” -o unregister
```

Linux

```
sudo ”/usr/lib/Acronis/RegisterAgentTool/RegisterAgent” -o register -a https://10.250.144.
↪179:9877 -u johndoe -p johnspasswd
```

```
sudo ”/usr/lib/Acronis/RegisterAgentTool/RegisterAgent” -o register -a https://10.250.144.
↪179:9877 -u johndoe -p johnspasswd --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo ”/usr/lib/Acronis/RegisterAgentTool/RegisterAgent” -o register -a https://10.250.144.
↪179:9877 --token 34F6-8C39-4A5C
```

```
sudo ”/usr/lib/Acronis/RegisterAgentTool/RegisterAgent” -o unregister
```

Ввод паролей со специальными символами или пробелами

Если пароль содержит специальные символы или пробелы, заключите его в кавычки при вводе в командной строке.

```
<путь_к_программе_регистрации> -o register -a <адрес_сервера_управления:порт> -u <имя_
↪пользователя> -p ”<пароль>”
```

Пример для Windows:

```
”%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe” -o register -a https://10.250.
↪144.179:9877 -u johndoe -p ”johns passwd”
```

В случае ошибок:

1. Зашифруйте пароль в формате Base64.
2. В командной строке укажите зашифрованный пароль, добавив параметр `-b` или `--base64`.

Пример для Windows:

```
”%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe” -o register -a https://10.250.
↪144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Установка и настройка узла хранения

Узел хранения — это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается путем организации и управления хранилищами, выделенными для корпоративных резервных копий (см. *Добавление управляемого хранилища*).

Один из сценариев использования узла хранения — обеспечить централизованный доступ к ленточным накопителям или библиотекам, например, для резервного копирования и восстановления данных с нескольких устройств на один и тот же ленточный накопитель или библиотеку (управляемое хранилище на ленте).

Другим вариантом использования является включение расширенных возможностей дедупликации, когда данные на нескольких устройствах могут быть сопоставлены друг с другом (дедуплицированы) и храниться в едином расположении (управляемом хранилище с включенной дедупликацией).

Примечание

Для всех резервных копий в формате TIBX по умолчанию включена дедупликация в архиве (подробнее см. раздел *Дедупликация в архиве*).

Установка узла хранения

Перед установкой узла хранения убедитесь, что машина соответствует *системным требованиям*.

Порядок установки узла хранения в ОС Linux

Подготовка

1. В системе, в которой не используется диспетчер пакетов RPM, необходимо установить этот диспетчер вручную. Как привилегированный пользователь выполните команду (например):

   ```
   apt-get install rpm
   ```

2. Убедитесь в том, что на машине установлены *необходимые пакеты для ОС Linux*.

3. Дайте разрешение на исполнение установочному файлу. Выполните следующую команду:

```
chmod +x CyberBackup_*
```

Подготовка к установке в ОС Astra Linux SE

Перед установкой продукта в ОС Astra Linux SE ознакомьтесь с разделом *Совместимость с ОС Astra Linux SE* и выполните следующие шаги. Предполагается, что включен режим замкнутой программной среды.

1. Распакуйте дистрибутив:

   ```
   tar --xattrs --xattrs-include=* -xvf CyberBackup_18_64-bit.x86_64.tar
   ```

2. Запустите файл установки с правами привилегированного пользователя:

   ```
   ./CyberBackup_18_64-bit.x86_64
   ```

3. Обновите образы initramfs:

   ```
   update-initramfs -u -k all
   ```

4. Перезагрузите систему.

Установка

1. Запустите файл установки (файл .i686 или .x86_64) как привилегированный пользователь:

   ```
   ./CyberBackup_18_64-bit.x86_64
   ```

2. Примите условия лицензионного соглашения.

3. Укажите устанавливаемые компоненты:

   1. Снимите флажок **Сервер управления**.
   2. Установите флажок **Узел хранения**. Флажок **Агент для Linux** будет установлен автоматически.
   3. Нажмите **Далее**.

4. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:

   1. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   2. Укажите учетные данные администратора сервера управления или маркер регистрации.

      Дополнительную информацию о создании маркера регистрации см. в разделе *Развертывание агентов с использованием групповой политики*.

3. Нажмите **Далее**.

5. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов, затем нажмите клавишу `Ввод`.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе *Отделы и административные учетные записи*.

   > **Примечание**
   >
   > Если в процессе установки возникнет ошибка сборки модуля ядра ”Не удалось построить модуль ядра SnapAPI. Операции с резервными копиями на уровне дисков будут недоступны”, продолжите установку. После завершения установки решите проблему с помощью статьи базы знаний Сборка модуля SnapAPI для Linux.

6. Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните пароль, который следует использовать (пароль привилегированного пользователя).

   > **Примечание**
   >
   > В процессе установки создается новый ключ, который используется для подписи модулей ядра. Необходимо зарегистрировать этот ключ в списке владельцев ключей машины (Machine Owner Key, MOK), перезапустив машину. Если не зарегистрировать ключ, агент не будет работать. Если безопасная загрузка UEFI включена после установки агента, повторите установку, включая шаг 6.

7. После завершения установки выполните одно из следующих действий:

   - Нажмите кнопку **Перезапустить**, если на предыдущем шаге вам было предложено перезапустить систему.

     Во время перезапуска системы выберите управление ключом владельца машины (MOK), выберите **Зарегистрировать MOK** и зарегистрируйте ключ, используя пароль, предложенный на предыдущем шаге.

   - В противном случае нажмите **Выход**.

Сведения об устранении неполадок представлены в файле `/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL`.

Порядок установки узла хранения в ОС Windows

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Щёлкните **Настройка параметров установки**.
5. В разделе **Устанавливаемые компоненты** щёлкните **Изменить**.
6. Выберите устанавливаемые компоненты:
   - Для установки узла хранения установите флажок **Узел хранения**. Флажок **Агент для Windows** будет установлен автоматически.
   - Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки.

   Чтобы продолжить, нажмите кнопку **Готово**.
7. Укажите сервер управления, на котором будут зарегистрированы компоненты:
   1. Перейдите на **Сервер управления Кибер Бэкап** и щёлкните **Указать**.
   2. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   3. Укажите учетные данные администратора сервера управления или маркер регистрации.

      Дополнительную информацию о создании маркера регистрации см. в разделе *Развертывание агентов с использованием групповой политики*.
   4. Нажмите кнопку **Готово**.
8. При поступлении запроса выберите, добавлять ли машину с узлом хранения в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе *Отделы и административные учетные записи*.
9. [Необязательно] Измените другие настройки установки, как описано в разделе *Настройка параметров установки*.
10. Нажмите **Установить**, чтобы продолжить установку.
11. После завершения установки нажмите кнопку **Закрыть**.

Добавление управляемого хранилища

Управляемое хранилище может быть организовано:

- В локальной папке.
  - На жестком диске, локальном по отношению к узлу хранения.
  - На хранилище SAN, которое операционная система определяет как локально подключенное устройство.
- В сетевой папке.
  - В общей папке SMB/CIFS.
  - На хранилище SAN, которое операционная система определяет как сетевую папку.
  - На устройстве NAS.
- В ленточном устройстве, локально подключенном к узлу хранения.

  Хранилища на основе ленточных устройств создаются в виде *пулов лент*. Один пул лент присутствует по умолчанию. При необходимости можно создать другие пулы лент, как описано далее в этом разделе.

Репликация резервной копии с использованием управляемого хранилища имеет свои особенности (см. разделы *Репликация* и *Замечания по использованию узла хранения*).

Порядок создания управляемого хранилища в локальной или сетевой папке

1. Выполните одно из следующих действий:
   - Щёлкните **Хранилища резервных копий** → **Добавить расположение**, затем щёлкните **Узел хранения**.
   - При создании плана защиты щёлкните **Место сохранения резервной копии** → **Добавить хранилище**, затем щёлкните **Узел хранения**.
   - Щёлкните **Настройки** → **Узел хранения**, выберите узел хранения, который будет управлять расположением, затем щёлкните **Добавить хранилище**.
2. В поле **Имя** укажите уникальное имя для хранилища. ”Уникальный” означает, что не должно быть другого расположения с тем же именем, которое управляется тем же узлом хранения.
3. [Необязательно] Выберите узел хранения, который будет управлять этим хранилищем. Если вы выбрали последний параметр в шаге 1, вы не сможете изменять узел хранения.
4. Выберите имя узла хранения или IP-адрес, которые будут использоваться агентом для доступа к хранилищу.

По умолчанию выбрано имя узла хранения. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою доступа. Чтобы изменить эту настройку позже, щёлкните **Хранилища резервных копий** → **Хранилище** → **Изменить**, затем измените значение поля **Адрес**.

5. Введите путь к папке или выберите ее в проводнике.
6. Нажмите кнопку **Готово**. Программа проверит доступ к указанной папке.
7. [Необязательно] Включите дедупликацию резервных копий в хранилище.

   Дедупликация минимизирует трафик резервного копирования и уменьшает размеры резервных копий в хранилище, удаляя дублированные блоки на диске.

   Дополнительную информацию об ограничениях дедупликации см. в разделе *Ограничения дедупликации*.
8. [Только если включена дедупликация] Укажите или измените значение в поле **Путь к базе данных дедупликации**.

   Это должна быть папка на жестком диске, локальном по отношению к узлу хранения. Для повышения производительности системы рекомендуется создавать базу данных дедупликации и управляемое хранилище на разных дисках.

   Дополнительную информацию о базе данных дедупликации см. в разделе *Рекомендации по дедупликации*.
9. [Необязательно] Укажите, нужно ли защитить хранилище паролем. Все данные, которые записываются в это хранилище, будут защищены. При чтении пароль будет подставлен узлом хранения незаметно для пользователя.

   Подробнее см. в разделе *Защита хранилища паролем*.
10. Нажмите кнопку **Готово**, чтобы создать хранилище.

Для создания управляемого хранилища на ленточном устройстве

1. Щёлкните **Хранилища резервных копий** → **Добавить хранилище**, или при создании плана защиты щёлкните **Место сохранения резервной копии** → **Добавить хранилище**.
2. Выберите **Ленты**.
3. [Необязательно] Выберите узел хранения, который будет управлять этим хранилищем.
4. Выполните действия, описанные в разделе *Создание пула*, начиная с шага 4.

Примечание

По умолчанию агенты используют имя узла хранения для доступа к управляемому хранилищу на основе ленточных устройств. Чтобы агенты использовали IP-адрес узла хранения, щёлкните **Хранилища резервных копий** → **Хранилище** → **Изменить**, затем измените значение поля **Адрес**.

Рекомендация по переподключению хранилищ

Управляемые хранилища рекомендуется переподключать к узлам хранения с той же ОС, что и при отключении хранилищ. В противном случае переподключение может занять долгое время.

Защита хранилища паролем

Если для хранилища установлена защита паролем, то при подключении хранилища к другому узлу хранения потребуется ввести пароль. Если носитель хранилища украден или доступ к нему получил неавторизованный пользователь, злоумышленник не сможет получить доступ к содержимому хранилища без доступа к узлу хранения.

Эта защита паролем не имеет ничего общего с защитой паролем резервной копии, которая задана в плане защиты и выполняется агентом. Если резервная копия уже защищена паролем, защита паролем на стороне узла хранения применяется поверх защиты паролем, выполненной агентом.

Для существующих управляемых хранилищ включение этого параметра невозможно. Защита хранилища паролем поддерживается только для формата резервных копий ”Версия 11” (см. раздел *Формат резервной копии*).

Как защитить хранилище паролем

На этапе развертывания управляемого хранилища (см. раздел *Добавление управляемого хранилища*) укажите и подтвердите пароль, который будет служить ключом защиты.

Поддерживаются следующие уровни защиты хранилища: **Базовый**, **Средний**, **Высокий**.

Чем выше уровень защиты, тем лучше будут защищены резервные копии.

Пароль на диске не хранится. Такая схема защиты позволяет обезопасить резервные копии от несанкционированного доступа, но восстановить утраченный пароль невозможно.

Дедупликация

В разделе описаны особенности дедупликации резервных копий на узле хранения. О дедупликации в архиве см. раздел *Дедупликация в архиве*.

Ограничения дедупликации

Общие ограничения

Дедупликация резервных копий на узле хранения поддерживается только для формата резервных копий ”Версия 11” (см. раздел *Формат резервной копии*).

Не поддерживается дедупликация резервных копий, защищенных паролем. Чтобы одновременно использовать и дедупликацию, и защиту паролем, не защищайте резервные копии, но укажите для них хранилище, где поддерживается как дедупликация, так и защита паролем.

Резервное копирование на уровне дисков

Дедупликация дисковых блоков не выполняется, если размер единицы выделения памяти (также называемый размером кластера или блока) тома не кратен 4 КБ.

> **Примечание**
>
> Размер единицы выделения памяти у большинства томов NTFS и ext3 равен 4 КБ. Это позволяет выполнять дедупликацию на уровне блоков. Другие примеры подходящих размеров единиц выделения памяти — 8 КБ, 16 КБ и 64 КБ.

Резервное копирование на уровне файлов

Дедупликация файла не выполняется, если файл защищен паролем.

Дедупликация и потоки данных NTFS

В файловой системе NTFS у файла может быть один или несколько связанных с ним дополнительных наборов данных, которые часто называют *альтернативными потоками данных*.

При создании резервной копии такого файла также создается копия альтернативных потоков данных. Однако эти потоки никогда не дедуплицируются, даже если дедуплицирован сам файл.

Рекомендации по дедупликации

Наиболее важные факторы, влияющие на скорость дедупликации:

- скорость доступа к базе данных дедупликации;
- объем оперативной памяти узла хранения;
- количество дедуплицирующих хранилищ, созданное в узле хранения.

Для увеличения производительности дедупликации следуйте рекомендациям ниже.

- Размещайте базу данных дедупликации и дедуплицирующее хранилище на разных физических носителях.

  В базе данных дедупликации содержатся хэш-значения всех элементов, которые хранятся в хранилище, кроме тех, которые не могут дедуплицироваться (например, файлы, защищенные паролем).

  Для увеличения скорости доступа к базе данных дедупликации база данных и хранилище должны быть размещены на разных физических носителях.

  Рекомендуется выделить специальные устройства для хранилища и базы данных. Если это невозможно, по крайней мере не размещайте хранилище или базу данных на диске с операционной системой. При работе операционной системы выполняется большое количество операций чтения/записи на жесткий диск, что существенно замедляет процесс дедупликации.

  Выбор диска для базы данных дедупликации:

  1. База данных должна находиться на стационарном диске. Не пытайтесь разместить базу данных дедупликации на внешних съемных носителях.
  2. Чтобы минимизировать время доступа к базе данных, сохраните ее на диске, подключенном напрямую, а не на подключенном сетевом томе. Задержка в сети может существенно снизить производительность дедупликации.
  3. Примерный объем дискового пространства, необходимого для базы данных дедупликации, вычисляется по следующей формуле:

     ```
     S = U \* 90 / 65536 + 10
     ```

     В этой формуле:

     - `S` — размер диска в ГБ;
     - `U` — планируемый объем уникальных данных в хранилище дедуплицированных данных (ГБ).

     Например, если планируемый объем уникальных данных в хранилище дедуплицированных данных U = 5 ТБ, для базы данных дедупликации потребуется объем свободного пространства не менее

     ```
     S = 5000 \* 90 / 65536 +10 = 17 ГБ
     ```

  Выбор диска для дедуплицирующего хранилища: для предотвращения потери данных рекомендуется использовать RAID 10, 5 или 6. RAID 0 не рекомендуется, поскольку не является отказоустойчивым. RAID 1 не рекомендуется из-за относительно низкой скорости. Можно

использовать как локальные диски, так и SAN.

- Используйте от 40 до 160 МБ ОЗУ на 1 ТБ уникальных данных.

  По достижении ограничения дедупликация выполняться не будет, а резервное копирование и восстановление продолжат выполняться. Если вы добавите ОЗУ в узел хранения после следующего резервного копирования, дедупликация восстановится. В общем, чем больше ОЗУ, тем больше размер томов с уникальными данными, которые можно сохранить.

- Используйте одно дедуплицирующее хранилище на каждый узел хранения.

  Настоятельно рекомендуется создавать только одно дедуплицирующее хранилище на узле хранения. В противном случае весь доступный объем ОЗУ будет распределен пропорционально количеству хранилищ.

- Избегайте приложений, конкурирующих за ресурсы.

  На машине с узлом хранения не должны быть запущены приложения, требующие большого количества системных ресурсов, например, системы управления базами данных (СУБД) или системы планирования ресурсов предприятия (ERP).

- Используйте многоядерные процессоры с тактовой частотой не менее 2,5 ГГц.

  Рекомендуется использовать процессор с количеством ядер не менее 4 и тактовой частотой не менее 2,5 ГГц.

- Убедитесь, что в хранилище достаточно свободного пространства.

  Для дедупликации в месте сохранения требуется столько же свободного пространства, сколько занимают данные резервной копии сразу после сохранения в хранилище. Без выполнения сжатия или дедупликации в источнике это значение равно размеру исходных данных, резервная копия которых создана во время данной операции резервного копирования.

- Используйте высокоскоростную локальную сеть.

  Рекомендуется скорость локальной сети 1 Гбит. Это позволит программе выполнить 5–6 операций резервного копирования параллельно с дедупликацией без заметного снижения скорости.

- Выполните резервное копирование типичной машины перед резервным копированием нескольких машин со сходным содержимым.

  При резервном копировании нескольких машин со сходным содержимым рекомендуется сначала выполнить резервное копирование одной машины и подождать завершения индексирования данных резервной копии. После этого резервное копирование остальных машин будет выполняться быстрее за счет эффективной дедупликации. Поскольку резервная копия первой машины была проиндексирована, большая часть данных уже находится в хранилище дедуплицированных данных.

- Выполняйте резервное копирование разных машин в разное время.

  При резервном копировании большого количества машин распределите операции резервного копирования по времени. Для этого необходимо создать несколько планов защиты с различными расписаниями.

Проверка наличия обновлений программного обеспечения

Эта функциональность доступна только для *администраторов организации*.

При каждом входе в веб-консоль Кибер Бэкап может проверять, доступна ли новая версия на веб-сайте Киберпротект. Если новая версия доступна, в веб-консоли Кибер Бэкап отображается ссылка на ее скачивание в нижней части каждой страницы на вкладках **Устройства**, **Планы** и **Хранилища резервных копий**. Ссылка также доступна на странице **Настройки** → **Агенты**.

Чтобы отключить автоматические проверки наличия обновлений (включены по умолчанию), измените системную настройку *Обновления*.

Чтобы проверить наличие обновлений вручную, щёлкните значок вопроса в верхнем правом углу, затем щёлкните **О программе** → **Проверить обновления**.

Управление лицензиями

Лицензирование Кибер Бэкап основано на количестве ресурсов, подлежащих резервному копированию. Подробнее о лицензиях см. в разделе *Издания и лицензии Кибер Бэкап*.

Чтобы приступить к использованию Кибер Бэкап, необходимо добавить на сервер управления хотя бы один лицензионный ключ. Лицензия автоматически назначается машине при применении плана защиты.

Кроме того, лицензии можно назначить и отозвать вручную. Ручные операции с лицензиями доступны только для *администраторов организации*.

Порядок доступа к разделу лицензий

1. Выполните одно из следующих действий:
   - Щёлкните **Настройки**.
   - Щёлкните значок учетной записи в правом верхнем углу.
2. Щёлкните **Лицензии**.

Добавление лицензионного ключа

1. Щёлкните **Добавить ключи**.
2. Введите лицензионные ключи.
3. Нажмите кнопку **Добавить**.

Назначение лицензии машине

1. Выберите лицензию.

   В программе отобразятся лицензионные ключи, соответствующие выбранной лицензии.
2. Выберите ключ, который нужно назначить.
3. Щёлкните **Назначить**.

   В программе отобразятся машины, которым можно назначить выбранный ключ.
4. Выберите машину и нажмите кнопку **Готово**.

Отзыв лицензии для машины

1. Выберите лицензию.

   В программе отобразятся лицензионные ключи, соответствующие выбранной лицензии. Машина, которой назначен ключ, указана в столбце **Кому назначено**.
2. Выберите лицензионный ключ, который нужно отозвать.
3. Щёлкните **Отозвать**.
4. Подтвердите операцию.

   Отозванный ключ останется в списке лицензионных ключей. Его можно назначить другой машине.

Автоматическое обнаружение машин

Функциональность обнаружения машин позволяет выполнять указанные ниже действия.

- Автоматизировать процесс установки агентов защиты и регистрации машины за счет автоматического выявления машин в домене Active Directory (AD) или локальной сети.
- Устанавливать и обновлять агент защиты на нескольких машинах.
- Использовать синхронизацию с Active Directory для уменьшения затрат, связанных с выделением ресурсов и управлением машиной в большой среде AD.

Важно

Обнаружение машины может выполняться только агентами, установленными на машинах Windows. В настоящее время агент обнаружения может обнаружить не только машины Windows, однако удаленная установка программного обеспечения возможна только на машинах Windows.

Если в вашей среде нет машин с установленным агентом, то функция автоматического обнаружения будет скрыта: раздел **Несколько устройств** будет скрыт в мастере **добавления нового устройства**.

После добавления машин в веб-консоль они подразделяются на указанные ниже категории.

- **Обнаружено**: обнаруженные машины без установленного агента защиты.
- **Управляемое**: машины, на которых установлен агент защиты.
- **Незащищенные**: машины, к которым не применен план защиты. Под незащищенными машинами подразумеваются как обнаруженные, так и управляемые машины без примененного плана защиты.
- **Защищено**: машины, к которым применен план защиты.

Принципы работы

При сканировании локальной сети агент обнаружения использует указанные ниже технологии. Обнаружение NetBIOS, Web Service Discovery (WSD) и таблица Address Resolution Protocol (ARP). Агент пытается получить следующие параметры для каждой машины:

- Имя (короткое/имя хоста NetBIOS)
- FQDN
- Домен/рабочая группа
- IP-адреса IPv4/IPv6
- MAC-адреса
- Операционная система (имя/версия/семейство)
- Категория машины (рабочая станция/сервер/контроллер домена)

Когда Active Directory выполняет сканирование, агент дополнительно извлекает параметр ”Организационная единица” и более подробную информацию об имени и операционной системе. Он не получает IP-адреса и MAC-адреса.

Предварительные требования

Прежде чем запустить обнаружение машин, необходимо установить агент защиты хотя бы на одной машине в локальной сети (см. *Установка агентов*), чтобы использовать его как агент обнаружения.

Если вы планируете выполнить обнаружение машин в домене Active Directory, необходимо установить агент как минимум на одной машине в этом домене. Этот агент будет использоваться как агент обнаружения при сканировании Active Directory.

Процесс обнаружения машины

В приведенной ниже схеме указаны основные этапы процесса обнаружения машины.



Как правило, весь процесс автоматического обнаружения состоит из следующих этапов:

1. Выберите метод обнаружения машины:
   - Сканирование Active Directory
   - Сканирование локальной сети

- Вручную: добавление машины по ее IP-адресу или имени хоста или импорт списка машин из файла

Первые два метода позволяют автоматически отфильтровывать результаты, чтобы исключить машины с установленными агентами.

При обнаружении машины вручную выполняется модернизация и перерегистрация существующих агентов. При автоматическом обнаружении с использованием той же учетной записи агент просто обновляется до последней версии (при необходимости). Если используется другая учетная запись, агент обновляется и перерегистрируется в клиенте, которому принадлежит учетная запись.

2. Выберите машины для добавления из списка, полученного в результате выполнение предыдущего действия.
3. Выберите способ добавления машин:
   - Агент защиты и дополнительные компоненты устанавливаются на машинах. Кроме того, они регистрируются в веб-консоли.
   - Машины регистрируются в веб-консоли (если они уже имеют установленный агент).
   - Машины добавляются в веб-консоль службы со статусом **Неуправляемое** без установки каких-либо агентов или компонентов.

   Если для добавления машины вы выбрали один из первых двух методов, можно также выбрать план защиты из существующих планов и применить его к машинам.
4. Укажите учетные данные пользователя с правами администратора на выбранных машинах.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. Проверьте, что можете подключиться к машинам, используя указанные учетные данные.

В следующих темах вы получите более подробную информацию о процедуре обнаружения.

Автоматическое и ручное обнаружение

Прежде чем запустить обнаружение, убедитесь, что соблюдены *предварительные требования*.

Обнаружение машин

1. В веб-консоли выберите пункты **Устройства** → **Физические и виртуальные машины**.
2. Нажмите кнопку **Добавить**.
3. В области **Несколько устройств** щёлкните **Windows-only (Только для Windows)**. Откроется мастер обнаружения
4. [Если в вашей организации есть отделы] Выберите отдел. Затем в агенте обнаружения вы сможете выбрать агенты, связанные с выбранным отделом и его дочерними отделами.
5. Выберите агент обнаружения, который выполнит сканирование для обнаружения машин.
6. Выберите метод обнаружения:
   - **Поиск в Active Directory**. Убедитесь, что машина с агентом обнаружения входит в домен Active Directory.
   - **Сканировать локальную сеть**. Если выбранному агенту обнаружения не удалось найти никаких машин, выберите другой агент обнаружения.
   - **Укажите вручную или импортируйте из файла**. Вручную определите машины для добавления или импортируйте их из текстового файла.
7. [Если выбран метод обнаружения Active Directory] Выберите метод поиска машин:
   - **В списке организационной единицы**. Выбор группы машин для добавления.
   - **По запросу диалекта LDAP**. Запрос диалект LDAP для выбора машин. **База поиска** определяет места поиска, а **Фильтр** позволяет указать критерий выбора машины.
8. [Если выбран метод обнаружения Active Directory или локальной сети] Используйте список для выбора машин, которые необходимо добавить.

   [Если выбран ручной метод обнаружения] Укажите IP-адреса машины или имена хостов либо импортируйте список машины из текстового файла. Файл должен содержать IP-адреса/имена хостов, по одному на строку. Ниже приводим пример файла:

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   После добавления адресов машины вручную или их импорте из файла агент попытается выполнить команду ping в отношении добавленных машин и определить их доступность.

9. Выберите действие, которое должно предприниматься после обнаружения:

   - **Установить агенты и зарегистрировать машины**. Компоненты для установки на машинах можно выбрать, щёлкнув **Выбор компонентов**. Дополнительную информацию см. в разделе *Выбор компонентов для установки*. Одновременно можно установить до 100 агентов.

     На экране **Выбор компонентов** укажите учетную запись, с которой будут запускаться службы. Для этого укажите **Учетная запись для входа службы агента**. Можно выбрать один из следующих вариантов:

     - **Использовать учетные записи пользователя услуги** (по умолчанию для службы агента)

       Учетные записи пользователя услуги — это системные учетные записи Windows, которые используются для запуска служб. Преимущество этой настройки состоит в том, что политики безопасности домена не влияют на права пользователей этих учетных записей. По умолчанию агент запускается в учетной записи **Локальная система**.

     - **Создать учетную запись**

       Имя учетной записи будет использоваться в качестве Agent User для агента.

     - **Использовать следующую учетную запись**

       При установке агента на контроллер домена система предложит указать существующие учетные записи (или ту же учетную запись) для агента. Из соображений безопасности система не может автоматически создавать учетные записи на контроллере домена.

     > **Важно**
     >
     > При установке агента на контроллер домена необходимо выбрать вариант **Использовать следующую учетную запись**, иначе установка завершится ошибкой.

     При выборе параметра **Создать учетную запись** или **Использовать следующую учетную запись** убедитесь, что политики безопасности домена не повлияют на права соответствующих учетных записей. Если права пользователя не были заданы для учетной записи при установке, данный компонент может работать неправильно или вообще не работать.

   - **Зарегистрировать машины с установленными агентами**. Этот параметр используется, если агент уже установлен на машинах и необходимо только зарегистрировать их в Кибер Бэкап. Если на машинах не найдено агента, они добавляются как машины со статусом **Неуправляемое**.

   - **Добавить как неуправляемые машины**. Агент не устанавливается на машинах. Вы сможете просмотреть их в веб-консоли и установить или зарегистрировать агент позже.

[Если выбрано действие после обнаружения **Установить агенты и зарегистрировать машины**] **При необходимости перезагрузите машину**: если выбран этот параметр, машина перезапускается столько раз, сколько необходимо для завершения установки.

Перезапуск машины может потребоваться в одном из следующих случаев:

- Все предварительно требуемые компоненты установлены. Необходимо перезапустить машину для продолжения установки.
- Установка завершена, но необходимо перезапустить машину, поскольку некоторые файлы были заблокированы при установке.
- Установка завершена, но необходимо перезапустить машину, поскольку на ней есть другие ранее установленные программы.

[Если выбран параметр **При необходимости перезагрузите машину**] **Не перезапускать, если пользователь в системе**: если этот параметр включен, машина не будет автоматически перезапускаться, когда в системе есть активный пользователь. То есть, если для установки потребуется перезапуск, когда пользователь работает, система не перезапускается.

Если необходимые компоненты были установлены, но перезапуск не выполнялся по причине активного пользователя в системе, то для завершения установки агента необходимо перезапустить машину и запустить установку снова.

Если агент был установлен, а перезапуск не выполнялся, необходимо перезагрузить машину.

[Если в вашей организации есть отделы] **Отдел для регистрации машины**: выберите отдел, в котором будут зарегистрированы машины.

Если выбрано одно из первых двух действий после обнаружения, то также есть возможность применить план защиты к машинам. При наличии нескольких планов защиты, необходимо выбрать конкретный план для использования.

10. Укажите учетные данные пользователя с правами администратора для всех машин.

> **Важно**
>
> Обратите внимание, что удаленная установка агента работает без каких-либо подготовительных действий только в том случае, когда указаны учетные данные встроенной учетной записи администратора (это первая учетная запись, созданная при установке системы). Если вы намерены создать настраиваемую учетную запись администратора, необходимо вручную выполнить дополнительные подготовительные операции, как описано в разделе Добавление машины с ОС Windows > ”Подготовка”.

11. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

    По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.

12. Система проверяет подключение ко всем машинам. Если не удастся установить подключение к некоторым машинам, можно изменить учетные данные для них.

При запуске процесса обнаружения машин соответствующее задание появится в действии **Обнаружение машин** (**Панель мониторинга** → **Действия**).

Выбор компонентов для установки

В таблице ниже приводится описание обязательных и дополнительных компонентов:

Компонент	Описание
Обязательный компонент	
Агент для Windows	Этот агент создает резервную копию дисков, томов и файлов. Он устанавливается на машинах Windows. Он устанавливается в любом случае (не подлежит выбору).
Дополнительные компоненты	
Агент для Hyper-V	Этот агент создает резервную копию виртуальных машин Hyper-V. Он устанавливается на хостах Hyper-V. Если этот компонент выбран, и на машине обнаружена роль Hyper-V, он будет установлен.
Агент для SQL	Этот агент создает резервную копию баз данных SQL Server. Он устанавливается на машинах с Microsoft SQL Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для Exchange	Этот агент создает резервную копию баз данных и почтовых ящиков Exchange. Он устанавливается на машинах с ролью почтового ящика Microsoft Exchange Server. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для Active Directory	Этот агент создает резервную копию данных доменных служб Active Directory. Он устанавливается на контроллерах домена. Если этот компонент выбран, и на машине обнаружена программа, он будет установлен.
Агент для VMware (Windows)	Этот агент создает резервную копию виртуальных машин VMware. Он устанавливается на виртуальных машинах Windows с сетевым доступом к vCenter Server. Если этот компонент выбран, он будет установлен.
Агент для Oracle	Этот агент создает резервную копию баз данных Oracle. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.
Мониторинг Защиты Данных	Этот компонент позволяет пользователю отслеживать выполнение запущенных заданий в области уведомлений, приостанавливать запуск планов защиты, устанавливать особые пароли для резервных копий машины. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Компонент	Описание
Инструмент командной строки	Кибер Бэкап поддерживает интерфейс командной строки с утилитой acrocmd. acrocmd не содержит никаких инструментов, которые физически выполняют команды. Она просто обеспечивает интерфейс командной строки для компонентов Кибер Бэкап — агентов и сервера управления. Если этот компонент выбран, он будет установлен.
Мастер создания загрузочных носителей	Этот компонент позволяет пользователям создать загрузочный носитель. Он устанавливается на машинах Windows (если выбрано).

Управление обнаруженными машинами

По окончании процесса обнаружения все обнаруженные машины отображаются в разделе **Устройства** → **Необслуживаемые машины**.

Этот раздел разбит на подразделы согласно используемым методам обнаружения. Полный список параметров машины показан ниже (зависит от метода обнаружения).

Имя	Описание
Имя	Имя машины. Если не удастся обнаружить имя машины, будет отображаться ее IP-адрес.
IP-адрес	IP-адрес машины.
Тип обнаружения	Метод обнаружения, использованный для выявления машины.
Организационная единица	Организационная единица в Active Directory, которой принадлежит машина. Этот столбец отображается при просмотре списка машин в разделе **Необслуживаемые машины** → **Active Directory**.
Операционная система	Операционная система, которая установлена на машине.

В разделе **Исключения** можно добавить машины, которые должны быть пропущены в процессе обнаружения. Например, если нет необходимости обнаруживать определенные машины, добавьте их в этот список.

Чтобы добавить машину в раздел **Исключения**, выберите ее в списке и щёлкните **Добавить в исключения**. Чтобы удалить машину из раздела **Исключения**, выберите пункты **Необслуживаемые машины** → **Исключения**, выберите машину и щёлкните **Удалить из исключений**.

Для установки агента защиты и регистрации группы обнаруженных машин в Кибер Бэкап можно выбрать их в списке и щёлкнуть **Установить и зарегистрировать**. В открытом мастере также можно назначить план защиты группе машин.

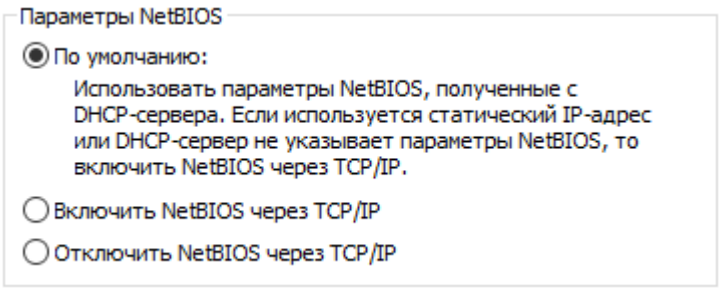
Те машины, на которых установлен агент защиты, отображаются в разделе **Устройства** → **Машины с агентами**.

Чтобы проверить статус защиты, откройте раздел **Панель мониторинга** → **Обзор** и добавьте виджет *Статус защиты* или виджет *Обнаруженная машина*.

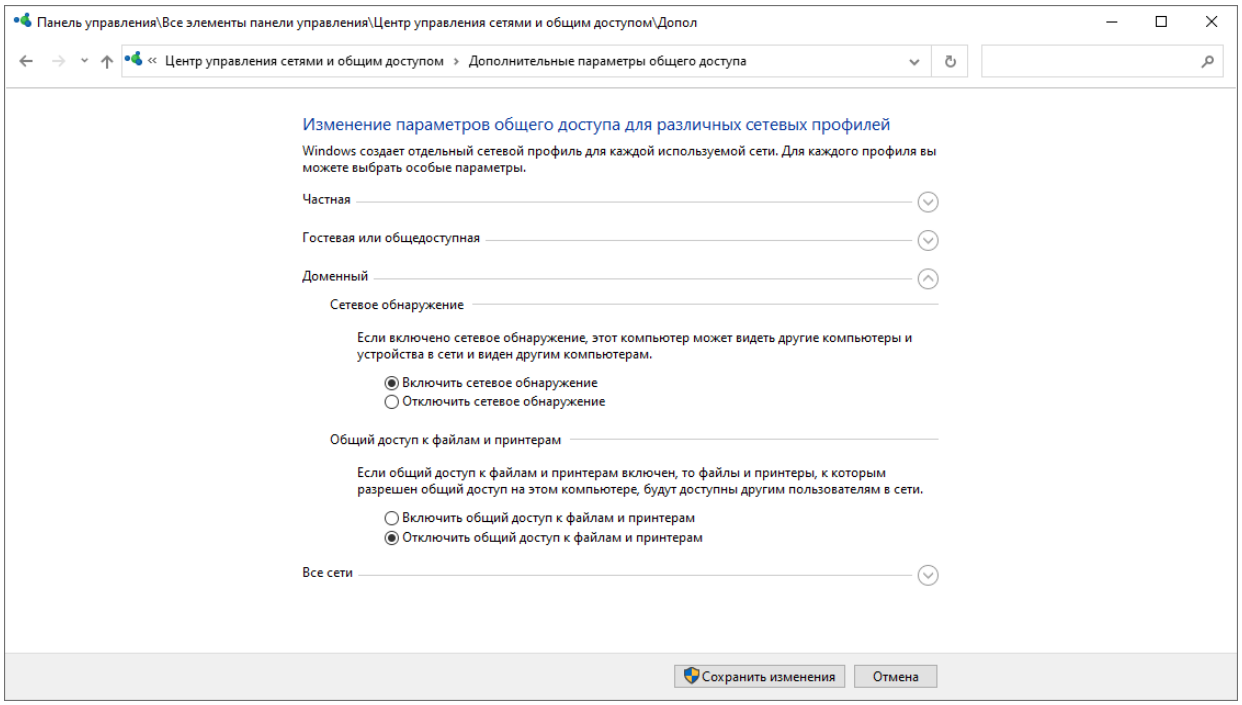
Устранение неисправностей при автоматическом обнаружении

Если есть какие-либо проблемы с функциональностью автоматического обнаружения, выполните указанные ниже действия.

1. Проверьте, что протокол ”NetBIOS через TCP/IP” включен или задан по умолчанию.



2. Выберите **Панель управления** → **Центр управления сетями и общим доступом** → **Дополнительные параметры общего доступа** и включите обнаружение сети.



3. Проверьте, что служба **Хост поставщика функции обнаружения** запущена на машине, которая выполняет обнаружение, и на машинах, которые должны быть доступны для обнаружения.

4. Проверьте, что служба **Публикация ресурсов обнаружения функции** запущена на машинах, которые должны быть доступны для обнаружения.

Обновление виртуальных устройств

В разделе описан порядок обновления агентов для платформ виртуализации.

Рекомендуется выполнять обновление агентов вне расписания резервного копирования. Все операции, выполняемые агентом во время его обновления, завершатся сбоем.

Порядок обновления виртуального устройства

1. Обновите сервер управления. Подробнее об этом см. раздел *Модернизация с предыдущих версий продукта*.
2. Скачайте пакет обновления агента.
3. Сохраните файлы `tar.bz2` в указанный ниже каталог на машине сервера управления:
   - Windows: `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
4. Для отображения списка виртуальных устройств в веб-консоли Кибер Бэкап выберите **Настройки** → **Агенты**.

   Для устаревших виртуальных устройств рядом с версией агента будет отображён оранжевый треугольник с восклицательным знаком.
5. Выберите виртуальные устройства, которые необходимо обновить. Эти виртуальные устройства должны быть включены.
6. Нажмите **Обновление агента**.

   Ход выполнения обновления показан на вкладке **Панель мониторинга** → **Действия**.
7. После завершения обновления откройте вкладку **Сведения** виртуального устройства. Проверьте версию устройства и статус подключения к платформе виртуализации.

Примечание

Агент для VMware (виртуальное устройство) версии более ранней, чем 15.24426 (выпущена в сентябре 2020 года), обновляется как агент, установленный на машине (см. раздел *Обновление агентов*).

Обновление агентов

Рекомендуется выполнять обновление агентов вне расписания резервного копирования. Все операции, выполняемые агентом во время его обновления, завершатся сбоем.

Агент, установленный на машине с ОС Linux, можно обновить, запустив новую версию его установочного файла.

Агент, установленный на машине с ОС Windows, можно обновить, запустив новую версию его установочного файла или из веб-консоли Кибер Бэкап.

Для работы функций Кибер Бэкап на машинах с ОС Windows требуется распространяемый компонент Microsoft Visual C++ 2022 версии не ниже 14.42.34438. Проверьте наличие этого компонента на машине или установите его перед обновлением агента. После установки может потребоваться перезагрузка. Распространяемый пакет Microsoft Visual C++ можно скачать по ссылке https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Примечание

Обновление агентов для виртуализации описано в разделе *Обновление виртуальных устройств*.

Проверка версии агента

1. В веб-консоли Кибер Бэкап перейдите в раздел **Настройки** → **Агенты**.
2. Посмотрите данные в столбце **Версия агента**.

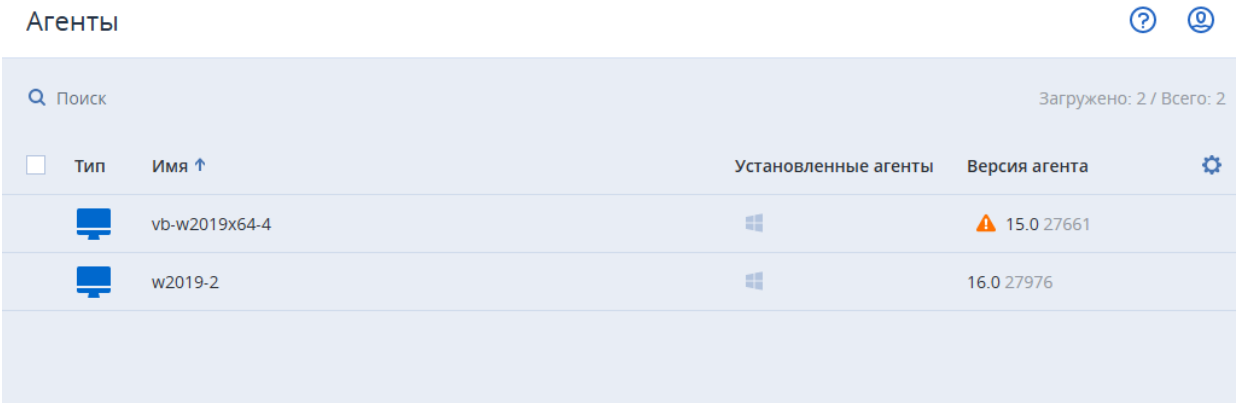
Порядок обновления агентов локально через установочный файл

1. Обновите сервер управления. Подробнее об этом см. раздел *Модернизация с предыдущих версий продукта*.
2. Скачайте установщик новой версии агента.
3. Запустите установщик на машине с агентом устаревшей версии.
4. Примите лицензионное соглашение и нажмите **Обновить**.
5. Для агентов на машинах с ОС Linux далее см. раздел *Ручная установка агентов в ОС Linux*.
6. Для агентов на машинах с ОС Windows далее см. раздел *Ручная установка агентов в ОС Windows*.

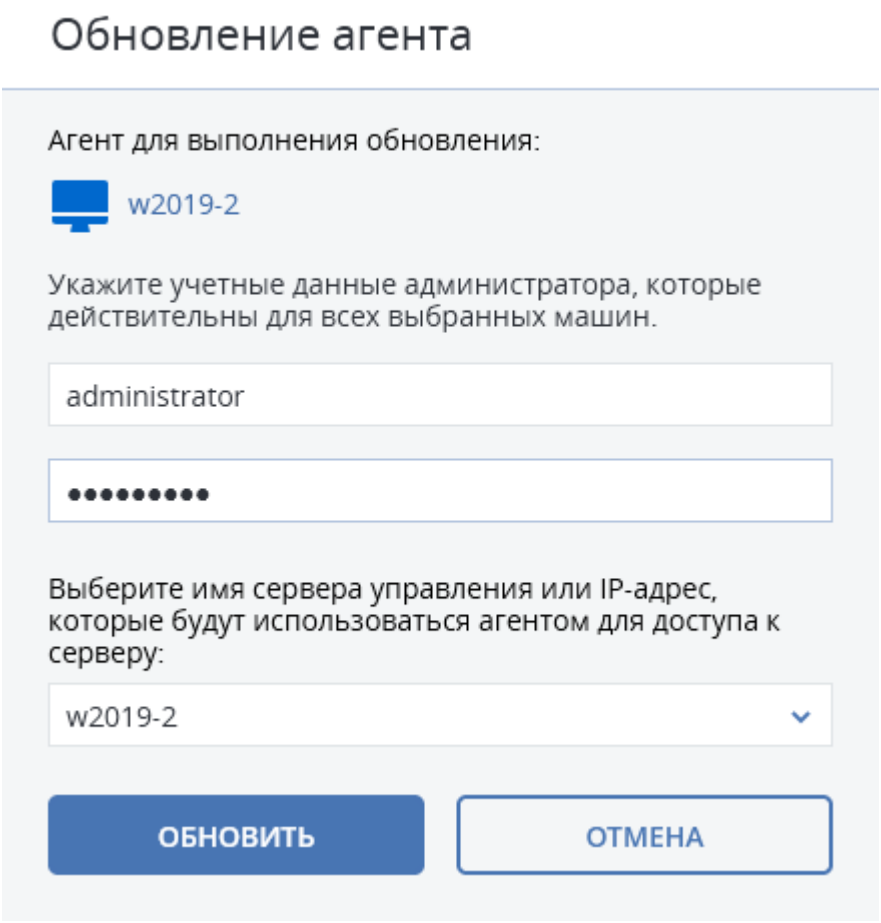
Порядок обновления агентов из веб-консоли Кибер Бэкап

1. Обновите сервер управления и узел хранения (подробнее см. раздел *Модернизация с предыдущих версий продукта*).
2. Убедитесь, что на машине с сервером управления есть пакеты установки (подробнее см. раздел *Добавление машины с ОС Windows*).
3. В веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** → **Агенты**.

   В программе будет выведен список машин. Машины с агентами устаревших версий будут помечены оранжевым восклицательным знаком.



4. Выберите машины, на которых нужно обновить агенты. Машины должны быть включены.
5. Щёлкните **Обновление агента**.



6. Выберите агент развертывания.
7. Укажите данные учетной записи с правами администратора на целевой машине.

> **Важно**
>
> Пароль учетной записи не должен быть пустым.

8. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
9. Ход выполнения обновления отображается на вкладке **Действия**.

Модернизация с предыдущих версий продукта

Можно выполнить модернизацию до последней версии непосредственно на машине с более ранней версией Кибер Бэкап или с предварительным удалением предыдущей версии продукта.

Предупреждение

Перед выполнением модернизации настоятельно рекомендуем создать резервную копию системы. Это позволит выполнить возврат к оригинальной конфигурации в случае сбоя модернизации.

Выполняйте обновление до новой версии согласно следующей таблице обновлений. Использование порядка обновлений, отличного от рекомендуемого, может привести к сбоям.

Установленная версия Кибер Бэкап	Рекомендуемая версия для обновления
12.5	15 обновление 2.6 — 17.1
15 обновление 2.5	15 обновление 2.6 — 17.1
15 обновление 2.6	17.0 — 17.4
15 обновление 2.7	17.0 — 17.4
16.0	17.0 — 17.4
16.5	17.0 — 17.4
17.0	18.0 — 18.6
17.1	18.0 — 18.6
17.2	18.0 — 18.6
17.3	18.0 — 18.6
17.4	18.0 — 18.6
18.0	19.0
18.1	19.0
18.5	19.0
18.6	19.0

Обратите внимание, что переход со старых версий на новые выполняется поэтапно. Например, если у вас установлена версия 16.0, то обновление до версии 19.0 будет включать в себя несколько шагов: обновление с версии 16.0 до любой из версий 17.0 — 17.4, далее обновление до любой из версий 18.0 — 18.6, и, наконец, обновление до версии 19.0.

Это связано с тем, что более старые версии лишь частично поддерживают функции более новых. Например, сервер управления в Кибер Бэкап 16.5 и 17.x версий обратно совместим с агентами версий 12.5 и 15 и поддерживает их. Однако эти агенты не поддерживают функции Кибер Бэкап версий 16.5 и 17.x.

Обновлять продукт необходимо, следуя порядку, указанному далее.

Порядок обновления на новую версию Кибер Бэкап

1. Обновление сервера управления и узла хранения.
2. Обновление агента Кибер Бэкап.

> **Важно**
>
> Если вы обновляете сервер управления и узел хранения по отдельности, первым всегда обновляйте сервер управления. Обновляйте агента Кибер Бэкап только после того, как обновили сервер управления и узел хранения.

Обновление сервера управления и узла хранения выполняется посредством установщика Кибер Бэкап новой версии.

Обновление агента Кибер Бэкап можно выполнить с помощью установщика новой версии Кибер Бэкап или через веб-консоль. Для обновления агента посредством установщика см. следующие пункты (”Обновление с предыдущей версии Кибер Бэкап в ОС Linux” и ”Обновление с предыдущей версии Кибер Бэкап в ОС Windows”). Для обновления агента посредством веб-консоли обратитесь к разделу *Обновление агентов*.

> **Важно**
>
> Во избежание сбоев не обновляйте сервер управления и узел хранения, когда выполняются следующие операции:
>
> - операции резервного копирования и восстановления данных;
> - операции с лентами, подключенными к узлу хранения (например, повторное сканирование лент).

Обновление агентов не влияет на существующие резервные копии и их настройки.

При необходимости настройте размер хранилища NATS для высоконагруженных конфигураций (см. *Рекомендуемые конфигурации оборудования для сервера управления*).

Обновление с предыдущей версии Кибер Бэкап в ОС Linux

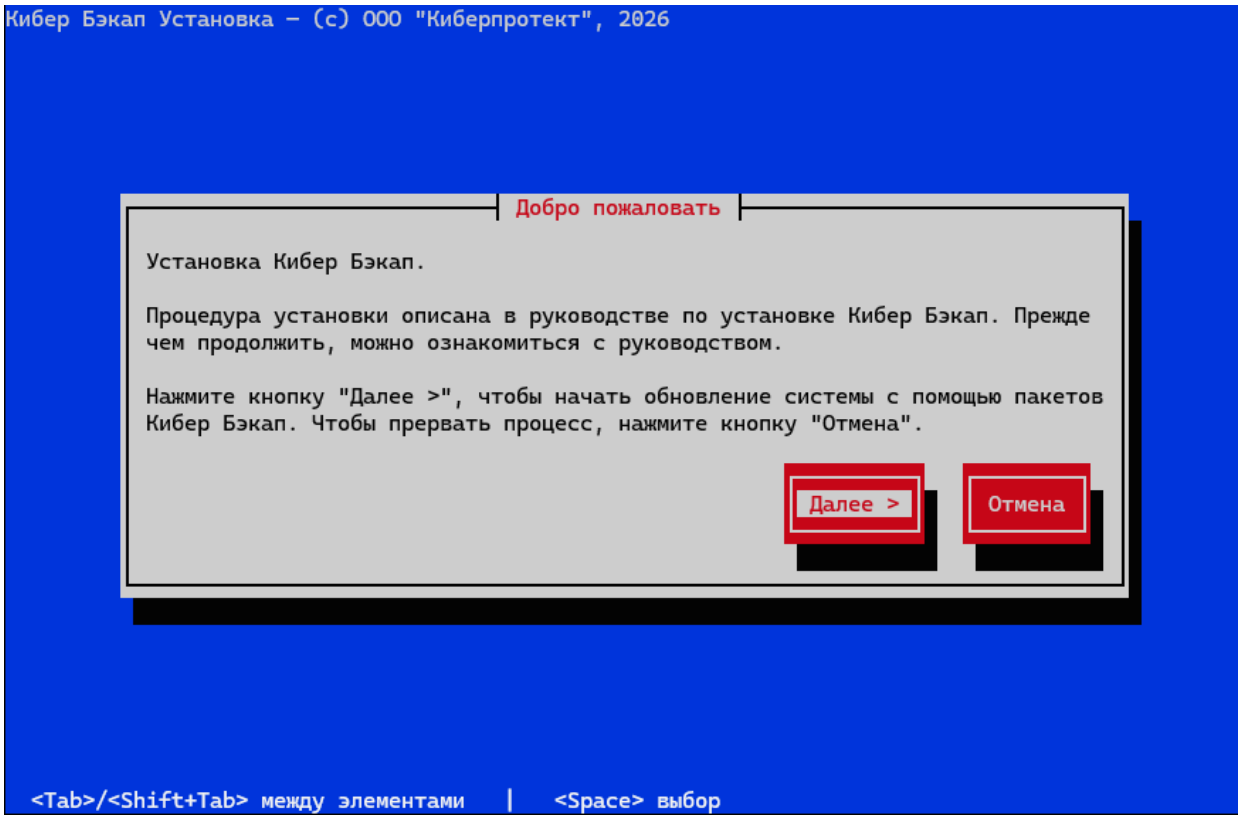
1. Загрузите файл установщика на машину с сервером управления или узлом хранения.
2. Дайте разрешение на исполнение установочному файлу. Например:

```
chmod +x CyberBackup_18_64-bit.x86_64
```

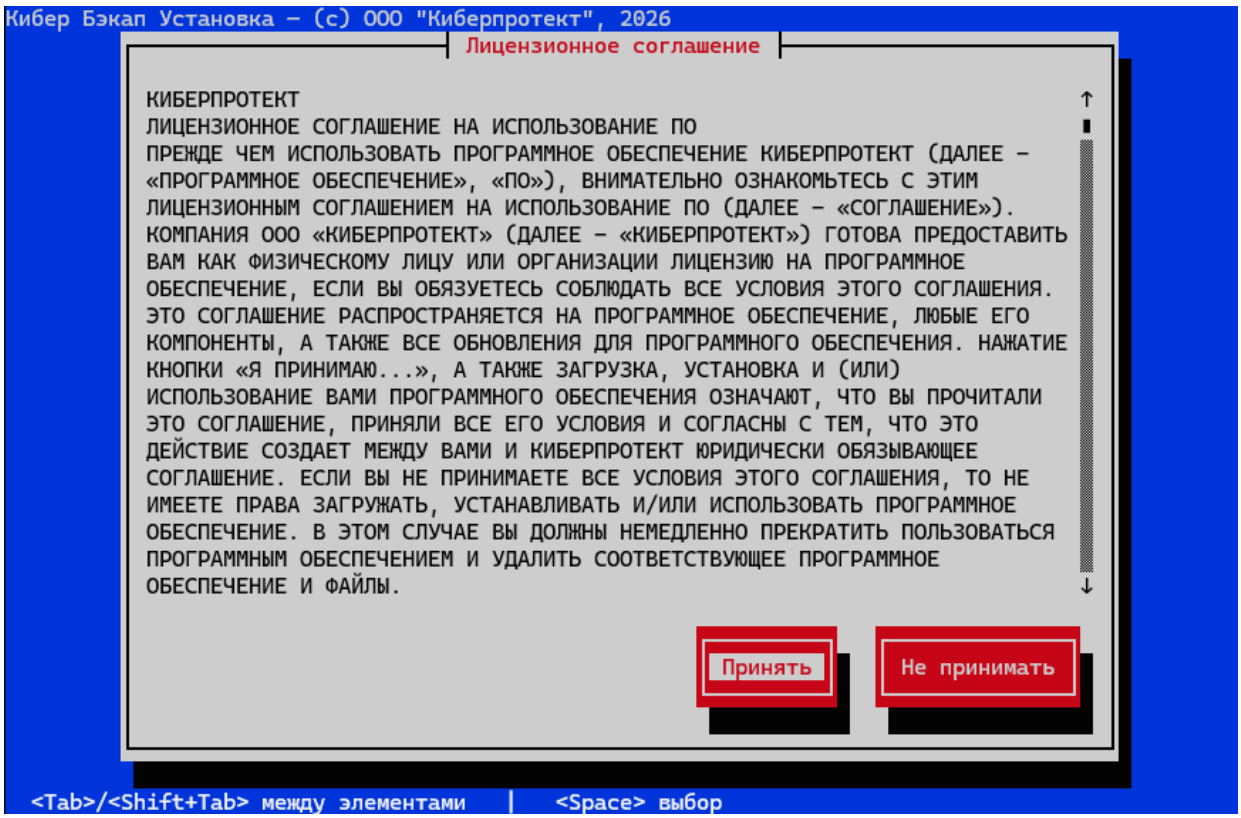
3. Запустите установщик. Например:

```
./CyberBackup_18_64-bit.x86_64
```

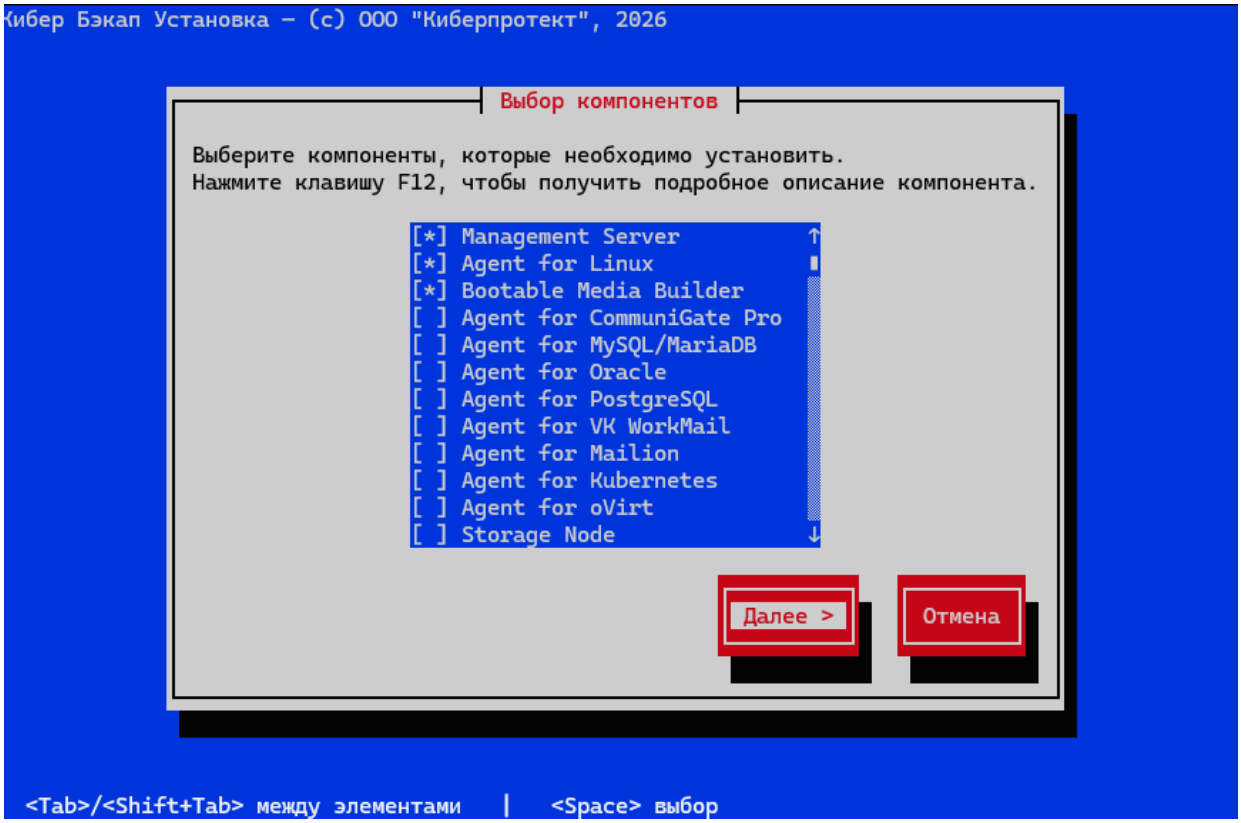
4. На экране **Добро пожаловать** нажмите **Далее**.



5. На экране **Лицензионное соглашение** примите условия лицензионного соглашения, нажав **Принять**.

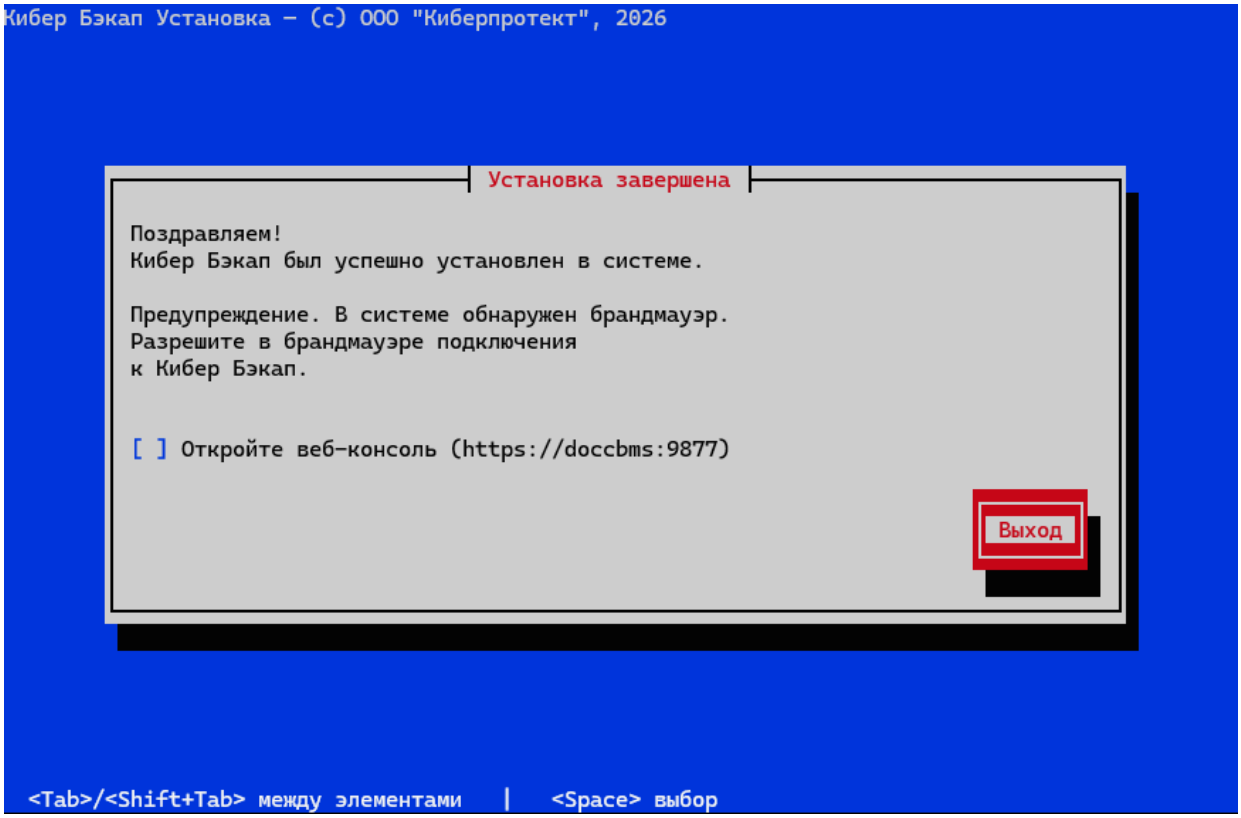


6. На экране **Выбор компонентов** нажмите **Далее**.



Дождитесь окончания установки

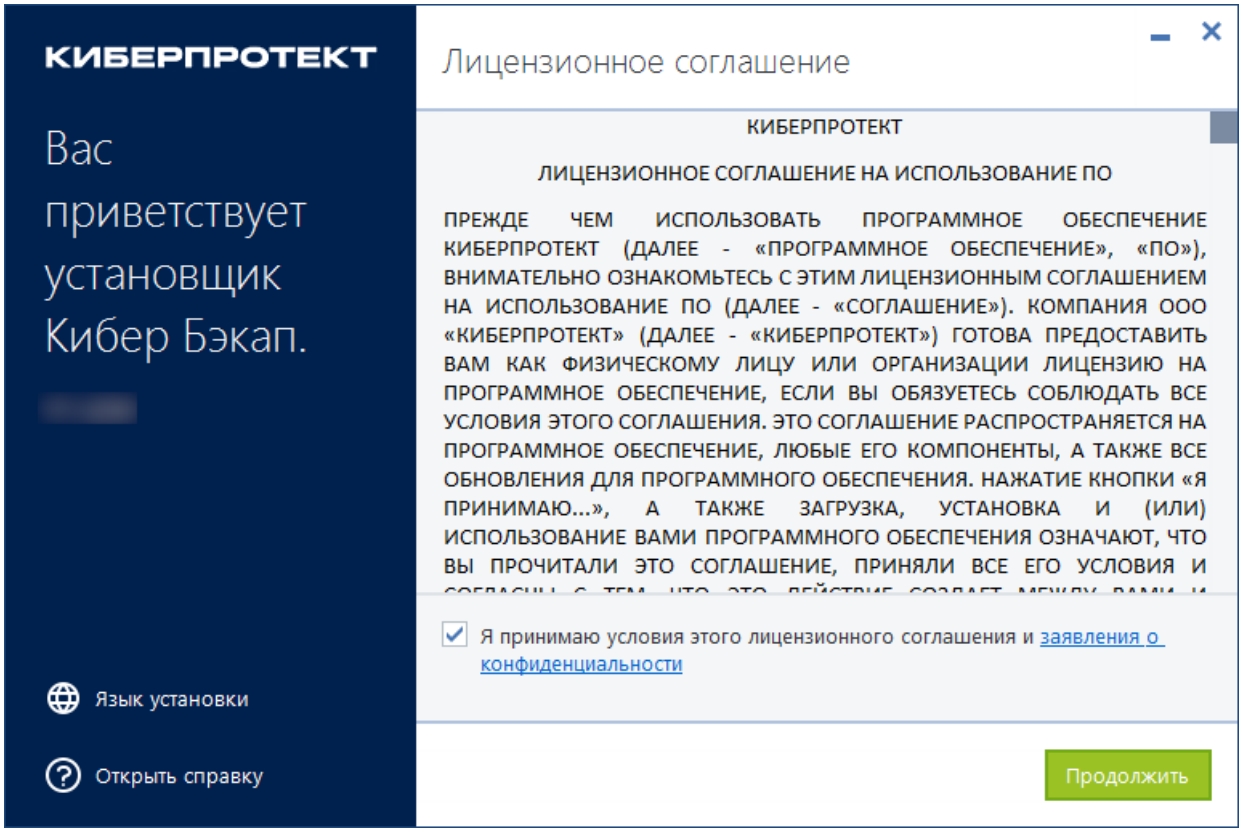
7. На экране **Установка завершена** нажмите **Выход**.



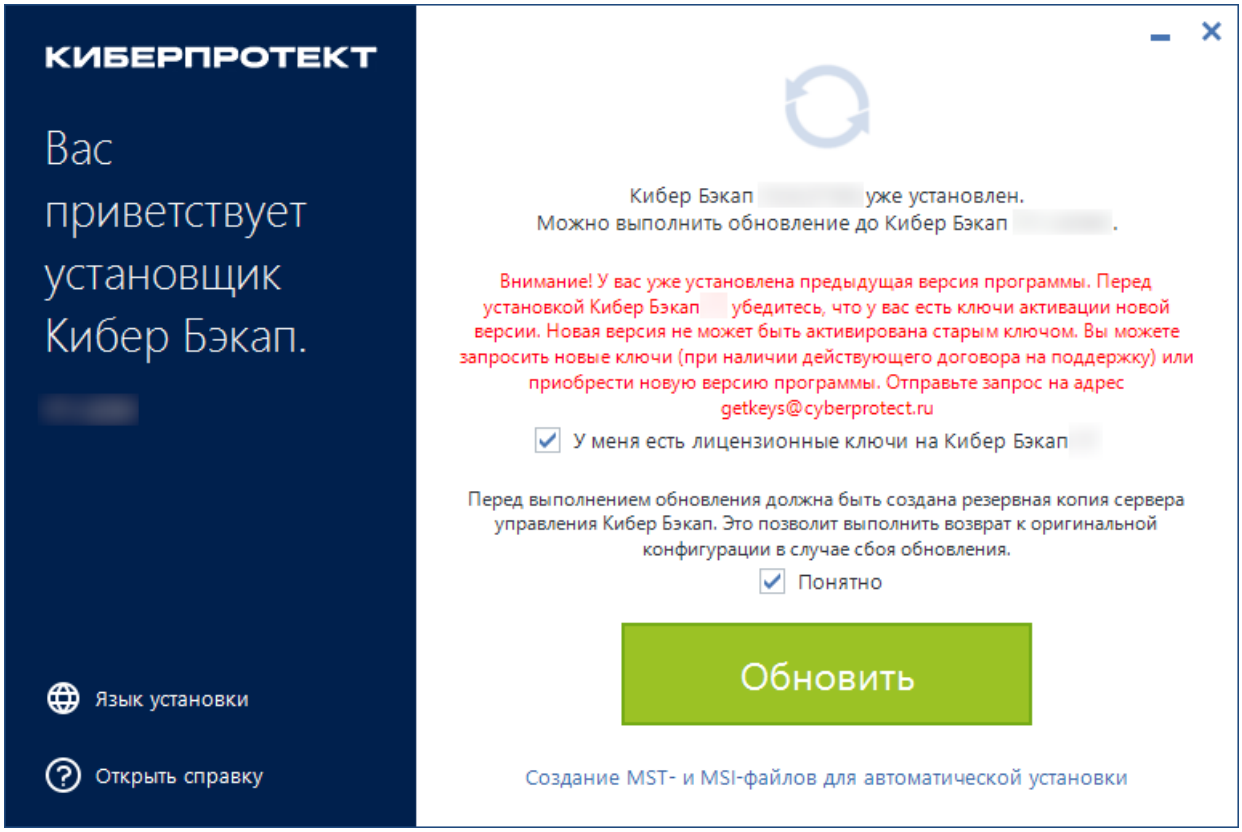
В результате установленная на вашей машине версия Кибер Бэкап будет обновлена.

Обновление с предыдущей версии Кибер Бэкап в ОС Windows

1. Запустите установщик на машине с сервером управления или узлом хранения. Для продолжения установки вам потребуется принять лицензионное соглашение.



2. При необходимости можно изменить язык отображения сообщений во время обновления, нажав **Язык установки**. После выбора языка установки нажмите **Продолжить**.
3. Для продолжения установки обновления подтвердите наличие у вас лицензии на новую версию Кибер Бэкап.



Для продолжения подтвердите также, что прочитали рекомендацию о создании резервной копии сервера управления. После этого нажмите **Обновить**. Установленная на вашем компьютере версия Кибер Бэкап будет обновлена.

Удаление продукта

Чтобы удалить с машины отдельные компоненты продукта, запустите программу установки, перейдите к изменению продукта и отмените выбор компонентов, которые больше не нужны. Ссылки на программы установки доступны на странице **Загрузки** (щёлкните значок учетной записи в правом верхнем углу и выберите пункт **Загрузки**).

Если нужно удалить все компоненты продукта с машины, следуйте приведенным ниже инструкциям.

Предупреждение

Выбирайте компоненты для удаления с осторожностью.

Если удалить сервер управления по ошибке, веб-консоль Кибер Бэкап станет недоступной и вы больше не сможете выполнять резервное копирование и восстановление машин, зарегистрированных на удаленном сервере управления.

Windows

1. Войдите как администратор.
2. Откройте **Панель управления** и выберите **Программы и компоненты** → **Кибер Бэкап** → **Удалить**.
3. [Необязательно] Установите флажок **Удалить журналы и параметры конфигурации**.

   Не устанавливайте этот флажок, если удаляете агент и планируете установить его снова. Если установить флажок, машина может быть дуплицирована в веб-консоли Кибер Бэкап. При этом резервные копии старой машины могут быть не связаны с новой машиной.
4. Подтвердите операцию.

Linux

1. В качестве привилегированного пользователя выполните `/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall`.
2. [Необязательно] Установите флажок **Очистить все следы продукта (удалить журналы продукта и параметры конфигурации)**.

   Не устанавливайте этот флажок, если удаляете агент и планируете установить его снова. Если установить флажок, машина может быть дуплицирована в веб-консоли Кибер Бэкап. При этом резервные копии старой машины могут быть не связаны с новой машиной.
3. Подтвердите операцию.

Удаление агента для VMware (виртуальное устройство)

1. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
2. Если виртуальное устройство включено, щёлкните его правой кнопкой мыши, а затем щёлкните **Питание** → **Выключить питание**. Подтвердите операцию.
3. Если виртуальное устройство использует локально присоединенное хранилище на виртуальном диске и нужно сохранить данные на диске, выполните указанные ниже действия.

   1. Щёлкните виртуальное устройство правой кнопкой мыши и выберите пункт **Изменить настройки**.
   2. Выберите диск с хранилищем и щёлкните **Удалить**. В разделе **Параметры удаления** нажмите кнопку **Удалить из виртуальной машины**.
   3. Нажмите кнопку **ОК**.

   В результате диск остается в хранилище данных. Можно подключить диск к другому виртуальному устройству.

4. Щёлкните виртуальное устройство правой кнопкой мыши и выберите пункт **Удалить с диска**. Подтвердите операцию.

Удаление машин из веб-консоли Кибер Бэкап

После удаления агента его регистрация на сервере управления будет отменена. Кроме того, из веб-консоли Кибер Бэкап будет автоматически удалена запись о машине, на которой был установлен агент.

Если при выполнении этой операции подключение к серверу управления будет утрачено (например, из-за проблемы в сети), агент может удалиться, но его машина при этом может продолжать отображаться в веб-консоли. В этом случае необходимо удалить машину из веб-консоли службы вручную.

Порядок удаления машины из веб-консоли вручную

1. В веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** → **Агенты**.
2. Выберите машину, на которой установлен агент.
3. Щёлкните **Удалить**.

Веб-консоль Кибер Бэкап

Веб-консоль является основным инструментом управления продуктом Кибер Бэкап.

Для доступа к веб-консоли Кибер Бэкап введите адрес страницы входа в адресной строке веб-браузера, а затем выполните вход, как описано ниже.

Адрес страницы входа — это IP-адрес или имя машины, на которой установлен сервер управления:

- `localhost:9877` — С сервера управления можно автоматически войти в систему от имени текущего пользователя.
- `ms_IP:9877` — При входе по IP-адресу сервера управления всегда нужно указывать имя пользователя и пароль.
- `ms_hostname:9877` — При входе по имени хоста сервера управления всегда нужно указывать имя пользователя и пароль.

На одном TCP-порту поддерживаются оба протокола (HTTP и HTTPS). Внести изменения в эту настройку можно при *установке сервера управления*. По умолчанию используется порт 9877.

Сервер управления можно настроить таким образом, чтобы запретить доступ к веб-консоли Кибер Бэкап по HTTP и использовать сторонний сертификат SSL.

Максимальная продолжительность активной сессии пользователя составляет 24 часа.

В Windows

Если сервер управления установлен в ОС Windows, существует два способа войти в веб-консоль Кибер Бэкап.

- Щёлкните **Войти**, чтобы войти как текущий пользователь Windows.

  Это самый простой способ входа с машины, на которой установлен сервер управления.

  Если сервер управления установлен на другой машине, этот способ работает при условии, что:

  - Машина, с которой выполняется вход, находится в одном домене Active Directory с сервером управления.
  - Вы вошли как пользователь домена.

  Рекомендуется настроить веб-браузер *для выполнения встроенной проверки подлинности Windows*. В противном случае веб-браузер запросит имя пользователя и пароль. Однако этот параметр можно отключить.

- Щёлкните **Ввести имя пользователя и пароль**, а затем укажите имя пользователя и пароль.

В любом случае учетная запись должна находиться в списке администраторов сервера управления. По умолчанию этот список содержит группу **Администраторы** на машине, где работает сервер управления. Дополнительные сведения см. в разделе *Отделы и административные учетные записи*.

Порядок отключения параметра входа под учетной записью текущего пользователя Windows

1. На машине с установленным сервером управления перейдите в папку `C:\Program Files\Acronis\AccountServer`.
2. Откройте файл `account_server.json` для редактирования.
3. Перейдите к разделу ”connectors” и удалите следующие строки:

```
{
”type”: ”sspi”,
”name”: ”1 Windows Integrated Logon”,
”id”: ”sspi”,
”config”: {}
},
```

4. Перезапустите службу Киберпротект Service Manager, как описано в разделе *Использование сертификата, выданного доверенным центром сертификации*.

В Linux

Если на сервере управления установлена ОС Linux, укажите имя пользователя и пароль учетной записи, которая включена в список администраторов сервера управления. По умолчанию в этот список входит только пользователь **root** на машине с запущенным сервером управления. Также в список администраторов можно добавить учетные записи других пользователей, в том числе из домена Active Directory. Дополнительные сведения см. в разделе *Отделы и административные учетные записи*.

Смена языка

После входа в систему можно изменить язык веб-интерфейса, щёлкнув значок учетной записи в правом верхнем углу.

Настройка веб-браузера для выполнения встроенной проверки подлинности Windows

Выполнение встроенной проверки подлинности Windows возможно при наличии доступа к веб-консоли Кибер Бэкап с машины с запущенной Windows и любого *поддерживаемого браузера*.

Рекомендуется настроить веб-браузер для выполнения встроенной проверки подлинности Windows. В противном случае веб-браузер запросит имя пользователя и пароль.

Настройка Microsoft Edge, Opera и Google Chrome

Если машина, на которой запущен браузер, находится в одном домене Active Directory с машиной, на которой работает сервер управления, добавьте страницу входа консоли к списку веб-узлов локальной интрасети.

В противном случае, добавьте страницу входа консоли к списку надежных веб-узлов и включите параметр **Автоматический вход в систему с текущим пользователем и паролем**.

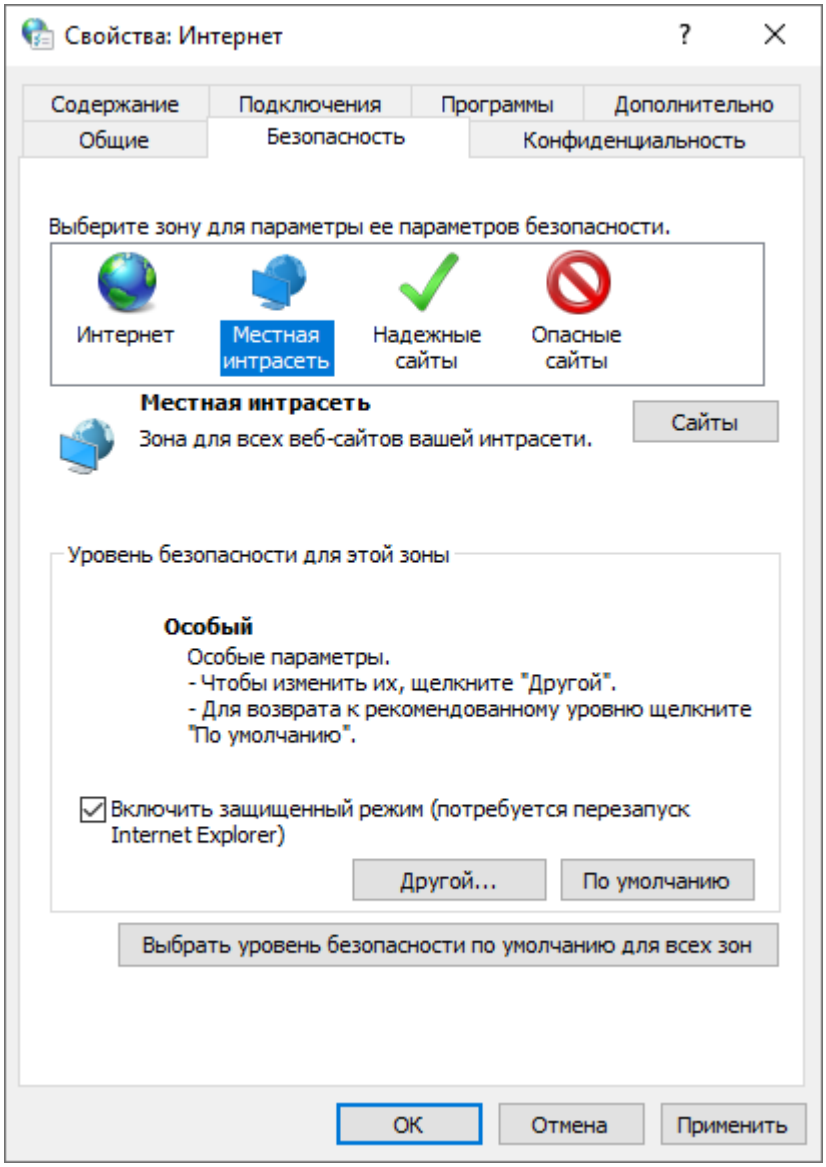
См. пошаговые инструкции далее в этом разделе. Поскольку эти браузеры используют параметры Windows, возможна их настройка с помощью групповой политики в домене Active Directory.

Настройка Mozilla Firefox

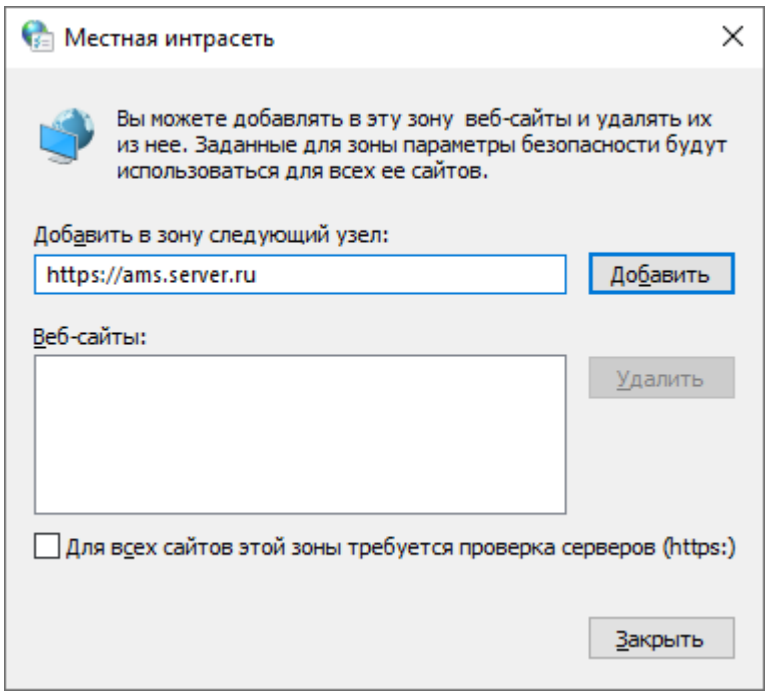
1. В Firefox перейдите на URL-адрес `about:config`, а затем нажмите кнопку **Я принимаю возможные риски**.
2. В поле `Поиск` выполните поиск настройки **network.negotiate-auth.trusted-uris**.
3. Дважды щёлкните настройку, а затем введите адрес страницы входа в веб-консоль Кибер Бэкап в одном из форматов, указанных в разделе *Веб-консоль Кибер Бэкап*. Например, `https://localhost:9877` или `http://localhost:9877`.
4. Повторите шаги 2-3 для настройки `network.automatic-ntlm-auth.trusted-uris`.
5. Закройте окно `about:config`.

Добавление консоли к списку веб-узлов локальной интрасети

1. Выберите **Панель управления** → **Свойства браузера**.
2. Во вкладке **Безопасность** выберите **Местная интрасеть**.



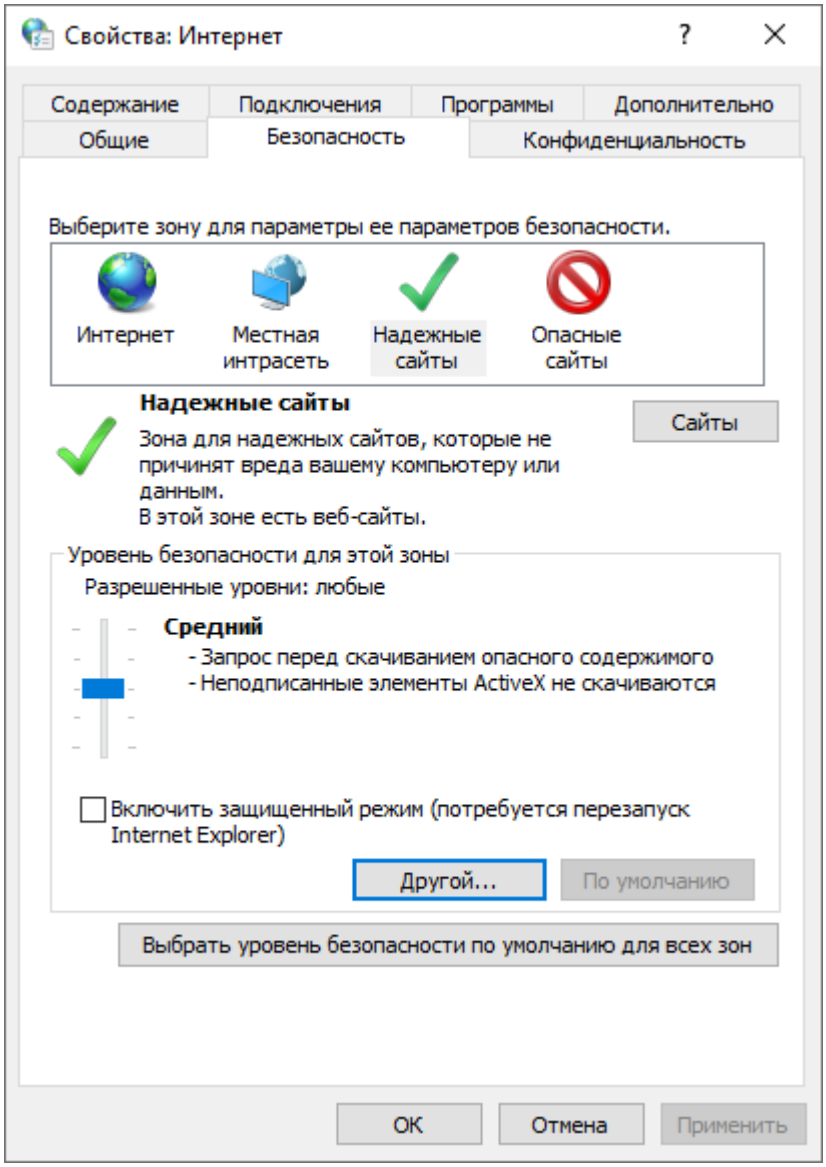
3. Нажмите кнопку **Сайты** и далее **Дополнительно**.
4. В поле **Добавить в зону следующий узел** введите адрес страницы входа в веб-консоль Кибер Бэкап, а затем щёлкните **Добавить**.



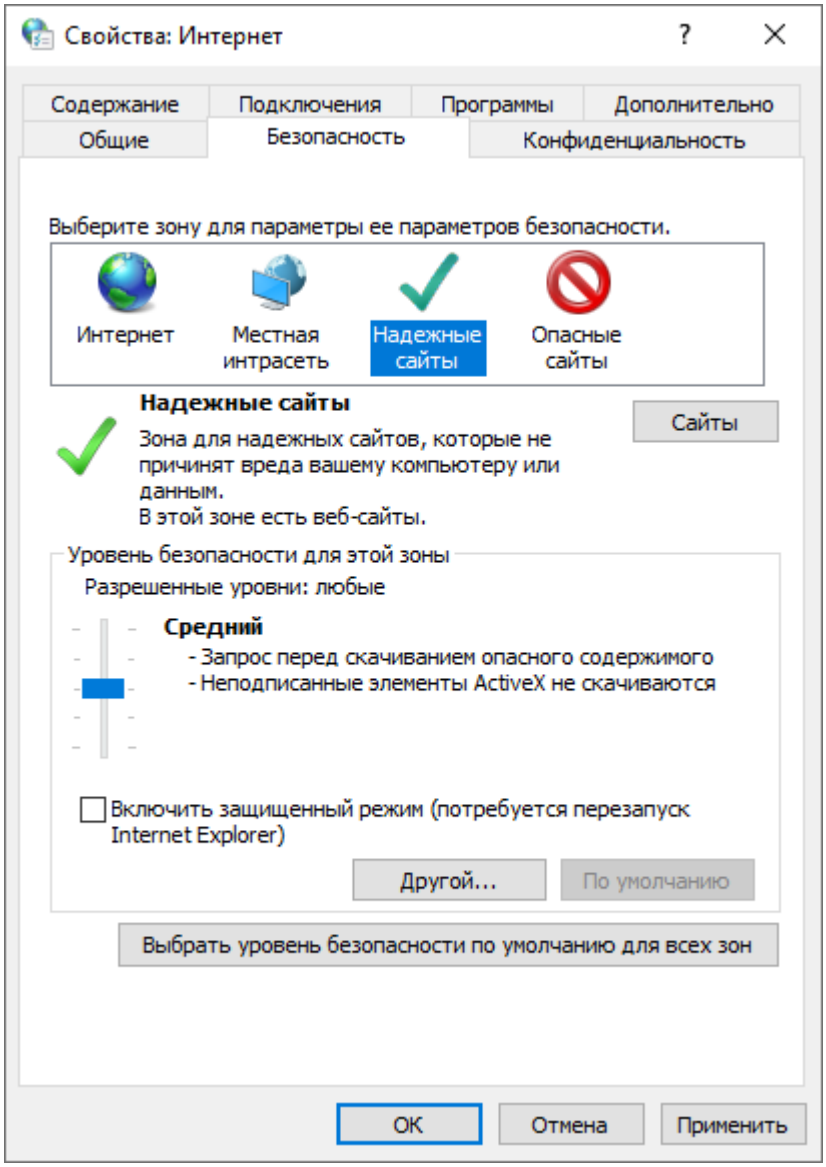
5. Нажмите кнопку **Закрыть**.
6. Нажмите кнопку **ОК** и далее **Применить**.

Добавление консоли к списку доверенных веб-узлов

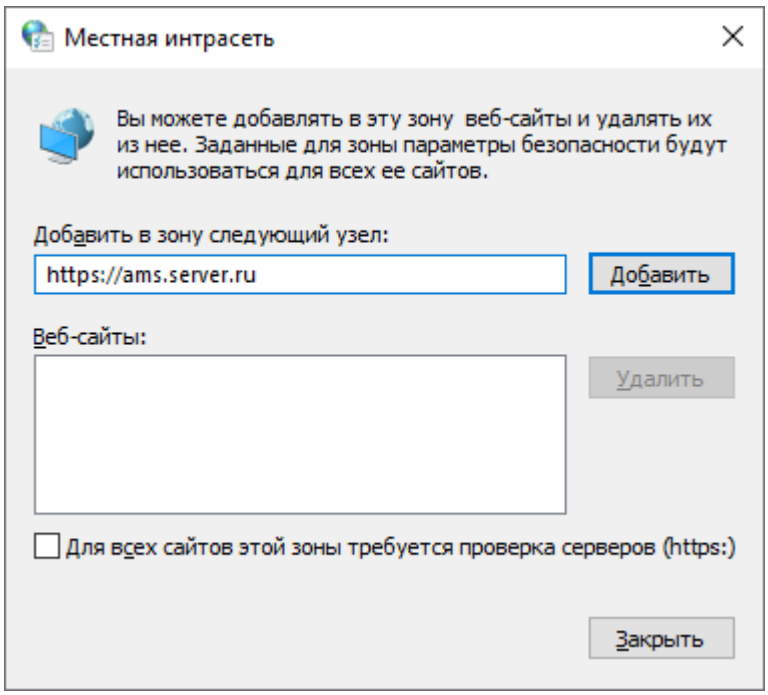
1. Выберите **Панель управления** → **Свойства браузера**.
2. Во вкладке **Безопасность** выберите **Надежные сайты**, а затем нажмите **Другой**.



3. В группе **Проверка подлинности пользователя** выберите **Автоматический вход в сеть с текущим именем пользователя и паролем**, а затем нажмите кнопку **OK** и далее **Применить**.



4. Во вкладке **Безопасность** при выбранной зоне **Надежные сайты** нажмите **Сайты**.
5. В поле **Добавить в зону следующий узел** введите адрес страницы входа в веб-консоль Кибер Бэкап, а затем щёлкните **Добавить**.



6. Нажмите кнопку **Закрыть**.
7. Нажмите кнопку **Применить**.

Настройки сертификата SSL

В этом разделе затронуты следующие темы:

- Настройка агента защиты, который использует самозаверяющий сертификат SSL, сгенерированный сервером управления.
- Замена самозаверяющего сертификата SSL, созданного сервером управления, на сертификат, выписанный доверенным центром сертификации (например, GlobalSign). В этом случае сертификат, используемый сервером управления, будет доверенным на любой машине. Оповещение безопасности браузера не будет появляться при входе в веб-консоль Кибер Бэкап по HTTPS.

При необходимости можно настроить сервер управления таким образом, чтобы запретить доступ к веб-консоли Кибер Бэкап по HTTP и перенаправлять всех пользователей через HTTPS.

Использование самозаверяющих сертификатов

Порядок настройки агента защиты в Windows

1. На машине с агентом откройте редактор реестра.
2. Найдите следующий раздел реестра:

`HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions`.

3. Задайте параметру **VerifyPeer** значение `0`.
4. Убедитесь, что параметру **VerifyHost** задано значение `0`.
5. Перезапустите Managed Machine Service (MMS):
    1. В меню **Пуск** щёлкните **Запустить**, а затем введите `cmd`.
    2. Нажмите кнопку **ОК**.
    3. Выполните следующие команды:

```
net stop mms
net start mms
```

Порядок настройки агента защиты в Linux

1. На машине с агентом откройте файл `/etc/Acronis/BackupAndRecovery.config` для редактирования.
2. Перейдите к разделу `CurlOptions` и задайте параметру `VerifyPeer` значение `0`. Убедитесь, что параметру `VerifyHost` задано значение `0`.
3. Сохраните внесенные изменения.
4. Перезапустите Managed Machine Service (MMS), выполнив следующую команду в любом каталоге:

```
sudo service acronis_mms restart
```

Порядок настройки виртуального устройства

1. Подключитесь к консоли виртуального устройства.

> **Примечание**
>
> Чтобы запустить командную оболочку, нажмите клавиши CTRL+SHIFT+F2.

2. Откройте файл `/etc/Acronis/BackupAndRecovery.config` для редактирования.
3. Перейдите к разделу `CurlOptions` и задайте параметрам `VerifyHost` и `VerifyPeer` значение `0`, например:

```
<value name=”VerifyHost” type=”Tdword”>”0”</value>
<value name=”VerifyPeer” type=”Tdword”>”0”</value>
```

4. Сохраните внесенные изменения.
5. Перезапустите виртуальное устройство.

Использование сертификата, выданного доверенным центром сертификации

Порядок изменения настроек сертификата SSL

1. Убедитесь, что у вас есть:
   - Файл сертификата (в формате .pem)
   - Файл с закрытым ключом для сертификата (обычно в формате .key)
   - Парольная фраза закрытого ключа (если ключ зашифрован)
2. Скопируйте файлы на машину, на которой запущен сервер управления.
3. На этой машине откройте указанный ниже файл конфигурации с текстовым редактором:
   - В ОС Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - В ОС Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
4. Найдите следующий раздел:

```
”tls”: {
    ”cert_file”: ”cert.pem”,
    ”key_file”: ”key.pem”,
    ”passphrase”: ””,
    ”auto_redirect”: false
}
```

5. Между двойными кавычками в строке ”cert_file” укажите полный путь к файлу сертификата. Пример:
   - В Windows (обратите внимание на символы косой черты): ”cert_file”: ”C:/certificate/local-domain.ams.pem”
   - В ОС Linux: ”cert_file”: ”/home/user/local-domain.ams.pem”
6. Между двойными кавычками в строке ”key_file” укажите полный путь к файлу закрытого ключа. Пример:
   - В Windows (обратите внимание на символы косой черты): ”key_file”: ”C:/certificate/private.key”

- В ОС Linux: "key_file": "/home/user/private.key"

7. Если закрытый ключ зашифрован, укажите его парольную фразу между двойными кавычками в строке "passphrase". Пример: "passphrase": "my secret passphrase"
8. Чтобы запретить доступ к веб-консоли Кибер Бэкап по HTTP и перенаправлять всех пользователей через HTTPS, измените значение "auto_redirect" с false на true. В противном случае пропустите этот шаг.
9. Сохраните файл api_gateway.json.

> **Важно**
>
> Будьте внимательны, чтобы не удалить в файле конфигурации ни одной запятой, скобки и двойной кавычки.

10. Перезапустите службу Киберпротект Service Manager, как описано ниже.

Порядок перезапуска службы Киберпротект Service Manager в Windows

1. В меню **Пуск** выберите команду **Выполнить** и введите: cmd.
2. Нажмите кнопку **ОК**.
3. Выполните следующие команды:

```
net stop asm
net start asm
```

Порядок перезапуска службы Киберпротект Service Manager в Linux

1. Откройте приложение терминала.
2. Выполните следующую команду в любом каталоге:

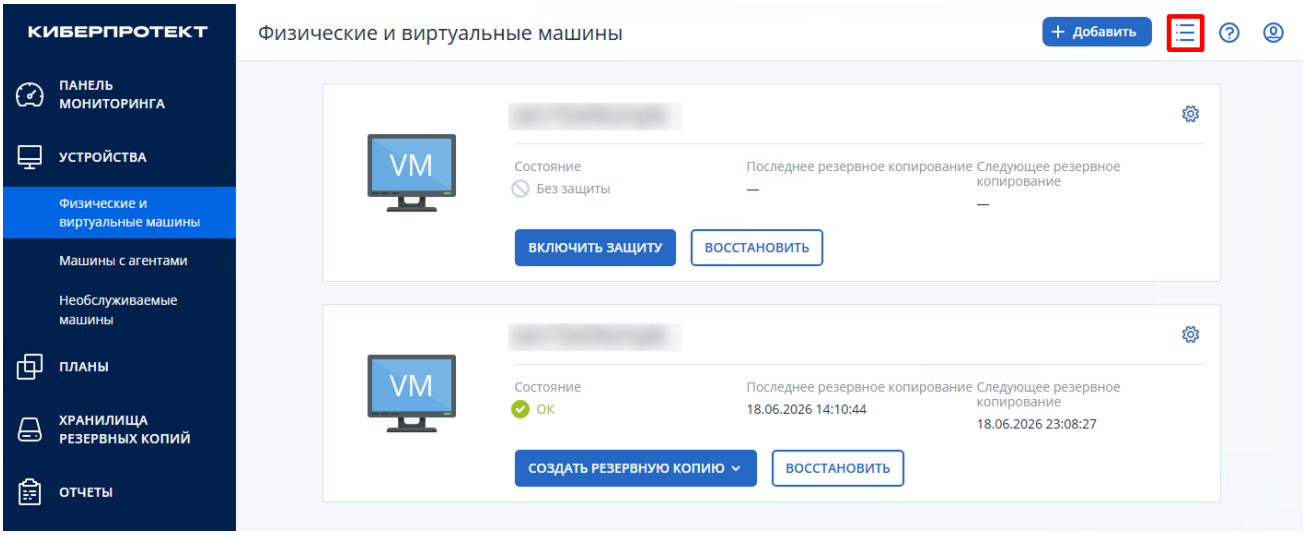
```
sudo service acronis_asm restart
```

Режимы отображения списка устройств

Список устройств в веб-консоли Кибер Бэкап можно отображать в **простом** и **табличном** режимах. Они различаются только типом представления данных. Набор доступных функций и операций при этом один и тот же.

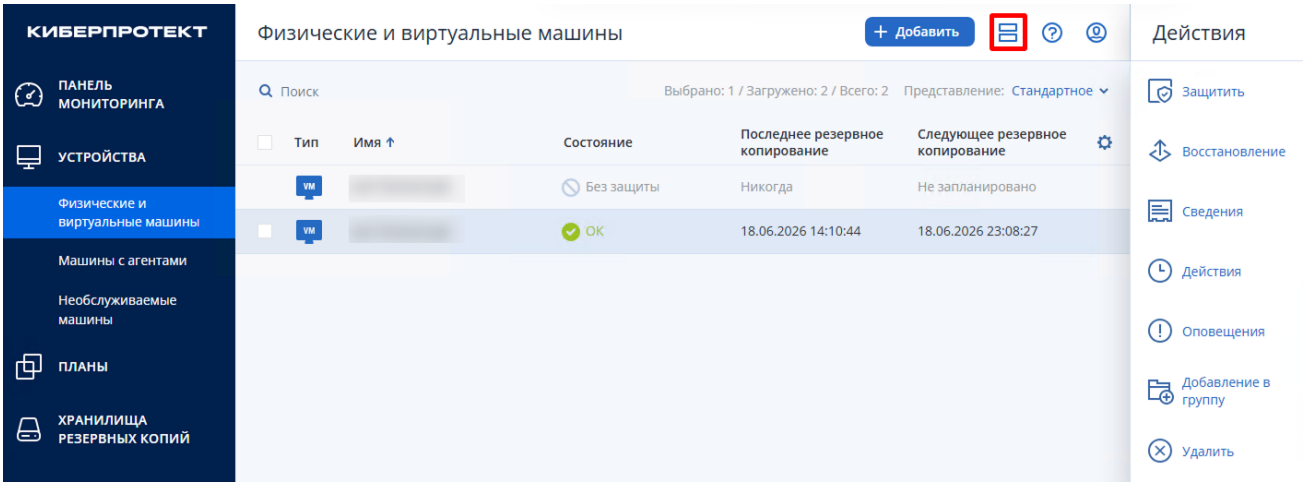
Простой режим

Пример отображения устройств в простом режиме приведён на рисунке ниже. Для переключения на табличный режим отображения щёлкните значок в правом верхнем углу веб-консоли.



Табличный режим

Пример отображения устройств в табличном режиме приведён на рисунке ниже. Для переключения на простой режим отображения щёлкните значок в правом верхнем углу веб-консоли.



Настройка представлений в табличном режиме

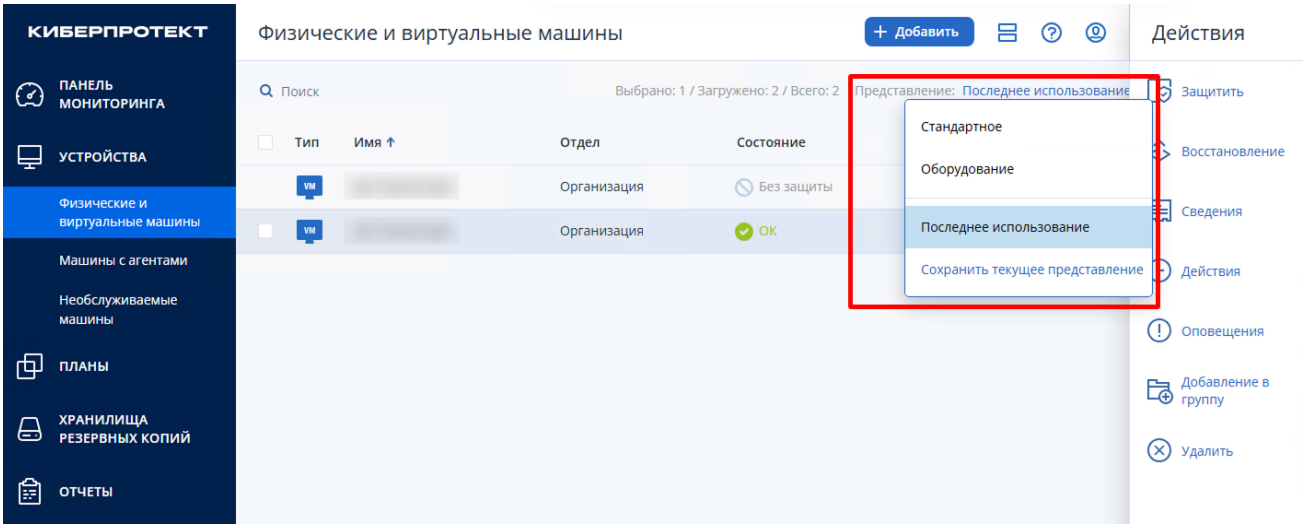
Кибер Бэкап в табличном режиме позволяет отображать только нужные столбцы с данными об устройствах. Доступны как предустановленные варианты представлений, так и возможность создания собственного (пользовательского) представления.

Чтобы выбрать представление, в верхней строке веб-консоли нажмите текущее название и в выпадающем списке выберите нужный вариант:

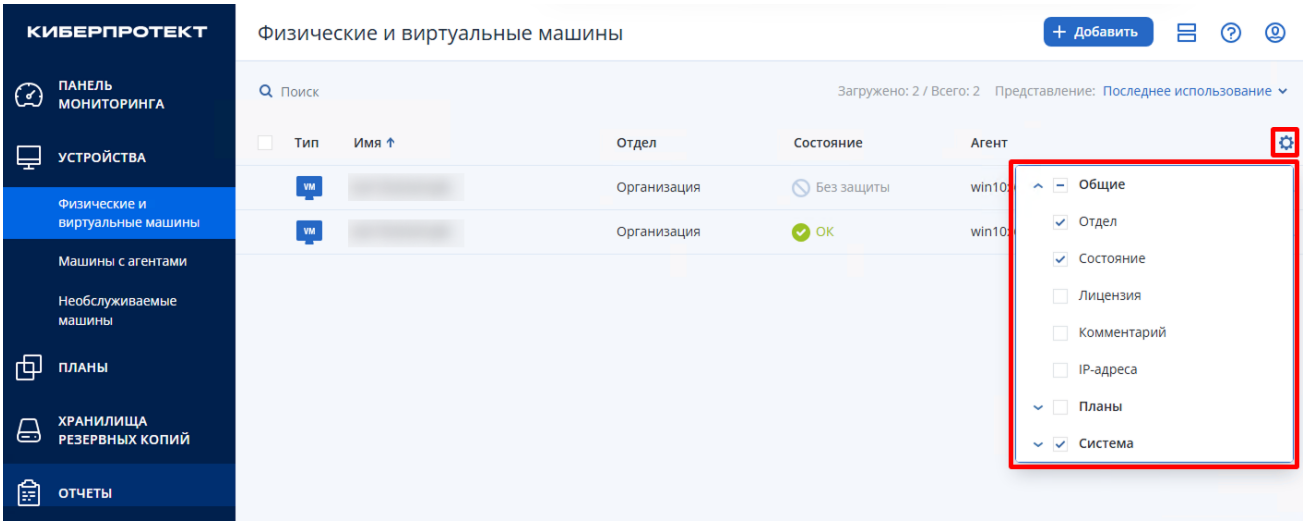
- **Стандартное** (значение по умолчанию). Отображаются столбцы: **Тип**, **Имя**, **Состояние**, **Последнее резервное копирование**, **Следующее резервное копирование**.
- **Оборудование**. Отображаются столбцы: **Тип**, **Имя**.
- **Последне использование**. Отображаются столбцы, выбранные пользователем в предыдущий раз (кроме сохранённых наборов).

> **Примечание**
>
> Данный вариант отображается, если пользователь настроил, но не сохранил собственный набор столбцов.

- Пользовательское представление (отображается название пользовательского представления после его сохранения).



Чтобы настроить пользовательский набор столбцов, щёлкните значок шестерёнки в правом верхнем углу веб-консоли и в выпадающем списке отметьте нужные столбцы или их группы.

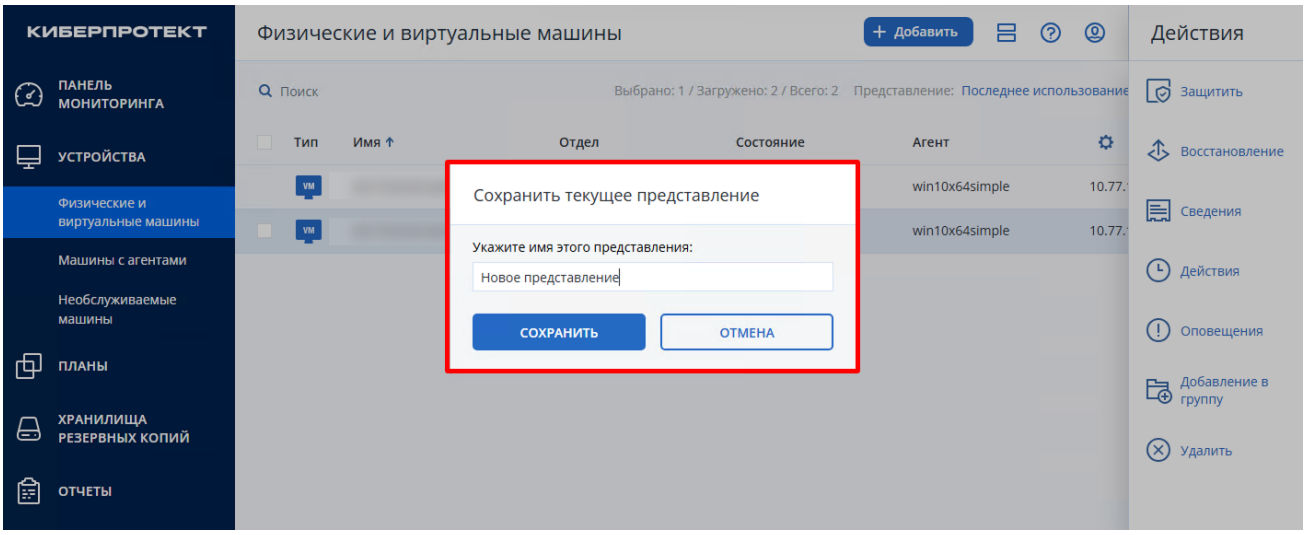


В результате выбранные столбцы будут отображены в таблице, а в верхней строке веб-консоли название представления поменяется на **Последнее использование**.

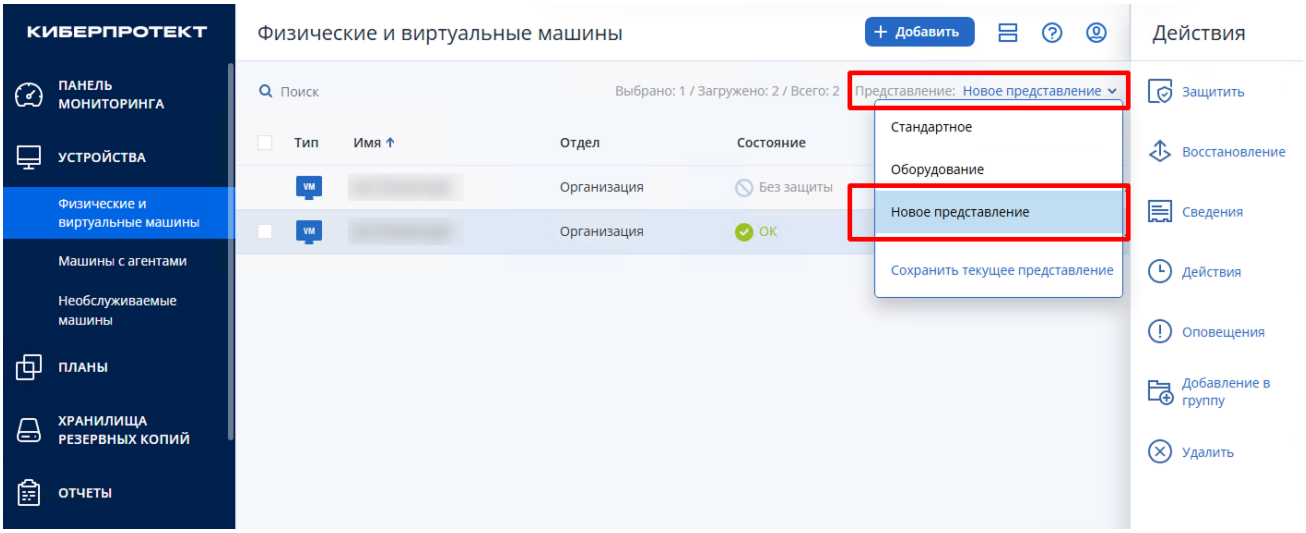
Сохранение пользовательских представлений

Пользовательский набор отображаемых столбцов можно сохранить. Для этого выполните следующие действия:

1. В верхней строке веб-консоли нажмите название текущего представления.
2. В выпадающем меню нажмите **Сохранить текущее представление**.
3. В окне **Сохранить текущее представление** введите название для нового представления и нажмите **Сохранить**.



В результате пользовательское представление будет сохранено и появится в списке представлений. Также его название появится в верхней строке веб-консоли службы.



Удаление пользовательских представлений

Для удаления пользовательского представления выполните следующие действия:

1. В верхней строке веб-консоли службы нажмите название текущего представления.
2. В выпадающем меню выберите представление и нажмите значок крестика в его строке.

В результате пользовательское представление будет удалено. Если оно использовалось в момент удаления, система автоматически переключится на **Стандартное** представление.

План защиты и модули

План защиты — это план, объединяющий в себе модули защиты данных, указанные ниже:

- *Резервное копирование* позволяет создавать резервную копию источников данных в выбранном хранилище данных.
- *Активная защита (Active Protection)* позволяет выполнять проверку компьютеров встроенным средством защиты от вредоносных программ.

Создавая гибкие планы для разных потребностей бизнеса, различные модули можно включить и отключить, задать их настройки.

Создание плана защиты

План защиты можно применить к нескольким машинам на этапе его создания или позже. При создании плана система проверяет операционную систему и тип устройства (например, рабочая станция, виртуальная машина и т. д.) и показывает только те модули плана, которые применимы к вашим устройствам.

План защиты можно создать одним из двух способов, которые описаны ниже.

- В разделе **Устройства**: при выборе устройства или устройств для защиты с последующим созданием плана для них.
- В разделе **Планы**: при создании плана с последующим выбором машин, к которым он будет применён.

Порядок создания плана защиты:

Из раздела Устройства

1. В веб-консоли Кибер Бэкап выберите **Устройства** → **Физические и виртуальные машины**.
2. Выберите машины, для которых нужно обеспечить защиту.
3. Щёлкните **Защитить**, а затем **Создать план**. Откроется план защиты с настройками по умолчанию.
4. [Необязательно] Для изменения имени плана защиты щёлкните значок карандаша рядом с именем.

> **Примечание**
>
> Для хранения имени плана может использоваться не более 128 байт. Тип используемых символов влияет на занимаемый ими объём: символ латиницы или цифра занимает 1 байт, символ русского алфавита — 2 байта, эмодзи — 4 байта и более.

5. [Необязательно] Для включения или отключения модуля плана защиты щёлкните переключатель рядом с именем модуля.
6. [Необязательно] Для настройки параметров модуля щёлкните соответствующий раздел плана защиты.
7. Щёлкните **Создать**.

Из раздела Планы

1. В веб-консоли Кибер Бэкап выберите **Планы** → **Защита**.
2. Щёлкните **Создать план**. Откроется план защиты с настройками по умолчанию.
3. В поле **Выбор данных** укажите ресурсы, для которых нужно обеспечить защиту.
4. [Необязательно] Для изменения имени плана защиты щёлкните значок карандаша рядом с именем.

> **Примечание**
>
> Для хранения имени плана может использоваться не более 128 байт. Тип используемых символов влияет на занимаемый ими объём: символ латиницы или цифра занимает 1 байт, символ русского алфавита — 2 байта, эмодзи — 4 байта и более.

5. [Необязательно] Для включения или отключения модуля плана защиты щёлкните переключатель рядом с именем модуля.
6. [Необязательно] Для настройки параметров модуля щёлкните соответствующий раздел плана защиты.
7. Щёлкните **Создать**.

Модуль **Резервное копирование** можно выполнить по требованию. Для этого щёлкните **Запустить сейчас** (подробнее см. в разделе *Запуск резервного копирования вручную*).

Для настройки модуля Active Protection см. раздел *Активная защита (Active protection)*.

Разрешение конфликтов плана

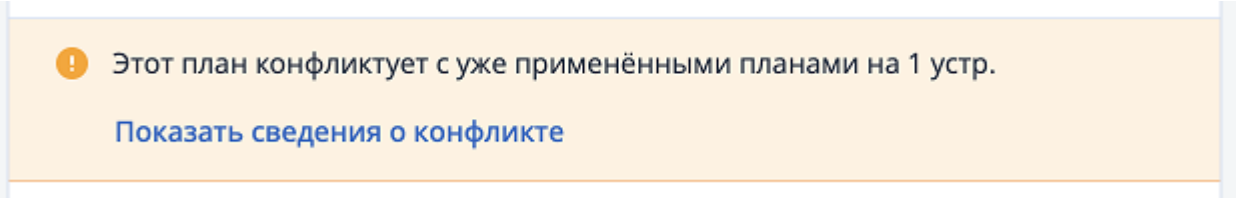
План защиты может иметь одно из указанных ниже состояний.

- **Активный**: план, который назначен устройствам и выполняется на них.
- **Неактивный**: план, который назначен устройствам, но отключен и не выполняется на них.

Применение нескольких планов к устройству

К одному устройству можно применить несколько планов защиты с модулем Резервное копирование. Планы с модулем Активная защита (Active Protection) применяются с ограничением: этот модуль можно применить к одному устройству только один раз. Например, можно применить план защиты с модулями Активная защита (Active Protection) и Резервное копирование и другой план, в котором включен только модуль Резервное копирование.

При попытке применения нескольких планов защиты с модулем Активная защита (Active Protection) возникнет конфликт. В этом случае Кибер Бэкап отобразит уведомление:



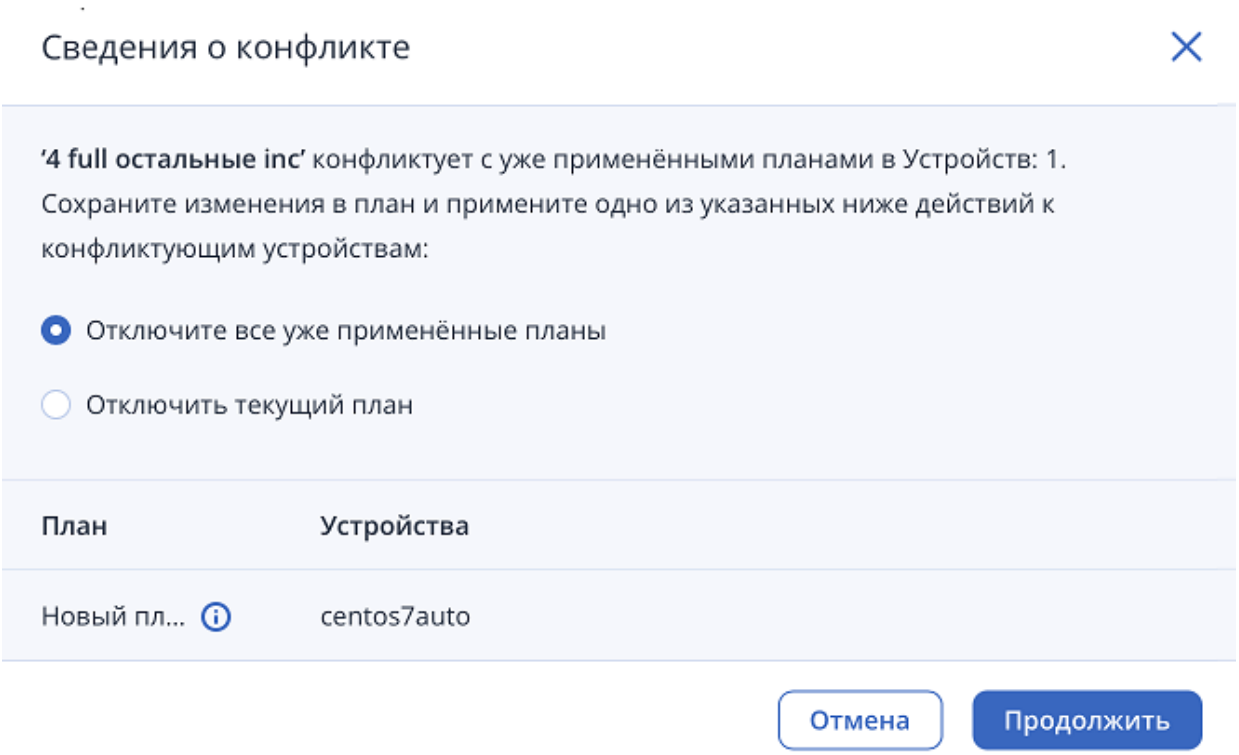
Разрешение конфликтов плана

План конфликтует с уже примененными планами

При создании нового плана на устройстве или устройствах с уже примененными планами, которые конфликтуют с новым планом, можно разрешить конфликт одним из указанных ниже способов.

При попытке сохранить план Кибер Бэкап предложит следующие варианты:

- Создать новый план, применить его и отключить все примененные ранее конфликтующие планы.
- Отключить созданный план.



При редактировании плана на устройстве или устройствах с уже примененными другими планами, которые конфликтуют с внесенными изменениями, можно разрешить конфликт одним из способов:

- Сохранить изменения, внесенные в редактируемый план, и отключить все уже примененные ранее конфликтующие планы.
- Отключить редактируемый план с внесенными изменениями.

План устройства конфликтует с планом группы

При попытке назначить новый план устройству из группы устройств с назначенным планом группы, система потребует разрешить конфликт посредством одного из следующих действий:

- Удаление устройства из группы и применение нового плана к устройству.
- Применение нового плана ко всей группе или изменение текущего плана группы.

Проблемы с лицензией

Назначенная лицензия на устройстве должна обеспечивать выполнение, обновление и применение плана защиты. Чтобы разрешить проблему с лицензией, выполните одно из действий:

- Отключите модули, которые не поддерживаются назначенной лицензией, и продолжите использовать план защиты.
- Измените назначенную лицензию вручную: откройте раздел **Устройства** → **'конкретное устройство'**

→ **Сведения** → **Лицензия**. После этого отзовите существующую лицензию и назначьте новую.

Операции с планами защиты

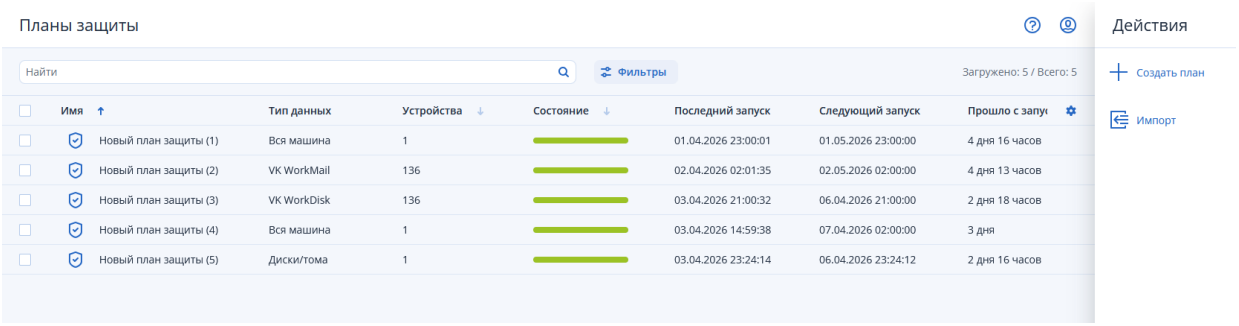
Доступные действия с планами защиты

Действия с планами доступны на вкладке **Планы** основного меню веб-консоли.

> **Важно**
>
> Вкладка **Планы** доступна при использовании расширенной редакции лицензии продукта. Подробнее о лицензиях см. в разделе *Издания и лицензии Кибер Бэкап*.

Для просмотра возможных действий с планами выполните следующее:

1. Откройте веб-консоль.
2. Перейдите на вкладку **Планы** → **Защита** для просмотра списка планов.

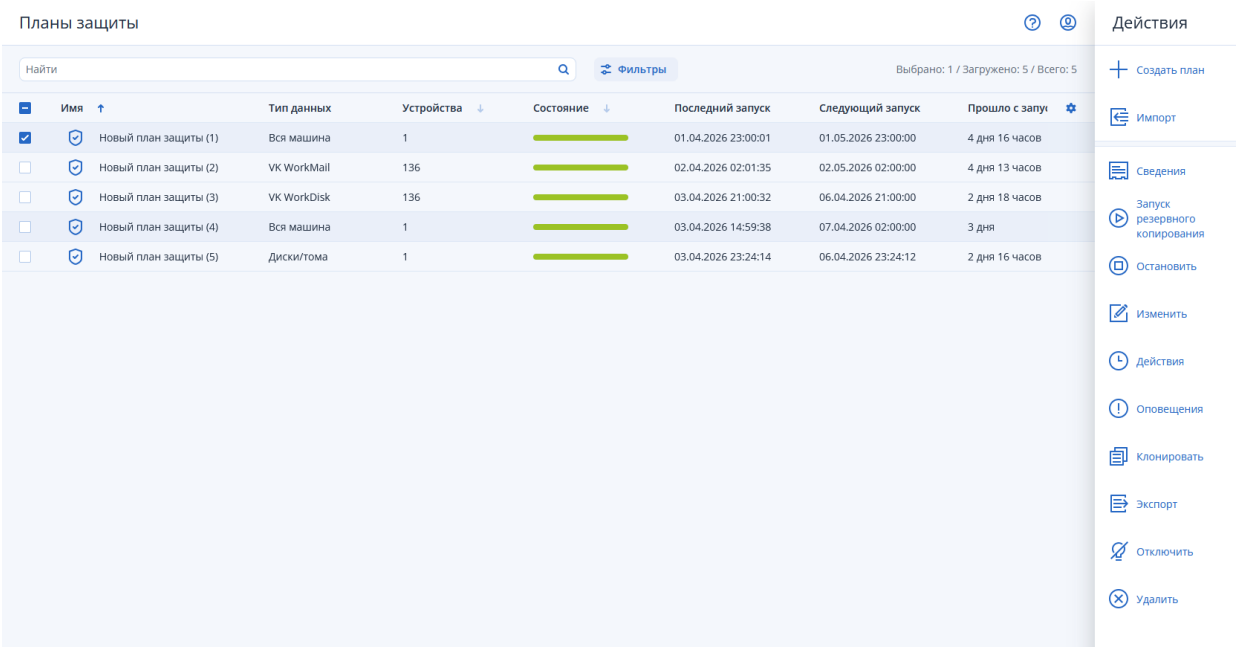


   Список планов можно сортировать по столбцам **Имя**, **Устройства**, **Состояние** и **Отдел**. Кроме того, список можно фильтровать по названию плана или его части (указав его в строке поиска), а также по типу защищаемых данных, состоянию плана и используемым хранилищам (нажав **Фильтры**, выбрав необходимые параметры и нажав **Применить**).

   Справа отображается меню действий с планами. Без выбора плана из этого меню вы можете:

   - создать план;
   - импортировать план.

3. Отметьте план в списке по вашему выбору. Справа в меню появится список действий с выбранным планом.



С выбранным планом можно выполнить указанные ниже действия:

- просмотреть сведения о плане;
- запустить резервное копирование по требованию;
- остановить выполнение плана;
- изменить план;
- применить план к устройствам или группе устройств;
- отозвать план с устройства;
- просмотреть журнал действий с планом;
- просмотреть оповещения, связанные с планом;
- клонировать план;
- экспортировать план;
- включить или отключить план;
- удалить план.

Примечание

Одно и то же действие с планами может быть доступно из разных вкладок меню действий с планами.

Примечание

Ряд действий с планами доступен также из вкладки **Устройства** основного меню веб-консоли.

Создание плана

Информацию о создании плана защиты см. в разделе *Создание плана защиты*.

Импорт плана

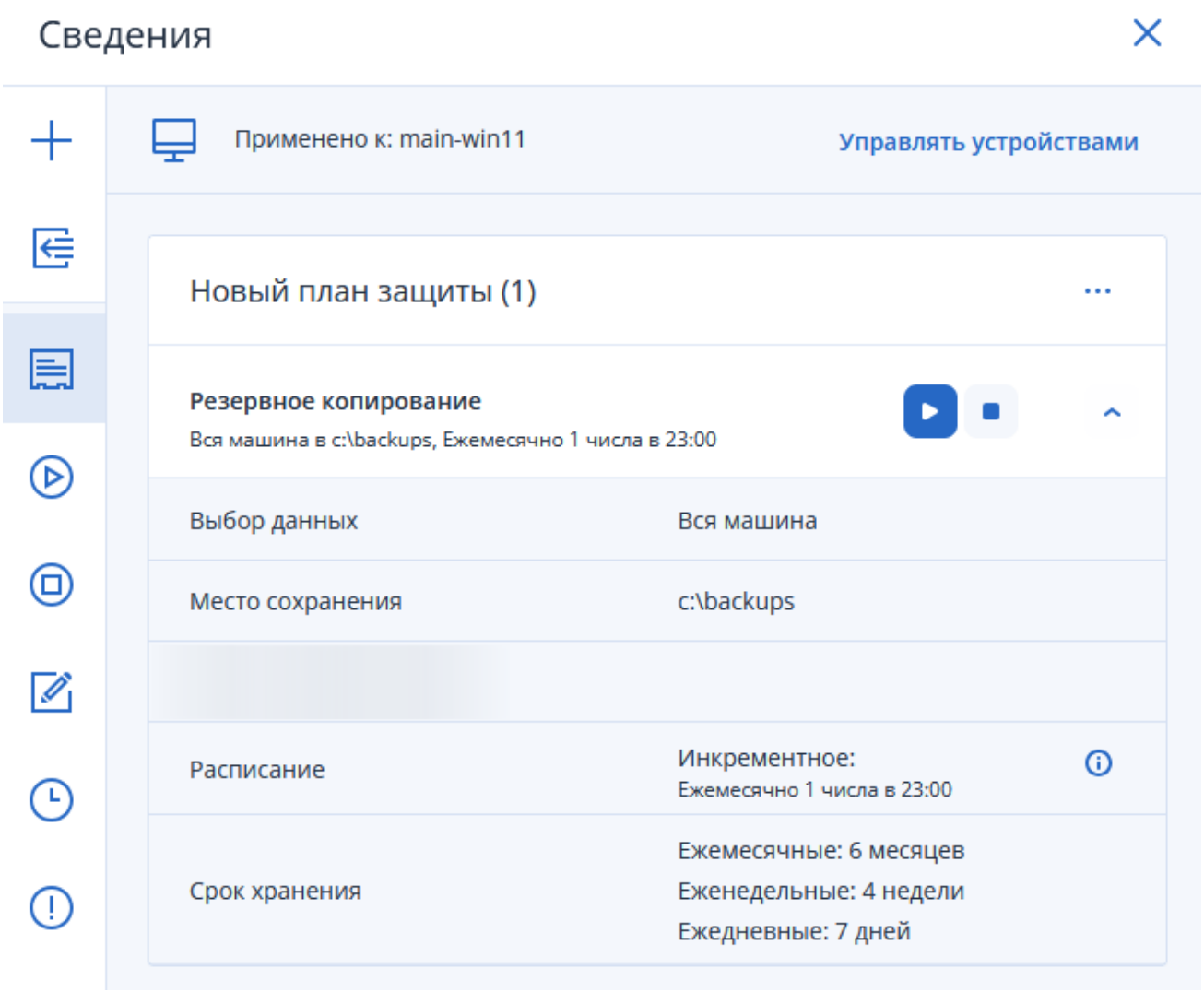
1. Щёлкните **Импорт** в меню действий с планом.
2. Выберите файл с планом и нажмите **Открыть**. План будет добавлен в список планов.

Примечание

Импортировать можно только те планы защиты, которые созданы в Кибер Бэкап 15 и более поздних версиях.

Просмотр сведений о плане

Для просмотра сведений о плане щёлкните **Сведения** в меню справа. Отобразится вкладка сведений о плане.



Запуск резервного копирования по требованию

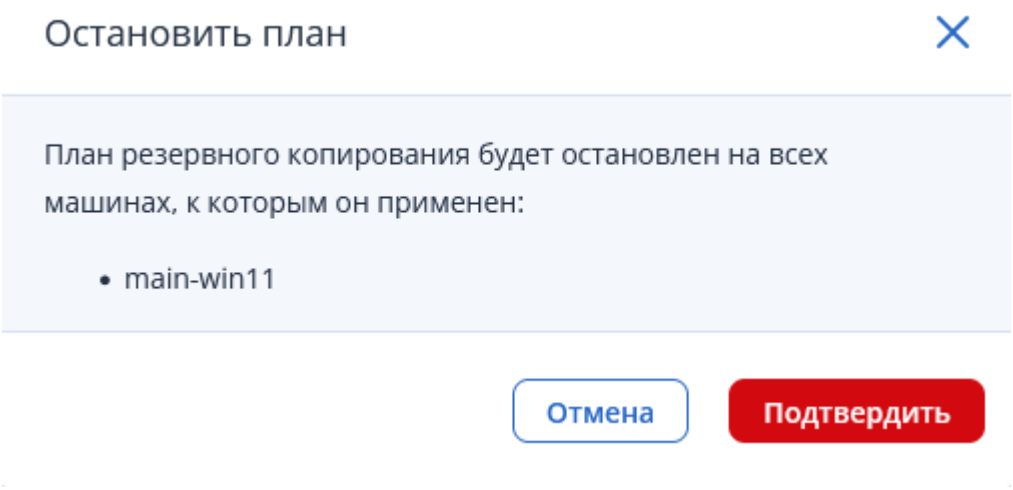
Запуск резервного копирования по требованию описан в разделе *Запуск резервного копирования вручную*.

Остановка выполнения плана

Для отмены выполняющегося резервного копирования остановите выполнение плана. Остановку выполнения плана можно произвести любым из следующих способов.

Остановка выполнения плана из меню действий с планом

1. Щёлкните **Остановить** в меню действий с планом. Откроется окно подтверждения.



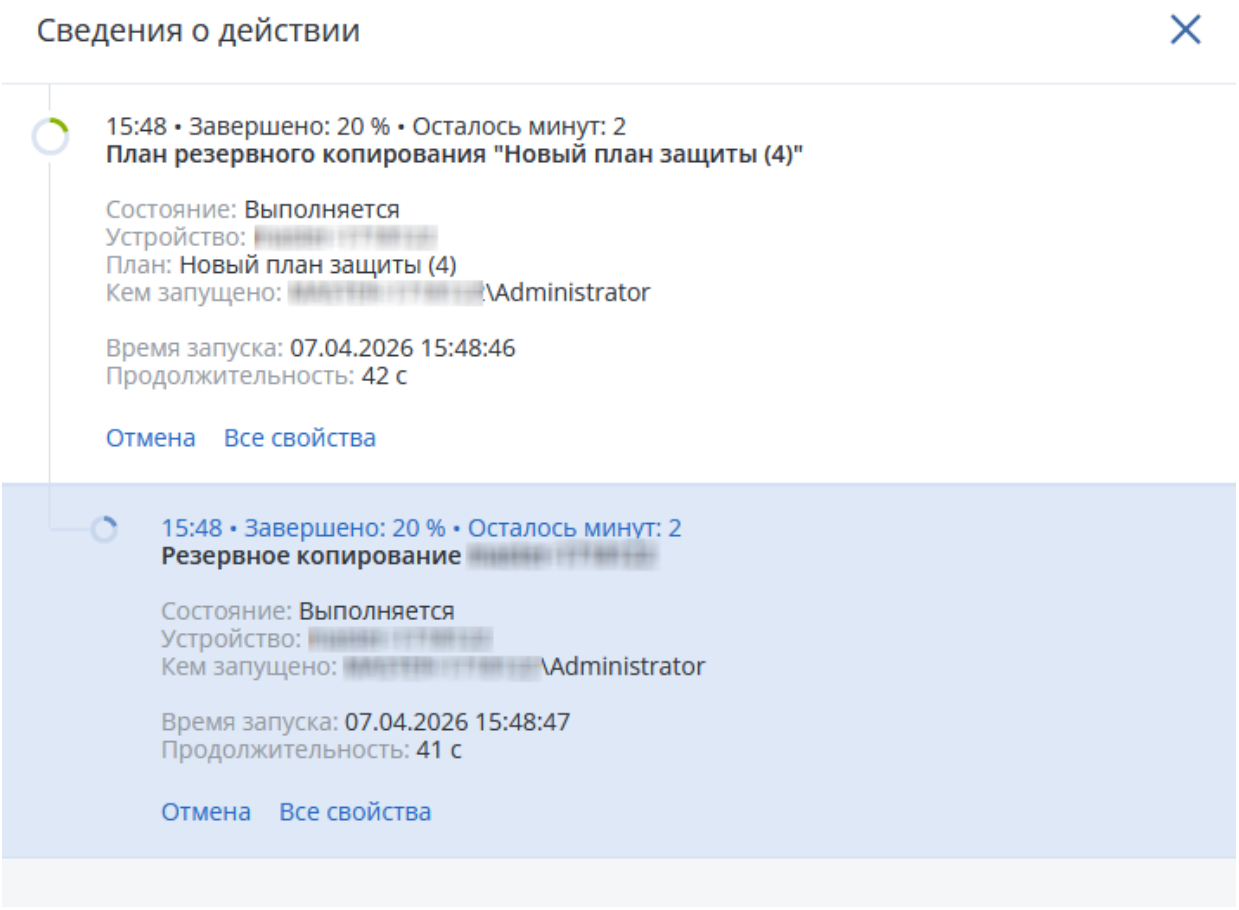
2. Нажмите **Подтвердить**. План будет остановлен.

Остановка выполнения плана из вкладки ”Сведения”

1. В меню действий с планом щёлкните **Сведения**.
2. Нажмите на значок остановки плана.
3. Нажмите **Подтвердить** в окне подтверждения. План будет остановлен.

Остановка выполнения плана из меню ”Устройства”

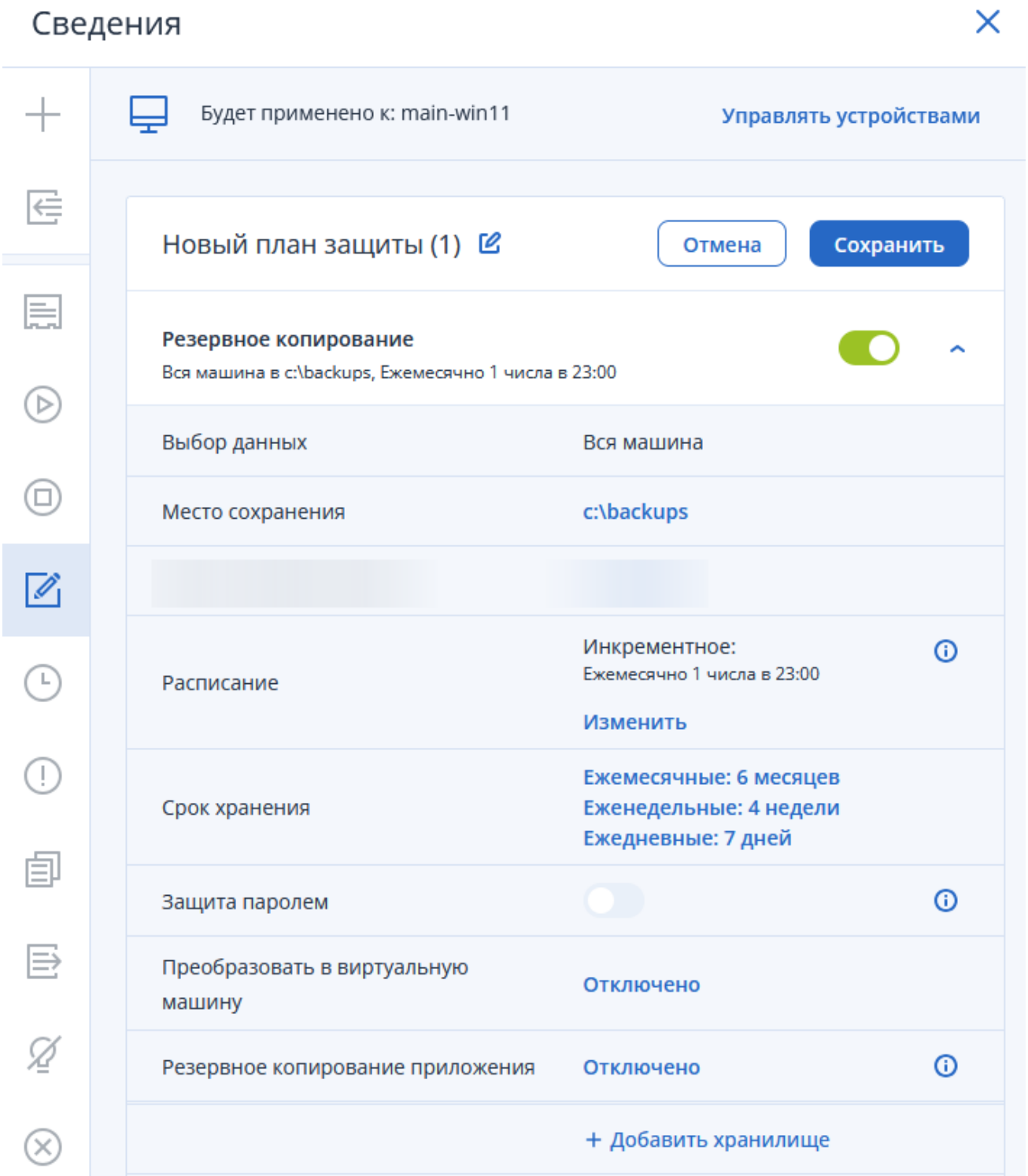
1. Перейдите в меню **Устройства**.
2. Отметьте в списке машину с выполняющимся планом и нажмите в меню справа **Действия**.
3. В списке действий выберите требуемое и нажмите **Отмена**.



План будет остановлен и появится сообщение об отмене операции.

Изменение плана

Щёлкните **Изменить** в меню действий с планом. Откроется вкладка с параметрами плана.



На вкладке можно сделать в т. ч. следующие изменения:

- переименовать план;
- изменить место сохранения резервных копий;
- изменить расписание выполнения плана;

- изменить срок хранения резервных копий;
- изменить дополнительные параметры резервного копирования.

Или (через вкладку **Устройства**):

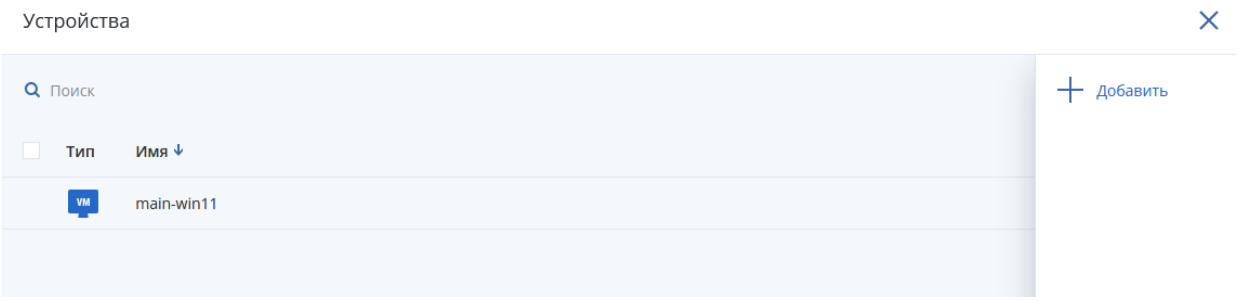
1. Чтобы изменить план защиты для всех машин, к которым он применен, выберите одну из них. В противном случае выберите машины, для которых необходимо изменить план защиты.
2. Щёлкните **Защитить**.
3. Выберите план защиты, который необходимо изменить.
4. Щёлкните значок многоточия рядом с именем плана резервного копирования и выберите команду **Изменить**.
5. Чтобы изменить параметры плана защиты, щёлкните соответствующий раздел на его панели.
6. Щёлкните **Сохранить изменения**.
7. Чтобы изменить план защиты для всех машин, к которым он применен, щёлкните **Применить изменения к этому плану защиты**. Или щёлкните **Создать новый план защиты только для выбранных устройств**.

Переименование плана

1. Щёлкните **Изменить** в меню действий с планом. Откроется вкладка с параметрами плана.
2. Нажмите на значок редактирования рядом с наименованием плана.
3. Введите в открывшемся окне новое наименование плана и нажмите **Продолжить**. План будет сохранен под новым именем.

Применение плана к устройству или группе устройств

1. В списке планов отметьте план, который вы хотите применить к устройству или устройствам.
2. В меню действий с планом щёлкните **Изменить**.
3. Во вкладке параметров плана нажмите **Управлять устройствами**.



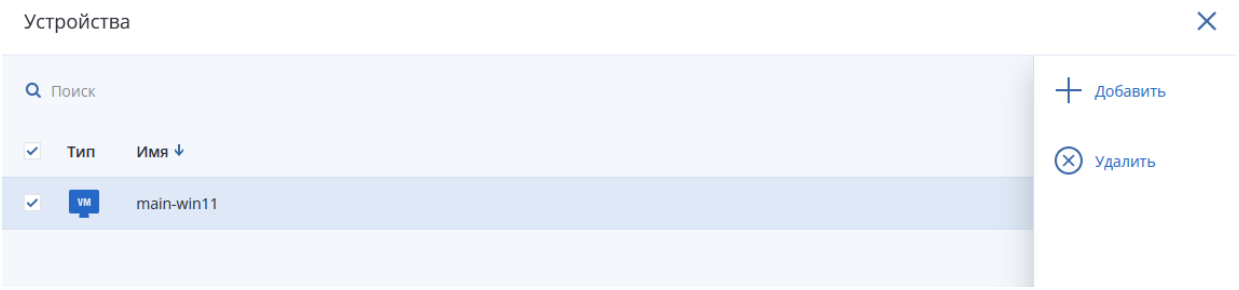
4. Нажмите **Добавить**.
5. В списке устройств отметьте одно или несколько устройств, к которым требуется применить план.
6. Щёлкните **Добавить** и затем **Готово**.

Или (через вкладку **Устройства**):

1. Выберите машины, для которых нужно обеспечить защиту.
2. Щёлкните **Защитить**. Если план защиты уже применен к выбранным машинам, щёлкните **Добавить план**.
3. В программе отображаются ранее созданные планы защиты.
4. Выберите необходимую защиту и щёлкните **Применить**.

Отзыв плана с устройства

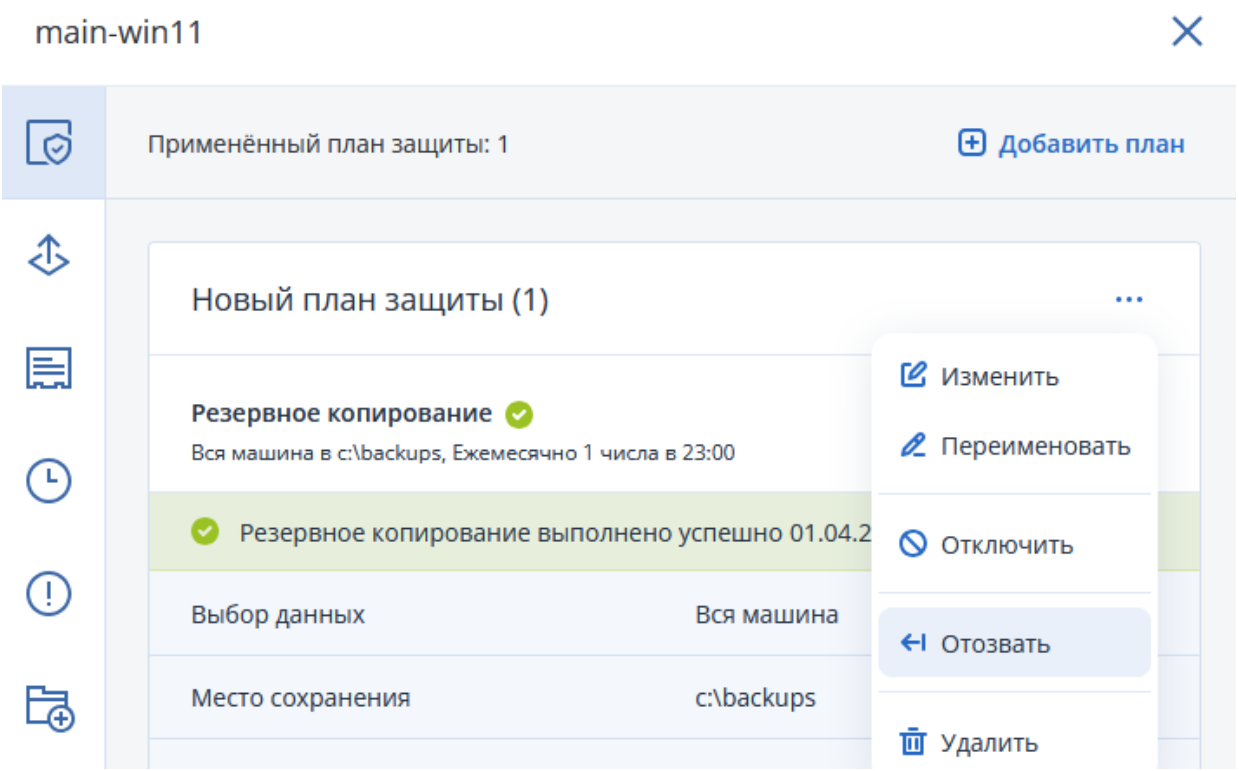
1. В списке планов отметьте план, который вы хотите отозвать с устройства.
2. В меню действий с планом щёлкните **Изменить**.
3. На вкладке **Изменить** нажмите **Управлять устройствами**. Появится список устройств, к которым применен план.
4. В списке устройств отметьте устройство, с которого хотите отозвать план.



5. Щёлкните **Удалить** и затем **Готово**.
6. Нажмите **Сохранить** для сохранения изменений.

Или (через вкладку **Устройства**):

1. Выберите машины, для которых нужно отозвать план защиты.
2. Щёлкните **Защитить**.
3. Если для машин применено несколько планов защиты, выберите тот из них, который необходимо отозвать.
4. Щёлкните значок многоточия рядом с именем плана защиты и выберите команду **Отозвать**.



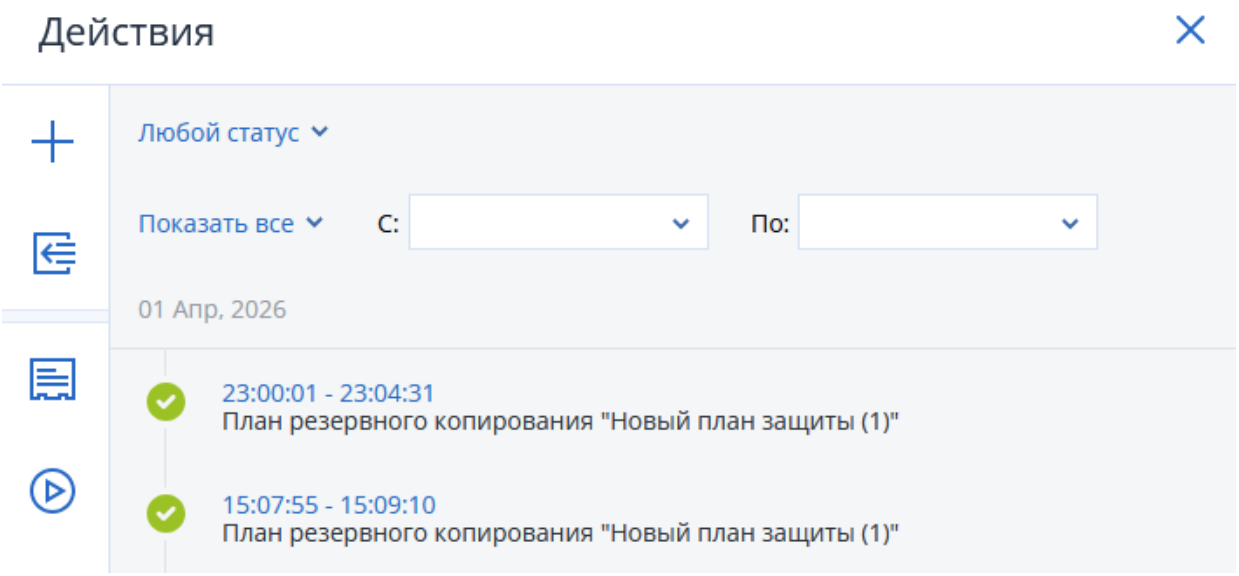
Отозванный план больше не применяется к устройствам.

Это действие удобно для администраторов, которым не нужно быстро защитить то же самое устройство тем же планом защиты. Для восстановления защиты, которая обеспечивалась отозванным планом, администратор должен знать имя этого плана, выбрать его из списка доступных планов, а затем заново применить план к желаемому устройству.

Просмотр журнала действий с планом

Для просмотра журнала действий с выбранным планом резервного копирования выполните следующие шаги:

1. Щёлкните **Действия** в меню действий с планом. В результате будет отображён список всех действий с планом.



2. Для просмотра более детальной информации нажмите на выбранную запись о действии. После этого будет открыто окно **Сведения о действии**, в котором будут отображены детальные данные.

Примечание

Записи о действиях, связанных с планами защиты, также отображаются во вкладке **Панель мониторинга** → **Действия** (см. подробнее раздел *Панель мониторинга "Действия"*).

Доступна фильтрация записей о действиях:

- по статусу;
- по временному интервалу.

Для фильтрации записей о действиях с планом по статусу нажмите **Любой статус** и в выпадающем списке выберите один из вариантов:

- любой статус;
- выполняется;
- выполнено с предупреждениями;
- успешно;
- с ошибками.

Для фильтрации записей о действиях с планом по временному интервалу можно:

- выбрать произвольные даты диапазона в полях **С** и **По**;
- нажать **Другой период** и в выпадающем списке выбрать один из вариантов:

- показать все;
- последние 24 часа;
- предыдущая неделя;
- предыдущий месяц.

В случае отсутствия записей в соответствии с примененным фильтром будет отображено сообщение ”Нет действий”.

Для снятия фильтра нажмите на значок крестика в полях **С** и **По**.

Оповещения

Для просмотра оповещений, связанных с выбранным планом защиты, щёлкните **Оповещения** в меню действий с планом. В результате будут отображены оповещения (при их наличии) или сообщение ”Нет оповещений” (при их отсутствии).

Для удаления выбранного оповещения нажмите **Очистить** в области соответствующего оповещения. Для удаления всех оповещений по выбранному плану защиты нажмите **Очистить все**.

Примечание

Оповещения, связанные с планами защиты, также отображаются во вкладке **Панель мониторинга** → **Оповещения** (см. подробнее раздел *Панель мониторинга ”Оповещения”*).

Важно

При удалении оповещений в меню действий с планом защиты они также удаляются и из оповещений во вкладке **Панель мониторинга**.

Клонирование плана

Клонирование плана позволяет быстро перенести параметры плана на другое устройство по вашему выбору.

1. В списке планов отметьте план, который вы хотите клонировать для другого устройства.
2. Щёлкните **Клонирование** в меню действий с планом. Откроется вкладка создания плана защиты с выбором устройства.
3. Нажмите **Добавить устройство**.
4. Выберите устройство из списка и нажмите **Добавить**.

5. Назначьте имя плану и нажмите **Сохранить**. План с действующими параметрами будет применен к выбранному устройству.

Экспорт плана

Экспорт плана позволяет сохранить план в файл в формате JSON.

1. Щёлкните **Экспорт** в меню действий с планом.
2. Введите имя файла и нажмите **Сохранить**. План вместе с параметрами будет сохранен в файл.

Включение / отключение плана

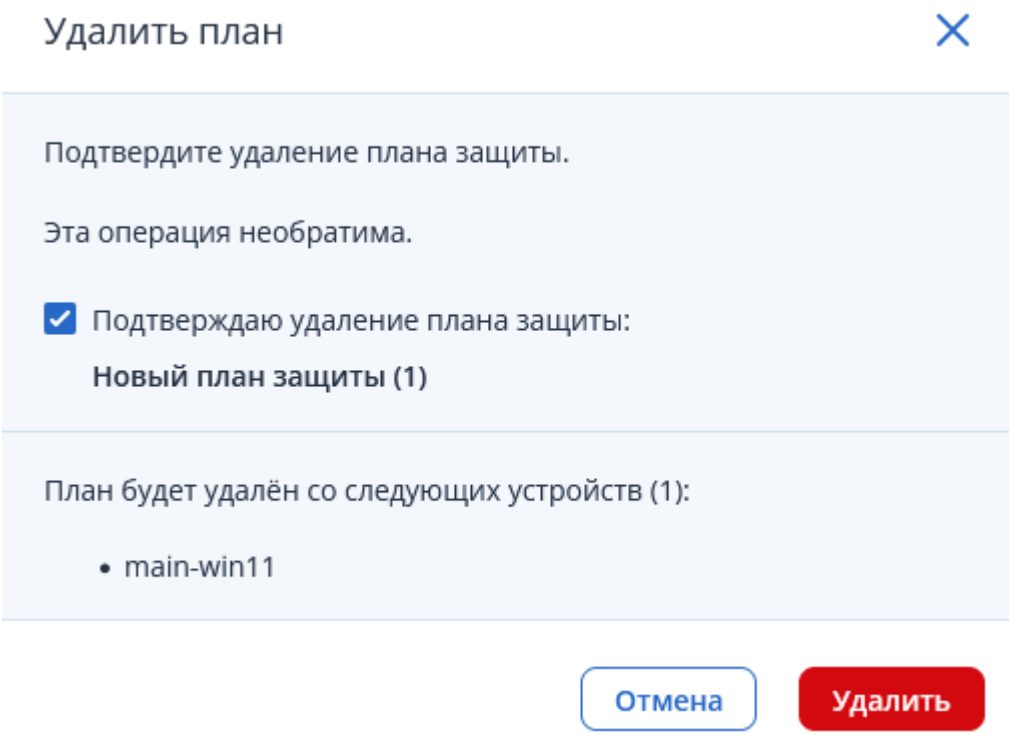
Нажмите **Включить** или **Отключить** в меню действий с планом. Сразу после нажатия совершится выбранное действие.

Отключенный план не будет выполняться на устройстве, к которому он применен.

Это действие удобно для администраторов, которые планируют защитить то же самое устройство тем же планом защиты позже. Поскольку план не отзывается с устройства, для восстановления защиты администратору необходимо только заново включить план.

Удаление плана

1. Щёлкните **Удалить** в меню действий с планом.
2. В открывшемся окне подтвердите удаление плана, отметив поле подтверждения.



3. Нажмите **Удалить**. План будет удален из списка планов.

Или (через вкладку **Устройства**):

1. Выберите любую машину, для которой применен план защиты, который необходимо удалить.
2. Щёлкните **Защитить**.
3. Если для машины применено несколько планов защиты, выберите тот из них, который необходимо удалить.
4. Щёлкните значок многоточия рядом с именем плана защиты и выберите команду **Удалить**.
5. В результате план защиты будет отозван для всех машин и полностью удален из веб-интерфейса.

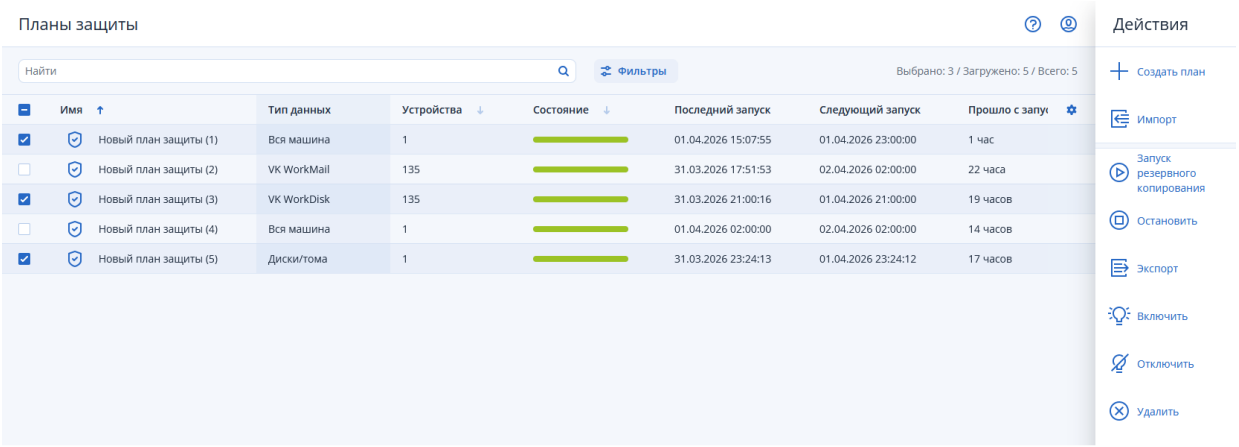
Групповые действия с планами

Начиная с версии 18.5, в Кибер Бэкап доступны групповые действия с планами защиты.

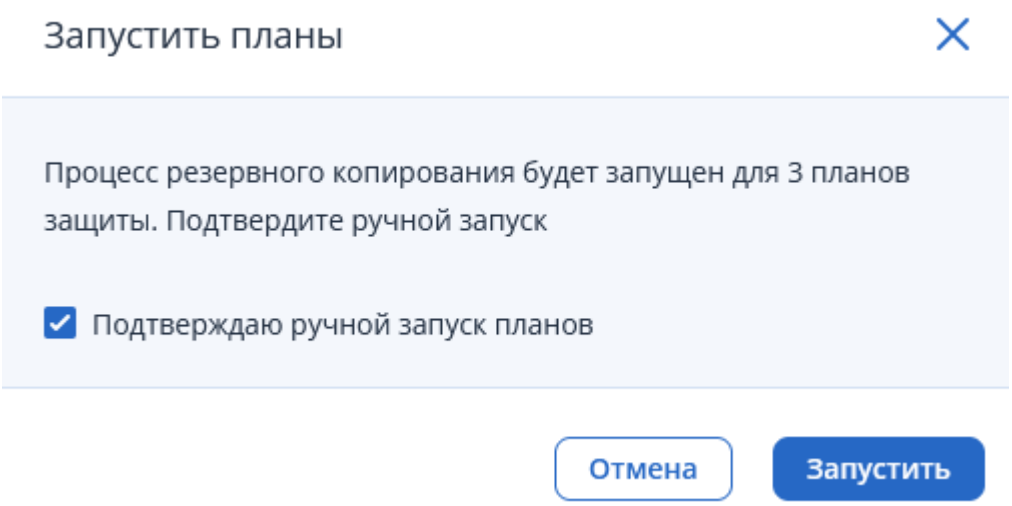
Важно

Перед выполнением групповых действий с планами защиты убедитесь, что включено одновременное резервное копирование (подробнее см. раздел *Одновременное резервное копирование*).

1. Отметьте в списке планов защиты нужные планы.



2. В меню справа выберите действие, которое необходимо совершить с выбранными планами, и щёлкните его.
3. В открывшемся окне подтвердите выбранное действие.



4. Дождитесь окончания операции.

Примечание

Одновременный запуск большого количества планов может приводить к снижению производительности резервного копирования. Во избежание этого запускайте планы небольшими группами.

Обзор групповых действий с планами доступен на вкладке **Панель мониторинга** → **Действия**.

Активная защита (Active Protection)

Active Protection — это отдельный модуль в *плане защиты*, который отслеживает процессы, запущенные на защищённом компьютере. Когда процесс сторонней программы пытается шифровать файлы или запускает математические вычисления в фоновом режиме, похищая вычислительную мощность и увеличивая сетевой трафик, Active Protection создаёт оповещение и выполняет дополнительные действия в соответствии с заданными настройками.

Также Active Protection предотвращает неавторизованные изменения собственных процессов, записей реестра, исполняемых и конфигурационных файлов и резервных копий, расположенных в локальных папках.

Для распознавания вредоносных процессов Active Protection использует поведенческий анализ. Active Protection сравнивает цепочку действий, выполняемых процессом, с цепочками событий, записанных в базе данных шаблонов вредоносного поведения. Такой подход позволяет обнаруживать новые вредоносные программы по их типичному поведению.

Служба Active Protection доступна для машин с ОС Windows (подробнее см. в разделе *Активная защита (Active Protection) для Windows*) и с ОС Linux (подробнее см. в разделе *Активная защита (Active Protection) для Linux*).

Примечание

Для использования службы Active Protection на машине — источнике данных должен быть установлен агент для Windows или для Linux. В случае отсутствия на ней агента для Windows или для Linux или при резервном копировании виртуальной машины в безагентном режиме служба Active Protection должна оставаться выключенной в настройках плана защиты.

Возможности службы Active Protection в зависимости от установленной на машине операционной системы приведены в таблице.

Функция	Машина с ОС Windows	Машина с ОС Linux
Действие при обнаружении	+	+
Исключения	+	+
Выявление процессов майнинга криптовалют	+	—
Самозащита	+	—
Защита сетевых папок	+	—
Защита на стороне сервера (внешняя защита сетевых папок)	+	—

Технические требования и ограничения службы Active Protection

Active Protection для Windows

Служба Active Protection доступна для машин с операционными системами, подерживаемыми агентом для Windows (см. раздел *Поддерживаемые операционные системы*).

На машине должен быть установлен агент для Windows.

Active Protection для Linux

Служба Active Protection доступна во всех операционных системах, поддерживающих агент для Linux (см. раздел *Поддерживаемые операционные системы*), с учётом следующих требований и ограничений:

- Ядро Linux должно поддерживать установку драйвера file_protection_linux.
- Ядра Linux новее версии 4.9 должны поддерживать технологию трассировки ftrace (Function Tracer).
- Не поддерживается совместная работа модуля с ПО Kaspersky Endpoint Security для Linux. Если включен модуль, блокируется установка Kaspersky Endpoint Security для Linux. Если включено ПО Kaspersky Endpoint Security для Linux, блокируется работа модуля.
- Не поддерживается работа модуля в ОС Astra Linux 1.7.x с ядром версии 6.1.90, а также ОС Astra Linux 1.8.x с ядрами версий 6.1.90, 6.6.28.
- Не поддерживается работа модуля в ОС Debian, Ubuntu, Astra Linux с защищёнными (hardened) ядрами.

На машине должен быть установлен агент для Linux.

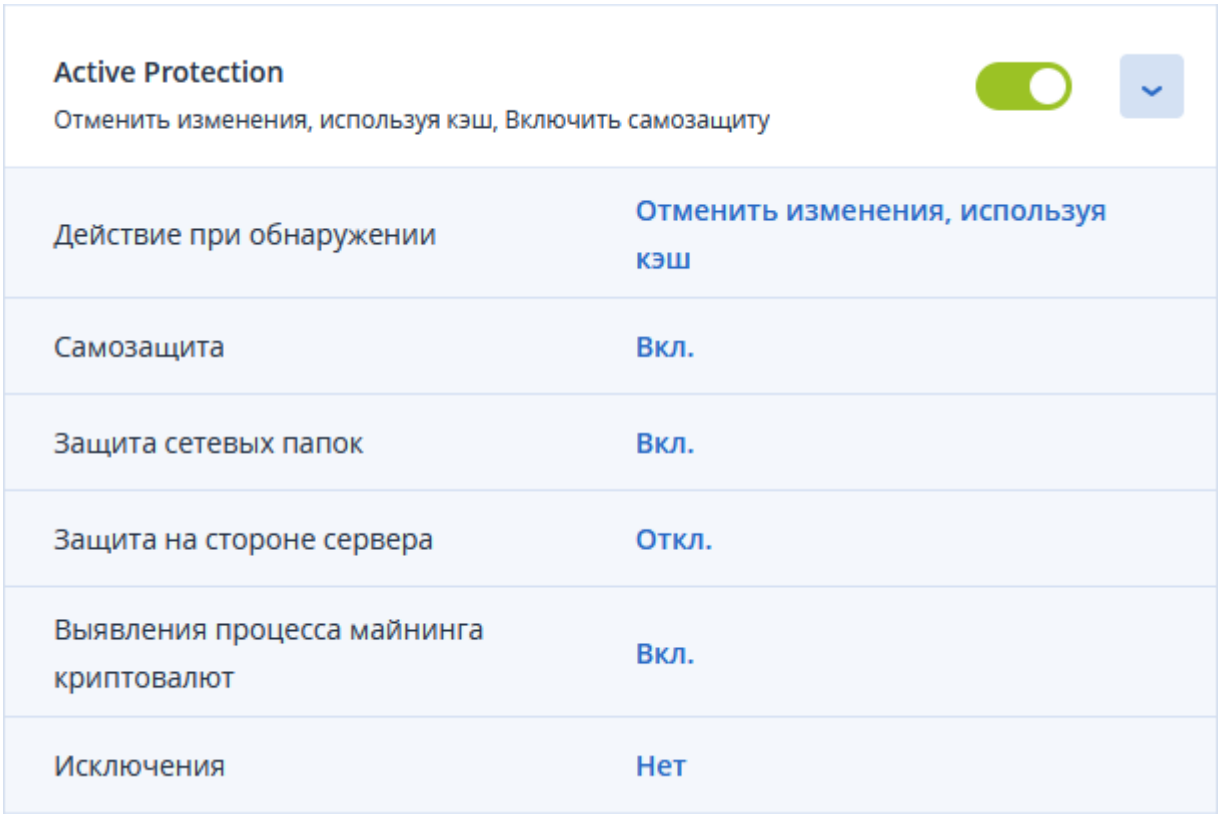
Активная защита (Active Protection) для Windows

На машине с ОС Windows служба Active Protection обеспечивает защиту компьютера от вредоносных программ и имеет следующие настройки:

- **Действие при обнаружении**;
- **Самозащита**;
- **Защита сетевых папок**;
- **Защита на стороне сервера**;
- **Выявления процессов майнинга криптовалют**;
- **Исключения**.

По умолчанию служба Active Protection выключена. Чтобы активировать её, в веб-консоли Кибер Бэкап перейдите на вкладку **Планы** → **Защита**, выберите план защиты из списка и на панели **Действия** щёлкните **Изменить** (либо создайте новый план защиты, подробнее см. раздел *Операции с планами защиты*), затем переведите соответствующий переключатель в положение **Включено**.

Для перехода к настройкам параметров службы Active Protection нажмите на стрелку справа от переключателя. Вид окна настроек службы Active Protection на машине с ОС Windows приведён на рисунке.



Действие при обнаружении

Параметр **Действие при обнаружении** определяет действие, которое будет выполняться при обнаружении подозрительной активности.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Действие при обнаружении**.
2. Выберите действие:
   - **Только уведомить** — программа создаст оповещение о процессе.
   - **Остановить процесс** — программа создаст оповещение о процессе и остановит процесс.
   - **Отменить изменения, используя кэш** (значение по умолчанию) — программа создаст оповещение, остановит процесс и отменит внесённые в файл изменения, используя кэш

службы.

3. Для сохранения выбранной настройки нажмите **Готово**.

Самозащита

Параметр **Самозащита** предотвращает несанкционированные изменения в собственных процессах программного обеспечения, записях реестра, исполняемых и конфигурационных файлах и резервных копиях, расположенных в локальных папках.

> **Примечание**
>
> Значение по умолчанию: **Вкл.** (включено). Отключение параметра **Самозащита** не рекомендуется.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Самозащита**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. [Необязательно] Установите флажок **Разрешить определённым процессам изменять резервные копии**.

   Нажмите **Добавить** и укажите процессы, которым разрешено изменять файлы резервных копий, даже если эти файлы защищены системой самозащиты. Это полезно, например, при удалении файлов резервных копий или перемещении их в другое место с помощью скрипта.

   Если функция **Разрешить определённым процессам изменять резервные копии** отключена, файлы резервных копий могут быть изменены только процессами, подписанными поставщиком программного обеспечения для резервного копирования. Это позволяет программному обеспечению применять правила хранения и удалять резервные копии, когда пользователь запрашивает это через веб-интерфейс. Другие процессы, независимо от того, подозрительные они или нет, не могут изменять резервные копии.

   Эта возможность относится к файлам резервных копий, которые имеют расширения .tibx, .tib, .tia и расположены в локальных папках.

4. Для сохранения настроек нажмите **Готово**.

Защита сетевых папок

Параметр **Защита сетевых папок** позволяет защитить сетевые папки, назначенные как локальные диски, от локальных вредоносных процессов.

Этот параметр применяется к папкам, к которым предоставляется общий доступ по протоколам SMB

или NFS.

Если файл изначально был расположен на подключённом диске, он не может быть сохранён в исходное местоположение при извлечении из кэша с помощью действия **Отменить изменения, используя кэш**. Вместо этого он будет сохранён в папку, указанную в настройках параметра.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Защита сетевых папок**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. [Необязательно] Укажите адрес локальной папки для сохранения восстановленных файлов. Если указанная папка не существует, она будет создана.

   > **Примечание**
   >
   > Сетевые папки, включая папки на подключённых дисках, не поддерживаются.

4. Для сохранения настроек нажмите **Готово**.

Значение по умолчанию: **Вкл.** (включено).

Защита на стороне сервера (внешняя защита сетевых папок)

Параметр **Защита на стороне сервера** определяет, будут ли защищены сетевые папки, к которым предоставлен общий доступ, от внешних входящих подключений с других серверов в сети, которые потенциально могут представлять угрозы.

Значение по умолчанию: **Откл.** (отключено).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Защита на стороне сервера**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. [Необязательно] щёлкните по вкладке **Доверенные**, нажмите **Добавить** и укажите имя пользователя и IP-адрес для подключения, которому разрешено изменять любые данные.
4. [Необязательно] щёлкните по вкладке **Заблокировано**, нажмите **Добавить** и укажите имя пользователя и IP-адрес для подключения, которому не разрешено изменять никакие данные.
5. Для сохранения настроек нажмите **Готово**.

Выявление процессов майнинга криптовалют

Параметр **Выявление процессов майнинга криптовалют** позволяет обнаруживать вредоносное программное обеспечение для майнинга криптовалют, снижающее производительность полезных приложений и увеличивающее потребление электроэнергии, что в результате может привести к сбоям системы и даже повреждению оборудования. Рекомендуется добавить вредоносные программы для майнинга в список вредоносных процессов для предотвращения их запуска.

Значение по умолчанию: **Откл.** (отключено).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Выявление процессов майнинга криптовалют**.
2. При необходимости переведите переключатель в положение **Вкл.** (включено).
3. Выберите действие, которое будет выполняться при обнаружении активности майнинга криптовалют:
    - **Только уведомить** — программа создаст оповещение о подозрительном процессе.
    - **Остановить процесс** — программа создаст оповещение и останавливает подозрительный процесс.
4. Для сохранения настроек нажмите **Готово**.

Исключения

Параметр **Исключения** позволяет свести к минимуму ресурсы, используемые для поведенческого анализа, и исключить так называемые ложные срабатывания, когда доверенная программа рассматривается как программа-вымогатель.

Данный параметр позволяет создать:

- список доверенных процессов, которые никогда не будут рассматриваться как вредоносные программы;
- список процессов, запуск которых всегда будет заблокирован, пока на компьютере включен модуль Active Protection.

> **Примечание**
>
> Процессы, подписанные корпорацией Майкрософт, всегда являются надёжными.

Значение по умолчанию: **Нет** (списки доверенных и заблокированных процессов пустые).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Исключения**.
2. [Необязательно] Щёлкните по вкладке **Доверенные** и укажите:
   - Полный путь к исполняемому файлу процесса, который никогда не будет рассматриваться как вредоносная программа.
   - Полный путь к папке, в которой не будут отслеживаться изменения файлов.
3. [Необязательно] Щёлкните по вкладке **Заблокировано** и укажите полный путь к исполняемому файлу процесса, который всегда будет заблокирован.
4. Для сохранения настроек нажмите **Готово**.

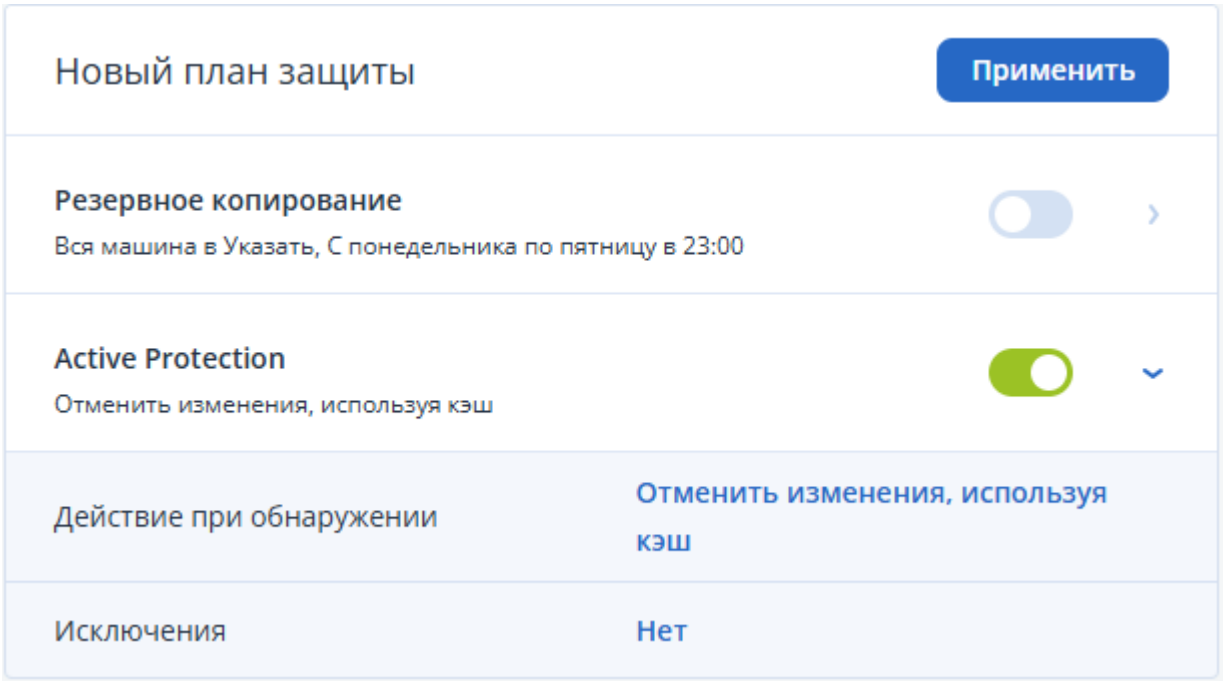
Активная защита (Active Protection) для Linux

На машине с ОС Linux служба Active Protection обеспечивает защиту компьютера от вредоносных программ и имеет следующие настройки:

- **Действие при обнаружении**;
- **Исключения**.

По умолчанию служба Active Protection выключена. Чтобы активировать её, в веб-консоли Кибер Бэкап перейдите на вкладку **Планы** → **Защита**, выберите план защиты из списка и на панели **Действия** щёлкните **Изменить** (либо создайте новый план защиты, подробнее см. раздел *Операции с планами защиты*), затем переведите соответствующий переключатель в положение **Включено**.

Для перехода к настройкам параметров службы Active Protection нажмите на стрелку справа от переключателя. Вид окна настроек службы Active Protection на машине с ОС Linux приведён на рисунке.



Действие при обнаружении

Параметр **Действие при обнаружении** определяет действие, которое будет выполняться при обнаружении подозрительной активности.

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Действие при обнаружении**.
2. Выберите действие:
   - **Только уведомить** — программа создаст оповещение о процессе.
   - **Остановить процесс** — программа создаст оповещение о процессе и остановит процесс.
   - **Отменить изменения, используя кэш** (значение по умолчанию) — программа создаст оповещение, остановит процесс и отменит внесённые в файл изменения, используя кэш службы.
3. Для сохранения выбранной настройки нажмите **Готово**.

Исключения

Параметр **Исключения** позволяет свести к минимуму ресурсы, используемые для поведенческого анализа, и исключить так называемые ложные срабатывания, когда доверенная программа рассматривается как программа-вымогатель.

Данный параметр позволяет создать:

- список доверенных процессов, которые никогда не будут рассматриваться как вредоносные программы;
- список процессов, запуск которых всегда будет заблокирован, пока на компьютере включен модуль Active Protection.

Значение по умолчанию: **Нет** (списки доверенных и заблокированных процессов пустые).

Для настройки параметра выполните следующие действия:

1. Щёлкните в области строки **Исключения**.
2. [Необязательно] Щёлкните по вкладке **Доверенные** и укажите:
    - Полный путь к исполняемому файлу процесса, который никогда не будет рассматриваться как вредоносная программа.
    - Полный путь к папке, в которой не будут отслеживаться изменения файлов.
3. [Необязательно] Щёлкните по вкладке **Заблокировано** и укажите полный путь к исполняемому файлу процесса, который всегда будет заблокирован.
4. Для сохранения настроек нажмите **Готово**.

Группы устройств

Группы устройств призваны обеспечить простое управление большим количеством зарегистрированных устройств.

Вы можете применить план защиты к группе. После появления нового устройства в группе, это устройство будет защищено планом. Если устройство удалено из группы, оно больше не будет защищено планом. Если план применим к группе, нельзя отменить его применение к одному из членов группы, только ко всей группе.

В группу могут быть добавлены устройства только одного типа. Например в **Hyper-V** вы можете создать группу виртуальных машин Hyper-V. В разделе **Машины с агентами** можно создать группу машин с установленными агентами. В разделе **Физические и виртуальные машины** невозможно создать группу.

Одно устройство может входить в несколько групп.

Встроенные группы

После регистрации устройства оно появляется в одной из встроенных корневых групп на вкладке **Устройства**.

Корневые группы *невозможно* редактировать или удалить. *Невозможно* применить план к корневым группам.

Некоторые корневые группы содержат встроенные подкорневые группы. Такие группы *невозможно* редактировать или удалить. Однако *возможно* применить планы к подкорневым встроенным группам.

Пользовательские группы

Защита всех устройств во встроенной группе с помощью одного плана защиты может быть неудовлетворительной из-за разных ролей машин. У каждого отдела есть свои данные для резервного копирования. Для некоторых данных резервные копии требуется создавать часто, тогда как для других — пару раз в год. Поэтому может потребоваться создать различные планы защиты, применяющиеся на разных группах машин. В этом случае следует рассмотреть возможность создания пользовательских групп.

Пользовательская группа может включать одну или несколько вложенных групп. Любую пользовательскую группу можно изменить или удалить. Существует несколько типов пользовательских групп.

- **Статические группы**

Статические группы содержат машины, добавленные вручную. Состав статической группы меняется, только если вы специально добавите или удалите машину.

Пример: Вы создали пользовательскую группу для отдела бухгалтерии и вручную добавили в группу машины бухгалтеров. Когда к этой группе будет применен план защиты, машины сотрудников бухгалтерии будут защищены. Если в отдел пришел новый сотрудник, следует включить его машину в эту группу вручную.

- **Динамические группы**

  Динамические группы содержат машины, добавленные автоматически в соответствии с поисковыми критериями, определенными при создании группы. Состав динамической группы меняется автоматически. Машина остается в группе до тех пор, пока отвечает заданным критериям.

  Пример 1: Имена хостов машин, принадлежащих к отделу бухгалтерии, содержат слово ”бухгалтерия”. Достаточно задать часть имени машины в качестве критерия членства в группе и применить к этой группе план защиты. Машина нового бухгалтера добавляется в группу сразу после регистрации. Таким образом она будет автоматически защищена.

  Пример 2: Отдел бухгалтерии формирует отдельную организационную единицу Active Directory (OU). Укажите организационную единицу бухгалтерии как критерий членства в группе и примените к данной группе план защиты. Машина нового бухгалтера добавляется в группу сразу после регистрации и добавления к организационной единице независимо от того, какое действие выполняется первым. Таким образом она будет автоматически защищена.

Операции со статическими группами

Со статическими группами доступны следующие операции:

- создание (см. далее в этом разделе);
- добавление устройств в группы и удаление из них (см. далее в этом разделе);
- применение плана защиты к группе (подробнее см. в разделе *Применение плана защиты к группе*);
- переименование (подробнее см. в разделе *Переименование группы*);
- удаление (подробнее см. в разделе *Удаление группы*).

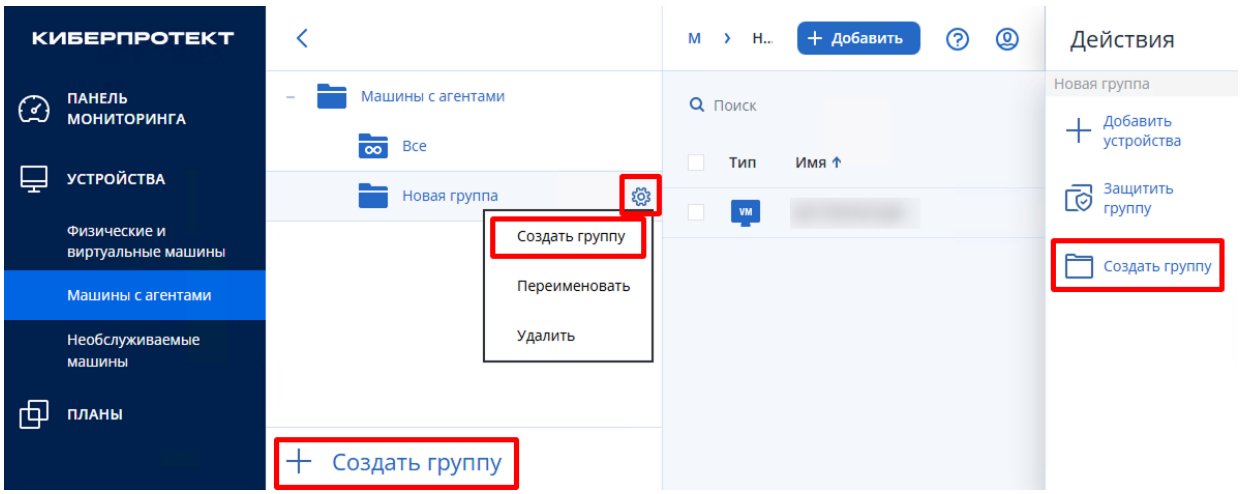
Создание статических групп

Для создания статической группы выполните следующие действия:

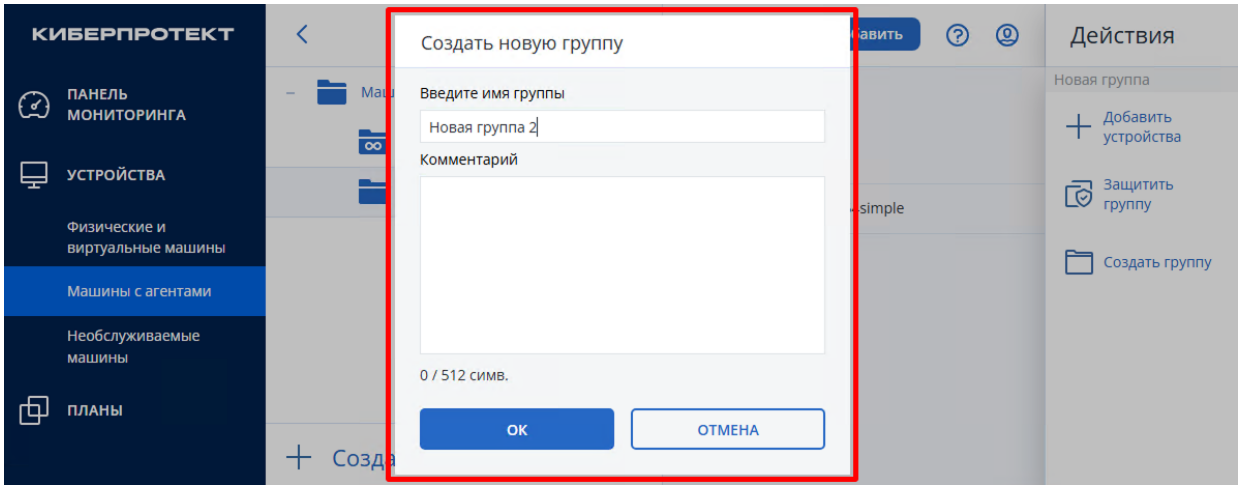
1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.
2. Выберите группу, внутри которой необходимо создать статическую группу.

> **Примечание**
>
> Доступно для встроенной корневой группы, а также пользовательских групп.

3. Выполните одно из указанных действий:
   - Нажмите на значок шестерёнки и в выпадающем меню выберите **Создать группу**.
   - В нижней части веб-консоли нажмите **Создать группу**.
   - Справа на панели **Действия** щёлкните **Создать группу** (доступно, если родительская группа не пустая).



4. В окне **Создать новую** группу введите имя группы. При необходимости добавьте комментарий длиной до 512 символов.
5. Нажмите **OK**.

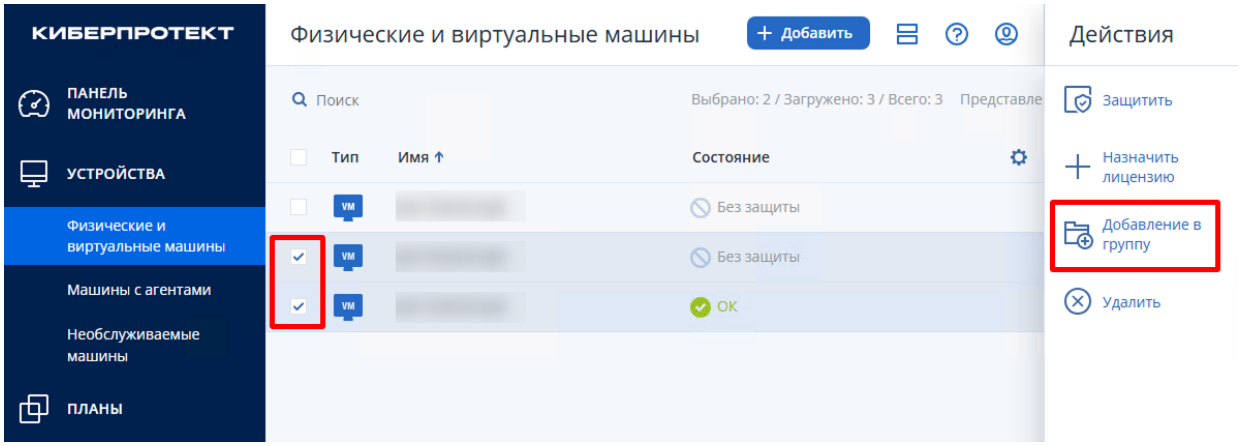


Добавление устройств в статические группы

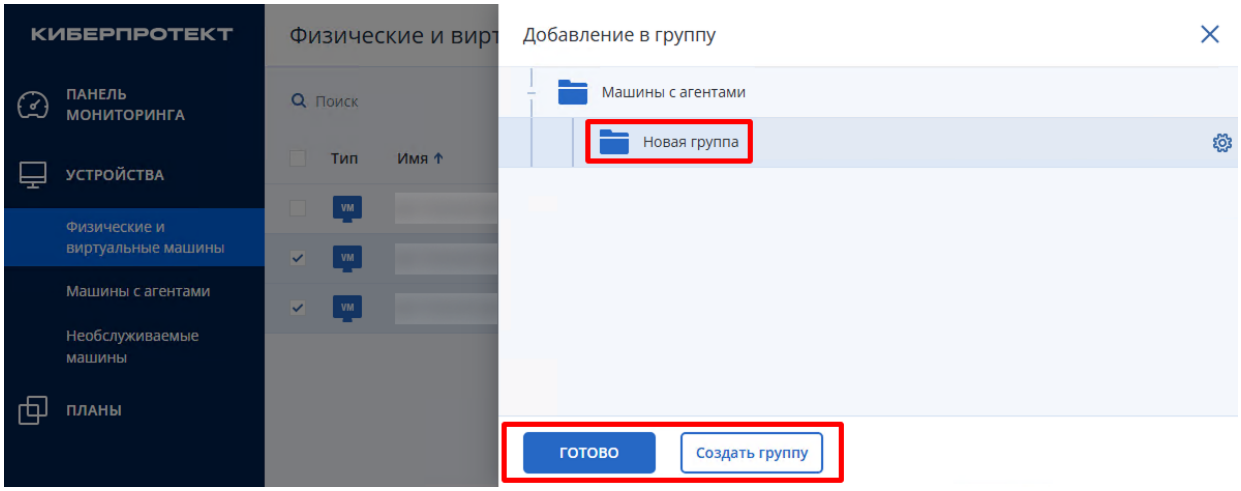
Добавить устройства в статическую группу можно несколькими способами.

Способ 1 (через раздел Физические и виртуальные машины)

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Физические и виртуальные машины**.
2. Установите флажки напротив выбранных машин.
3. Справа на панели **Действия** щёлкните **Добавление в группу**.

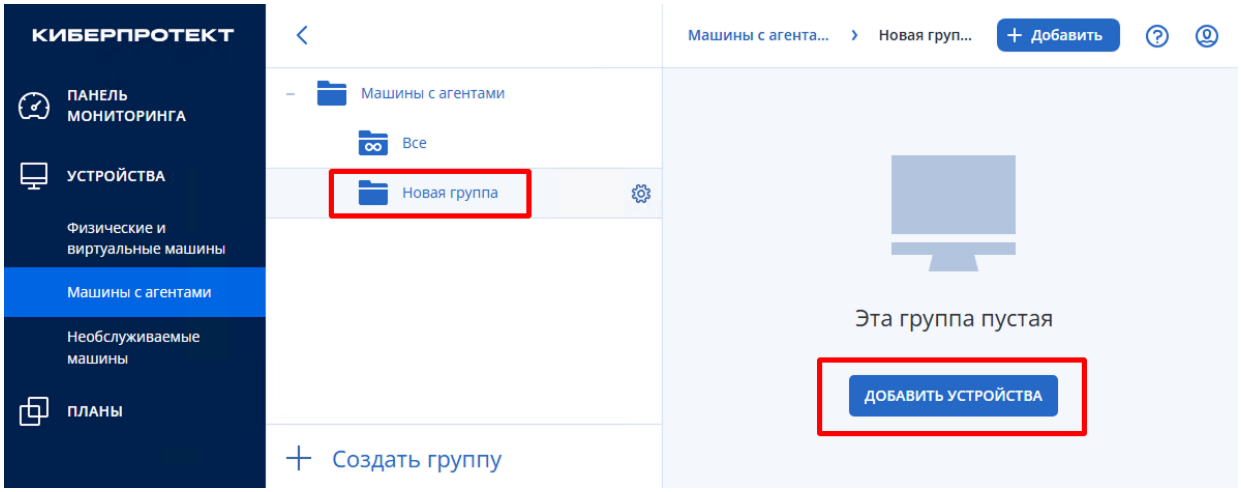


4. [Для добавления в существующую группу] Выберите группу и нажмите **Готово**.
5. [Для добавления в новую группу] Выберите группу, внутри которой будет создана новая группа, и нажмите **Создать группу**. Затем в окне **Создать новую группу** введите имя группы. При необходимости добавьте комментарий длиной до 512 символов.

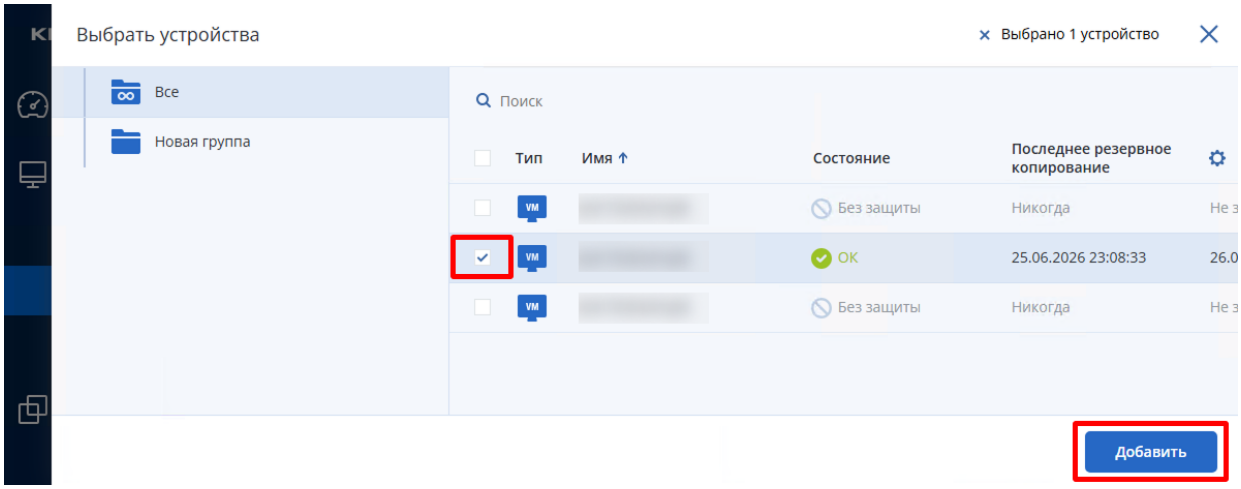


Способ 2 (через раздел Машины с агентами)

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.
2. Выберите группу.
3. Нажмите **Добавить устройства** (если в группе есть устройства, кнопка отображается на панели **Действия**, если в группе нет устройств — в области справа рядом с сообщением **Эта группа пустая**).



4. В области **Выбрать устройства** установите флажки напротив выбранных машин и нажмите **Добавить**.

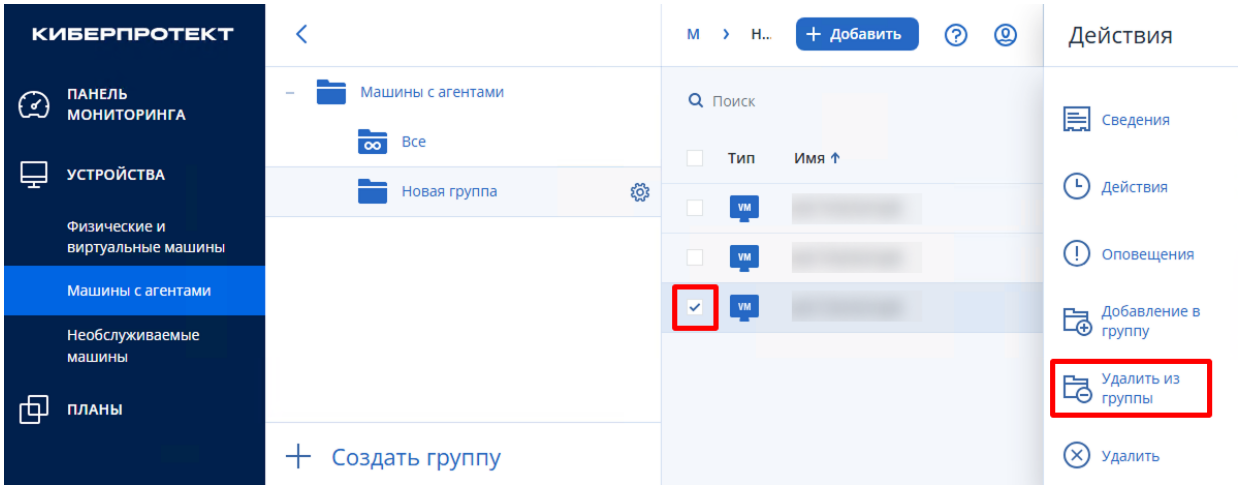


В результате выбранные устройства будут добавлены в статическую группу.

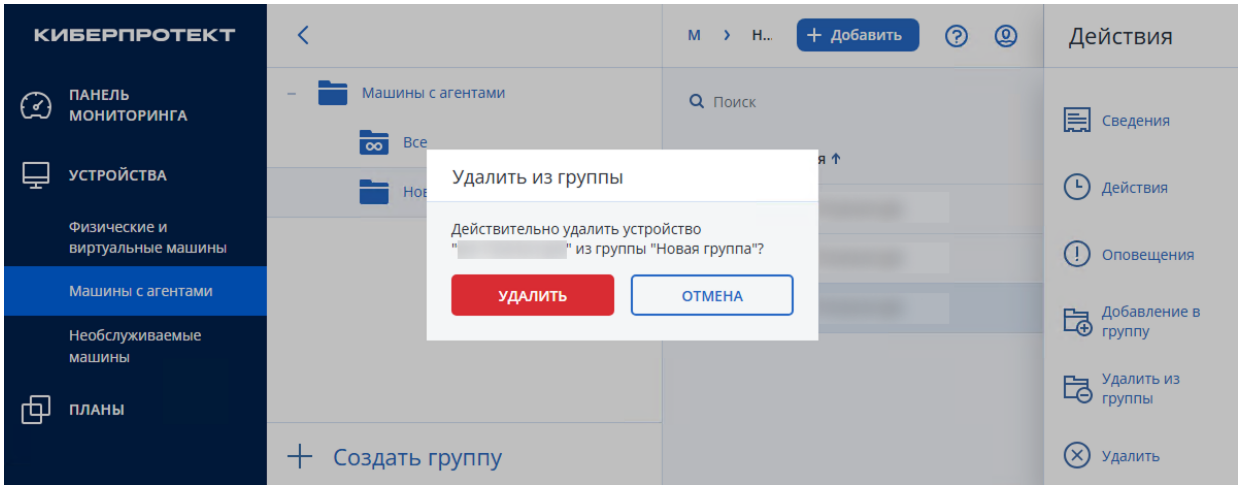
Удаление устройств из статических групп

Для удаления устройств из статической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.
2. Выберите группу, из которой нужно удалить устройства.
3. Установите флажки напротив выбранных машин.
4. Справа на панели **Действия** щёлкните **Удалить из группы**.



5. В окне **Удалить** из группы подтвердите удаление, щёлкнув **Удалить**.



В результате выбранные устройства будут удалены из статической группы.

Операции с динамическими группами

С динамическими группами доступны следующие операции:

- создание (см. далее в этом разделе);
- применение плана защиты к группе (подробнее см. в разделе *Применение плана защиты к группе*);
- переименование (подробнее см. в разделе *Переименование группы*);
- удаление (подробнее см. в разделе *Удаление группы*).

Создание динамических групп

Для создания динамической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.
2. В поле поиска введите условие выбора устройств для добавления в группу и нажмите **Поиск**.

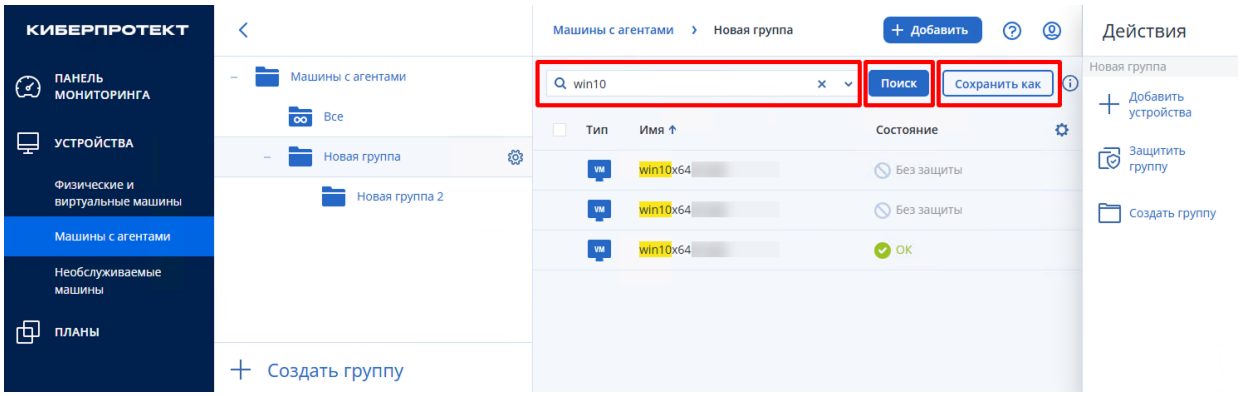
   Если не задать критерии поиска, по умолчанию будет выполнен поиск по имени. Критерии можно комбинировать с помощью операторов (они должны быть указаны в явном виде, например, `name LIKE '%name%' AND comment = ''`).

Примечание

- Некоторые критерии поиска не поддерживаются при создании группы. См. таблицу в разделе ”Условия поиска” ниже.
- Не поддерживается создание динамических групп на основе поиска во встроенной группе

Виртуальные устройства.

3. Если результаты поиска удовлетворительны, нажмите **Сохранить как** (справа от поля поиска).



4. В окне **Создать новую группу** введите имя группы. При необходимости добавьте комментарий длиной до 512 символов.

5. Нажмите **OK**.

В результате динамическая группа будет создана, а устройства, соответствующие критериям поиска, будут добавлены в неё автоматически.

Условия поиска

Доступные условия поиска приведены в следующей таблице.

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
name	• Имя хоста для физических машин. • Имя для виртуальных машин. • Имя базы данных. • Адрес электронной почты для почтовых ящиков.	name = 'en-00'	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
comment	Комментарий для устройства. Значение по умолчанию: • Для физических машин с ОС Windows описание компьютера считывается в свойствах компьютера в ОС Windows. • Пусто для других устройств. Чтобы просмотреть комментарий, в разделе **Устройства** выберите устройство, щёлкните **Подробнее** и перейдите к разделу **Комментарий**. Чтобы добавить или изменить комментарий, щёлкните **Добавить** или **Изменить**.	comment = 'important machine' comment = '' (все машины без комментария)	Да
ip	IP-адрес (только для физических машин).	ip RANGE ('10.250.176.1', '10.250.176.50')	Да Только при поиске с оператором RANGE
memorySize	Размер ОЗУ в мегабайтах (МиБ).	memorySize < 1024	Да
insideVm	Виртуальная машина с агентами в ней. Возможные значения: • true; • false.	insideVm = true	Да
tzOffset	Смещение часового пояса машины в минутах.	tzOffset = 120	Да
osName	Название операционной системы.	osName LIKE '%Windows 10%'	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
osType	Тип операционной системы. Возможные значения: • 'windows'; • 'linux'.	osType IN ('linux')	Да
osProductType	Тип продукта операционной системы. Возможные значения: • 'dc'. Означает контроллер домена. • 'server'. • 'workstation'.	osProductType = 'server'	Да
osSp	Пакет обновления операционной системы.	osSp = 1	Да
osVersionMajor	Основной номер версии операционной системы.	osVersionMajor = 1	Да
osVersionMinor	Дополнительный номер версии операционной системы.	osVersionMinor = 1	Да
isOnline	Доступность машины. Возможные значения: • true; • false.	isOnline = true	Нет
tenant	Название отдела, которому принадлежит устройство.	tenant = 'Unit 1'	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддер-живается для создания группы
tenantId	Идентификатор отдела, которому принадлежит устройство. Для получения идентификатора отдела напротив пункта **Устройства** выберите устройство и нажмите **Сведения → Все свойства**. Идентификатор отобразится в поле **ownerId**.	tenantId = ’3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9’	Да
state	Состояние устройства. Возможные значения: • ’idle’; • ’interactionRequired’; • ’canceling’; • ’backup’; • ’recover’; • ’install’; • ’reboot’; • ’failback’; • ’testReplica’; • ’run_from_image’; • ’finalize’; • ’failover’; • ’replicate’; • ’createAsz’; • ’deleteAsz’; • ’resizeAsz’.	state = ’backup’	Нет

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
status	Состояние ресурса. Возможные значения: • 'notProtected'; • 'ok'; • 'warning'; • 'error'; • 'critical'.	status = 'ok'	Нет
protectedByPlan	Устройства, защищённые посредством плана защиты с указанным идентификатором. Для получения идентификатора плана нажмите **Планы** → **Резервное копирование**, выберите план, нажмите на диаграмму в колонке **Статус** и затем нажмите на статус. Будет создан новый поиск с идентификатором плана.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
okByPlan	Устройства, защищённые посредством плана защиты с указанным идентификатором и со статусом **OK**.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
errorByPlan	Устройства, защищённые посредством плана защиты с указанным идентификатором и со статусом **Ошибка**.	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
warningByPlan	Устройства, защищённые посредством плана защиты с указанным идентификатором и со статусом **Предупреждение**.	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
runningByPlan	Устройства, защищённые посредством плана защиты с указанным идентификатором и со статусом **Выполняется**.	runningByPlan = ’4B2A7A93-A44F-4155-BDE3-A023C57C9431’	Нет
interactionByPlan	Устройства, защищённые посредством плана защиты с указанным идентификатором и со статусом **Требуется вмешательство**.	interactionByPlan = ’4B2A7A93-A44F-4155-BDE3-A023C57C9431’	Нет
ou	Машины, которые принадлежат к указанной организационной единице Active Directory.	ou IN (’RnD’, ’Computers’)	Да
id	Идентификатор устройства. Для получения идентификатора устройства напротив пункта **Устройства** выберите устройство и нажмите **Сведения** → **Все свойства**. Идентификатор отобразится в поле **Id**.	id != ’4B2A7A93-A44F-4155-BDE3-A023C57C9431’	Да Только при указании двух и более идентификаторов устройств.
lastBackupTime	Дата и время последнего успешного создания резервной копии в формате ’ГГГГ-ММ-ДД чч:мм’.	lastBackupTime > ’2016-03-11’ lastBackupTime <= ’2016-03-11 00:15’ lastBackupTime is null	Нет
lastBackupTryTime	Дата и время последней попытки резервного копирования в формате ’ГГГГ-ММ-ДД чч:мм’.	lastBackupTryTime >= ’2016-03-11’	Нет
nextBackupTime	Дата и время следующего резервного копирования в формате ’ГГГГ-ММ-ДД чч:мм’.	nextBackupTime >= ’2016-03-11’	Нет
agentVersion	Версия установленного агента защиты.	agentVersion LIKE ’12.0.*’	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддер-живается для создания группы
hostId	Внутренний идентификатор агента защиты. Для получения идентификатора агента защиты напротив пункта **Устройства** выберите машину и щёлкните **Сведения** → **Все свойства**. Используйте значение id свойства agent.	hostId = ’4B2A7A93-A44F-4155-BDE3-A023C57C9431’	Да
resourceType	Тип ресурса. Возможные значения: • ’machine’; • ’virtual_machine.vmwesx’; • ’virtual_machine.mshyperv’; • ’virtual_machine.rhev’; • ’virtual_machine.kvm’; • ’virtual_machine.xen’.	resourceType = ’machine’ resourceType in (’mssql_aag_database’, ’mssql_database’)	Да
hasAsz	Агент защиты на физической машине с Зоной безопасности. Возможные значения: • true; • false.	hasAsz=true	Да
chassis	Тип корпуса машины. Возможные значения: • unknown; • laptop; • desktop; • server; • other.	chassis=”laptop”	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Критерий	Значение	Примеры поисковых запросов	Поддерживается для создания группы
tagName	• Теги vSphere Tags виртуальных машин VMware. Отображаются только в разделе **Устройства** → **VMware**. • Теги виртуальных машин oVirt. Отображаются только в разделе **Устройства** → **oVirt**.	tagName = ’Tag 1’	Да

Примечание

Если пропустить значение для часов и минут, начальное время будет в формате `ГГГГ-ММ-ДД 00:00`, а конечное время — в формате `ГГГГ-ММ-ДД 23:59:59`. Например, `lastBackupTime = 2020-02-20` означает, что в результаты поиска будут включены все резервные копии из интервала `lastBackupTime >= 2020-02-20 00:00` и `lastBackup time <= 2020-02-20 23:59:59`.

Операторы

Доступные операторы приведены в следующей таблице.

Оператор	Значение	Примеры
AND	Логический оператор конъюнкции.	name like ’en-00’ AND tenant = ’Unit 1’
OR	Логический оператор дизъюнкции.	state = ’backup’ OR state = ’interactionRequired’
NOT	Логический оператор отрицания.	NOT(osProductType = ’workstation’)

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Оператор	Значение	Примеры
LIKE ’шаблон подстановочного символа’	Этот оператор используется для проверки того, соответствует ли выражение шаблону подстановочного символа. В этом параметре не учитывается регистр. Могут быть использованы следующие операторы подстановочного знака: • ”*” (звёздочка) или ”%” (знак процента) могут заменять собой произвольное число символов, включая их отсутствие. • ”_” (нижнее подчеркивание) может заменять собой один символ.	name LIKE ’en-00’ name LIKE ’*en-00’ name LIKE ’*en-00*’ name LIKE ’en-00_’
IN (<значение1>,... <значениеN>)	Этот оператор используется для проверки того, соответствует ли выражение любому значению из указанного списка значений. В этом параметре учитывается регистр.	osType IN (’windows’, ’linux’)
RANGE(<starting_value>, <ending_value>)	Этот оператор используется для проверки того, находится ли значение в диапазоне значений (включительно).	ip RANGE(’10.250.176.1’, ’10.250.176.50’)

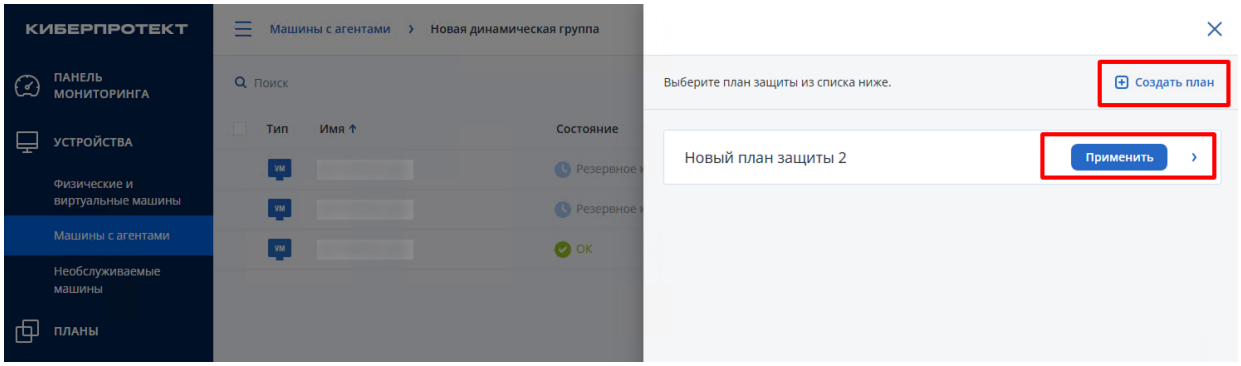
Применение плана защиты к группе

Для применения плана защиты к статической или динамической группе выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.

2. Выберите группу, к которой необходимо применить план защиты.
3. Справа на панели **Действия** щёлкните **Защитить группу**.

   В результате отобразится список планов защиты, которые можно применить к группе.
4. Выполните одно из следующих действий:
   - [Для применения существующего плана] Щёлкните **Применить**, при необходимости нажмите на иконку со стрелкой для просмотра информации о плане защиты.
   - [Для создания нового плана] Щёлкните **Создать план** и создайте новый план защиты, как описано в разделе *Резервное копирование*.



В результате план защиты будет применён к группе устройств.

Переименование группы

Для переименования статической или динамической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.
2. Выберите группу и нажмите на значок шестерёнки рядом с её названием.
3. В выпадающем меню выберите **Переименовать**.
4. В окне **Переименовать группу** введите новое имя группы. При необходимости добавьте комментарий длиной до 512 символов.
5. Нажмите **OK**.

В результате новое название группы будет отображено в списке групп.

Удаление группы

Для удаления статической или динамической группы выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Машины с агентами**.
2. Выберите группу и нажмите на значок шестерёнки рядом с её названием.
3. В выпадающем меню выберите **Удалить**.
4. В окне **Удалить группу** подтвердите удаление, нажав **Удалить**.

В результате группа будет удалена, а применённые к ней планы резервного копирования будут отозваны.

Резервное копирование

В разделе описывается дисковое и файловое резервное копирование серверов и виртуальных машин. О защите данных разнообразных инфраструктур см. в разделе *Защита приложений, сервисов, баз данных*.

Для резервного копирования данных необходимо создать план их защиты. План защиты с включенным модулем **Резервное копирование** — это набор правил, определяющий способ защиты указанных данных на конкретной машине.

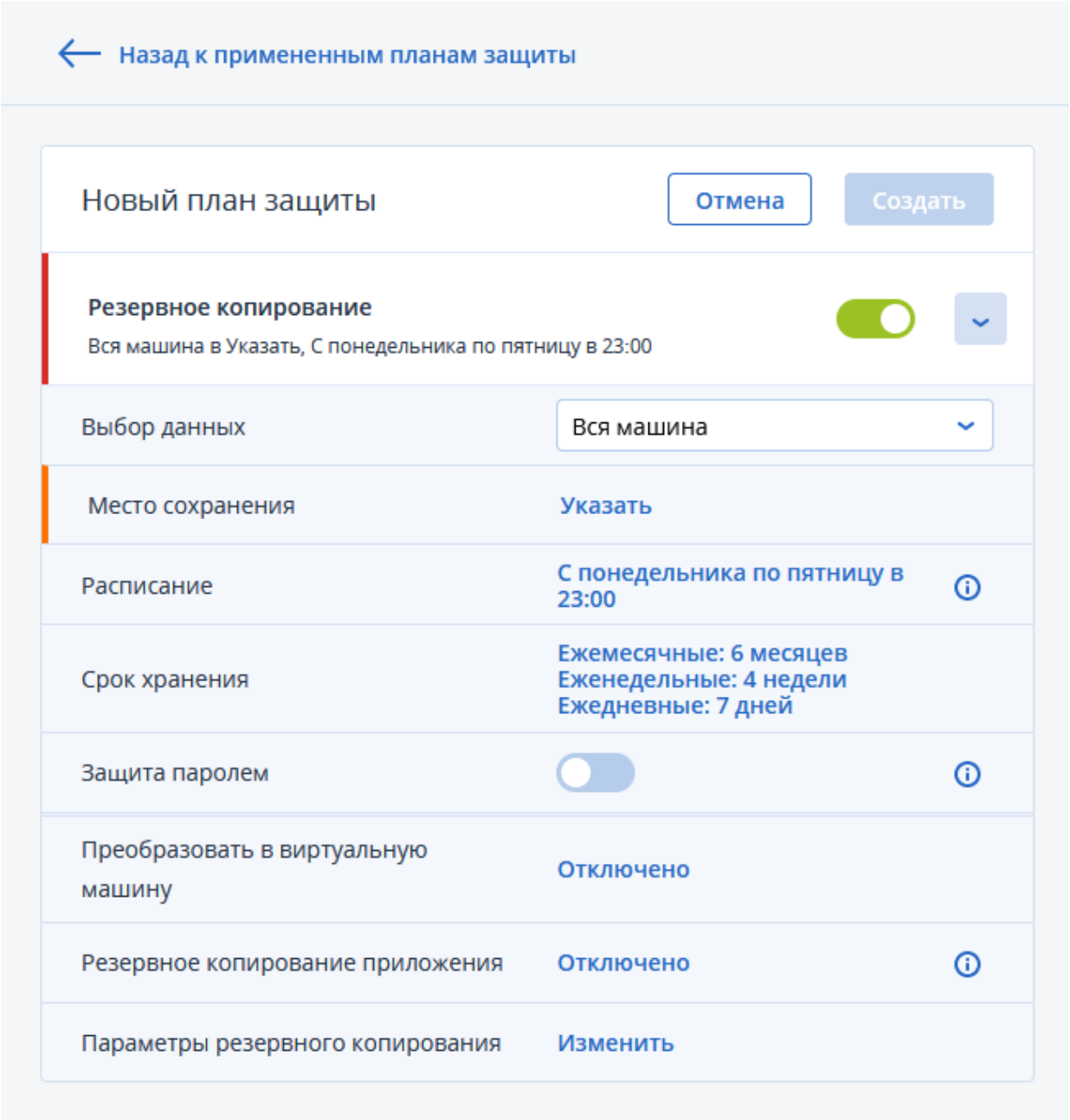
План защиты можно применить к нескольким машинам на этапе его создания или позже.

> **Примечание**
>
> При наличии только стандартных лицензий план защиты можно применить к одному или нескольким устройствам, выбранным вручную. Назначить план защиты для группы устройств невозможно.

Порядок создания первого плана защиты с включенным модулем ”Резервное копирование”

1. Выберите машины, резервные копии которых необходимо создать.
2. Щёлкните **Защитить**.

   В программе выводятся планы защиты, которые применены к машине. Если для машины еще не назначено ни одного плана, будет предложено применить план защиты по умолчанию. Можно задать настройки по собственному усмотрению и применить этот план или создать новый.

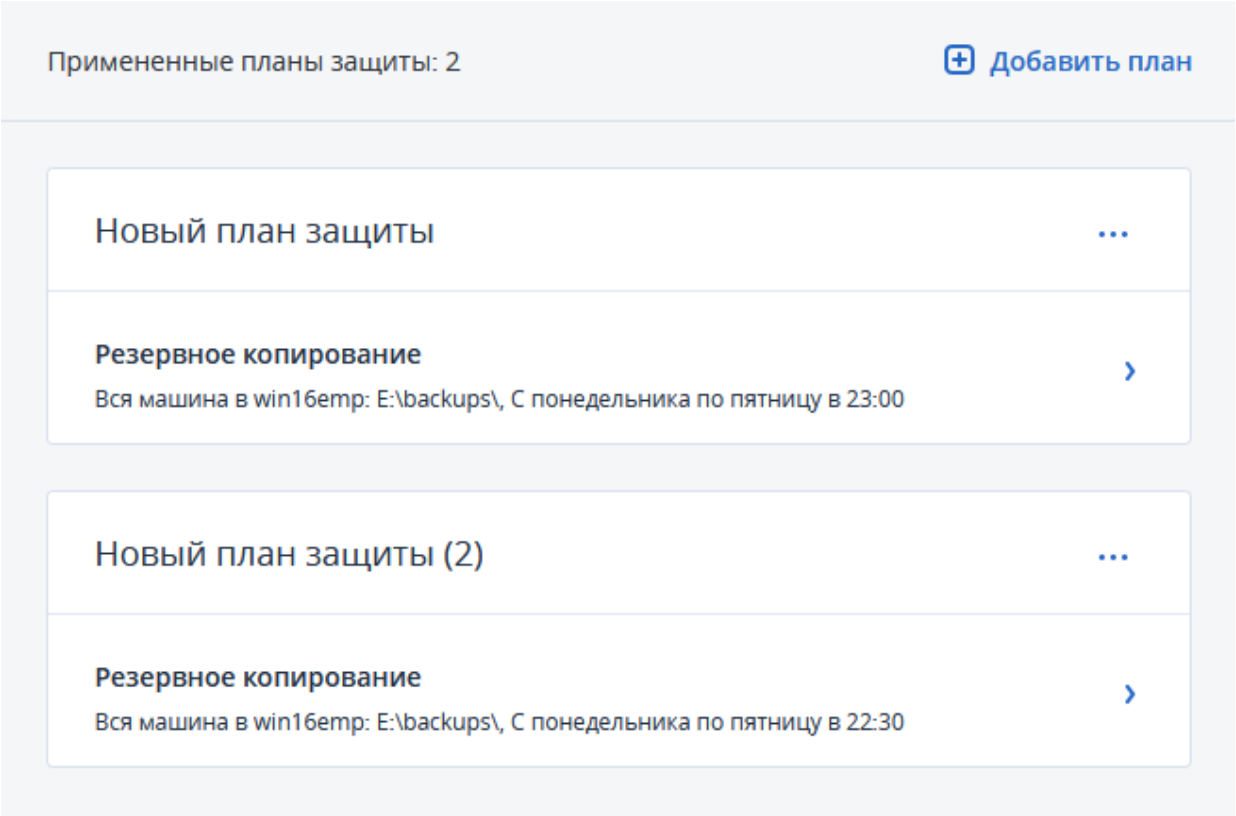


3. Чтобы создать новый план, щёлкните **Создать план**. Включите модуль **Резервное копирование** и разверните настройки.
4. [Необязательно] Для изменения имени плана защиты щёлкните имя по умолчанию.
5. [Необязательно] Чтобы изменить параметры модуля **Резервное копирование**, щёлкните соответствующий раздел панели плана защиты.
6. [Необязательно] Чтобы изменить параметры резервного копирования, щёлкните **Изменить** рядом с **Параметры резервного копирования**.
7. Нажмите кнопку **Создать**.

Порядок применения существующего плана резервного копирования

1. Выберите машины, резервные копии которых необходимо создать.
2. Щёлкните **Защитить**. Если к выбранным машинам уже применен стандартный план защиты, щёлкните **Добавить план**.

   В программе отображаются ранее созданные планы защиты.



3. Выберите план защиты для применения.
4. Нажмите кнопку **Применить**.

Агент

Агент — это основная часть ПО Кибер Бэкап. Агенты управляют всеми процессами резервного копирования (подробнее см. *Развертывание Кибер Бэкап*).

Агент устанавливается в ту программную среду, в которой находятся защищаемые объекты (см. *Установка агентов резервного копирования*).

Основные функции агента реализуются при его работе в рамках одного или нескольких планов защиты (см. *План защиты и модули*).

Агент Кибер Бэкап может выполнять резервное копирование данных в режиме многозадачности.

Многозадачность агента заключается в его способности выполнять одновременное резервное копирование нескольких элементов в рамках различных планов защиты (см. *Одновременное резервное копирование*).

Типы резервных копий

Кибер Бэкап работает со следующими типами резервных копий:

- **Полная** — содержит все исходные данные и является самодостаточной. Для восстановления такой резервной копии не требуется доступ к каким-либо другим. Первая резервная копия, создаваемая планом защиты, всегда полная.
- **Инкрементная** — содержит изменения данных с момента создания последней резервной копии любого типа. Для восстановления инкрементной резервной копии нужна вся цепочка предыдущих копий, от которых она зависит, вплоть до исходной полной.
- **Дифференциальная** — содержит изменения данных с момента создания последней полной резервной копии. Для восстановления дифференциальной резервной копии нужна полная резервная копия, от которой она зависит.

При настройке схемы резервного копирования можно выбрать комбинацию используемых типов резервных копий (подробнее см. в разделе *Расписание*).

Формат TIBX

Резервные копии, создаваемые Кибер Бэкап, в большинстве сценариев сохраняются в формате TIBX.

Этот формат обеспечивает следующие возможности:

- Хранение всех данных, относящихся к резервным копиям (включая полные или дифференциальные резервные копии и зависимые от них цепочки инкрементных резервных копий, метаданные и другие служебные данные) в едином архиве с возможностью принудительного *деления на части заданного размера* для соответствия ограничениям файловых систем и емкости носителей.
- Отсутствие деградации производительности резервного копирования и восстановления по мере роста числа инкрементных резервных копий в цепочке вплоть до сотни.
- Отсутствие деградации производительности восстановления из инкрементных резервных копий по сравнению с восстановлением из полных резервных копий классических форматов хранения.
- *Дедупликацию данных* внутри каждой цепочки резервных копий, осуществляемую на источнике данных.

- Проверку целостности структуры резервной копии при каждой операции чтения.
- Управляемое на уровне параметров резервного копирования *сжатие* данных резервной копии.
- Отчуждаемость резервной копии от экземпляра сервера управления, с помощью которого она была создана.
- Синтез полной резервной копии *до последней* или *до выбранной* точки восстановления вне источника данных с проверкой целостности структуры резервной копии и данных внутри нее.

Модуль резервного копирования: памятка

В таблице ниже вкратце описаны доступные параметры модуля ”Резервное копирование”. С ее помощью вы сможете легко создать план, который лучше всего отвечает вашим потребностям.

Элементы для резервного копирования	**Элементы для резервного копирования / Способы выбора**	**Место сохранения**	**Расписание / Схемы резервного копирования**	**Время хранения**
Диски/тома (физические машины)	*Напрямую* *Правила политики* *Фильтры файлов*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Зона безопасности* *Управляемое хранилище* *Ленточное устройство*	*Всегда инкрементное* *Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Ежемесячно полное, еженедельно диф-ференциальное, ежедневно инкрементное (GFS)* *Настраиваемый вариант (П-Д-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Элементы для резервного копирования	Элементы для резервного копирования / Способы выбора	Место сохранения	Расписание / Схемы резервного копирования	Время хранения
Диски/тома (виртуальные машины)	*Правила политики* *Фильтры файлов*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище* *Ленточное устройство*	*Всегда инкрементное* *Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Ежемесячно полное, еженедельно диф-ференциальное, ежедневно инкрементное (GFS)* *Настраиваемый вариант (П-Д-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*
Файлы (только физические машины)	*Напрямую* *Правила политики* *Фильтры файлов*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Зона безопасности* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Ежемесячно полное, еженедельно диф-ференциальное, ежедневно инкрементное (GFS)* *Настраиваемый вариант (П-Д-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Элементы для резервного копирования	Элементы для резервного копирования / Способы выбора	Место сохранения	Расписание / Схемы резервного копирования	Время хранения
Конфигурация ESXi	*Напрямую*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS*	*Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Ежемесячно полное, еженедельно диф-ференциальное, ежедневно инкрементное (GFS)* *Всегда инкрементное* *Настраиваемый вариант (П-Д-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*
Базы данных Microsoft SQL Server	*Напрямую*	*Локальная папка* *Сетевая папка* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Настраиваемый вариант (П-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*
Базы данных Microsoft Exchange Server	Напрямую	*Локальная папка* *Сетевая папка* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Настраиваемый вариант (П-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Элементы для резервного копирования	Элементы для резервного копирования / Способы выбора	Место сохранения	Расписание / Схемы резервного копирования	Время хранения
Почтовые ящики Exchange	*Напрямую*	*Локальная папка* *Сетевая папка* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище*	*Всегда инкрементное*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*
Базы данных Oracle	*Команды до и после процедуры* *Резервное копирование сервера Oracle*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Зона безопасности* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*
Базы данных PostgreSQL	*Напрямую*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище*	*Всегда полное* *Еженедельно полное, ежедневно инкрементное* *Настраиваемый вариант (П-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *Хранить бессрочно*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Элементы для резервного копирования	Элементы для резервного копирования / Способы выбора	Место сохранения	Расписание / Схемы резервного копирования	Время хранения
Данные CommuniGate Pro	*Напрямую*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище*	*Всегда полное* *Всегда инкрементное* *Еженедельно полное, ежедневно инкрементное*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *Хранить бессрочно*
Данные VK WorkMail и VK WorkDisk	*Напрямую*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное* *Всегда инкрементное* *Еженедельно полное, ежедневно инкрементное*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *Хранить бессрочно*
Данные Kubernetes	*Напрямую*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Управляемое хранилище*	*Всегда полное* *Всегда инкрементное* *Еженедельно полное, ежедневно инкрементное* *Настраиваемый вариант (П-И)*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *Хранить бессрочно*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Элементы для резервного копирования	Элементы для резервного копирования / Способы выбора	Место сохранения	Расписание / Схемы резервного копирования	Время хранения
РЕД База Данных	*Команды до и после процедуры*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Зона безопасности* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*
Серверы SAP HANA	*Команды до и после процедуры*	*Локальная папка* *Сетевая папка* *Сервер SFTP* *NFS* *Кибер Инфраструктура или Кибер Хранилище* *Зона безопасности* *Управляемое хранилище* *Ленточное устройство*	*Всегда полное* *Всегда инкрементное*	*По возрасту резервной копии (одно правило на набор резервных копий)* *По количеству резервных копий* *По общему размеру резервных копий* *Хранить бессрочно*

Ограничения

Сетевая папка

Для резервного копирования в сетевые папки на машине с установленным агентом для Linux необходимо иметь установленные дополнительные пакеты Linux. Например, для CentOS 7 должны быть установлены следующие пакеты (в зависимости от места сохранения резервных копий):

Место сохранения	Необходимый компонент Linux
SMB NTLM	cifs-utils
SMB with Kerberos	cifs-utils keyutils
NFS	nfs-utils

Для более подробной информации об установке пакетов см. *Пакеты Linux*.

Примечание

Для разных операционных систем на основе Linux названия этих пакетов могут отличаться.

Сервер SFTP и ленточное устройство

- Эти хранилища не могут использоваться для резервных копий с поддержкой приложений.
- Схема резервного копирования **Всегда инкрементное** недоступна при выполнении резервного копирования в эти хранилища.
- Правило хранения **По общему размеру резервных копий** недоступно для этих хранилищ.

NFS

- Резервное копирование в общие папки NFS недоступно в Windows.
- Схема резервного копирования **Всегда инкрементное** для файлов (физических машин) недоступна при выполнении резервного копирования в общие папки NFS.

Кибер Инфраструктура или Кибер Хранилище

Для подробной информации см. раздел *О продуктах Кибер Инфраструктура и Кибер Хранилище*.

Зона безопасности

- Схема резервного копирования **Всегда инкрементное** для файлов (физических машин) недоступна при выполнении резервного копирования в зону безопасности.

Управляемое хранилище

- Управляемое хранилище с активированной функцией дедупликации или защитой паролем не может быть выбрано в качестве места хранения:
  - если используется схема резервного копирования **Всегда инкрементное**,

- если используется формат резервной копии **Версии 12**,
- для резервных копий почтовых ящиков Exchange.

- Правило хранения **По общему размеру резервных копий** недоступно для управляемых хранилищ с активированной функцией дедупликации.

Всегда инкрементное

- Схема резервного копирования **Всегда инкрементное** недоступна при выполнении резервного копирования на SFTP-сервер или ленточное устройство.

По общему размеру резервных копий

- Правило хранения **По общему размеру резервных копий** недоступно:
  - если используется схема резервного копирования **Всегда инкрементное**,
  - при выполнении резервного копирования на SFTP-сервер, ленточное устройство или управляемое хранилище с активированной функцией дедупликации.

Выбор данных для резервного копирования

Выбор всей машины

Чтобы настроить резервное копирование всей машины, в области **Выбор данных** плана выберите **Вся машина**.

Для физической или виртуальной машины с агентом, установленным в гостевой ОС, резервная копия всей машины — это резервная копия всех ее несъёмных дисков. В таких сценариях в план необходимо добавлять объекты из раздела **Устройства** → **Машины с агентами**. Задание по резервному копированию будет выполнено агентом в гостевой ОС.

Для виртуальной машины без агента резервная копия всей машины — это резервная копия всех ее несъёмных дисков, которые попадают в снимок ВМ, а также данных о конфигурации ВМ (ЦП, ОЗУ, дисках, сетевых адаптерах и прочем). В таких сценариях в план необходимо добавлять объекты из подраздела соответствующей системы виртуализации в разделе **Устройства**, например, **oVirt** или **OpenNebula**. Задание по резервному копированию будет выполнено агентом для данной системы виртуализации с помощью снимка ВМ на уровне гипервизора.

Примечание

Одна и та же машина может отображаться в разных местах раздела **Устройства**, поскольку данные о

ней поступают от разных агентов Кибер Бэкап. Например, если у виртуальной машины VMware есть агент в гостевой ОС и для неё же есть агент на уровне гипервизора, она будет отображаться в подразделах **Устройства** → **Машины с агентами** и **Устройства** → **VMware**. Резервное копирование первого из этих ресурсов будет выполнено агентом в гостевой ОС, второго — агентом на уровне гипервизора.

Примечание

Внешние диски, такие как USB-накопители или другие съемные носители, не включаются в резервную копию всей машины. Для них необходимо настроить резервное копирование дисков и томов (подробнее см. в разделе *Выбор дисков и томов*).

Выбор файлов и папок

Резервное копирование на уровне файлов доступно для физических и виртуальных машин, если для них настроено резервное копирование с помощью агента, установленного в гостевой системе.

Для восстановления операционной системы резервной копии на уровне файлов недостаточно. Выберите этот способ, если необходимо сохранять только определенные данные (например, текущий проект). Это позволит уменьшить размер архива и тем самым сократить потребность в дисковом пространстве.

Есть два способа выбора файлов: напрямую на каждой машине или с помощью правил политики. Для каждого из этих способов выбор можно уточнить с помощью *фильтров файлов*.

Выбор напрямую на машине

1. В области **Выбор данных** выберите вариант **Файлы/папки**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Напрямую**.
4. Для каждой машины, включенной в план защиты, выполните указанные ниже действия.
    1. Щёлкните **Выбрать файлы и папки**.
    2. Щёлкните **Локальная папка** или **Сетевая папка**.

       Общая папка должна быть доступна с выбранной машины.
    3. Перейдите к требуемым файлам и папкам или введите путь и нажмите кнопку со стрелкой. Если потребуется, укажите имя пользователя и пароль для доступа к общей папке.

Резервное копирование папки с анонимным доступом не поддерживается.

4. Выберите файлы и папки.
5. Нажмите кнопку **Готово**.

Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **С использованием правил политики**.
4. Выберите готовые правила, введите собственные или используйте оба варианта.

   Правила политики будут применены ко всем машинам, которые входят в план защиты. Если на машине при запуске резервного копирования отсутствуют объекты, соответствующие хотя бы одному правилу, копирование завершится сбоем.
5. Нажмите кнопку **Готово**.

Правила выбора для Windows

- Полный путь к файлу или папке, например `D:\Work\Text.doc` или `C:\Windows`.
- Шаблоны
  - `[All Files]` позволяет выбрать все файлы на всех томах машины.
  - `[All Profiles Folder]` позволяет выбрать папку, в которой хранятся все профили пользователей (обычно это `C:\Users` или `C:\Documents and Settings`).
- Переменные среды:
  - `%ALLUSERSPROFILE%` позволяет выбрать папку, в которой хранятся общие данные всех профилей пользователей (обычно это `C:\ProgramData` или `C:\Documents and Settings\All Users`).
  - `%PROGRAMFILES%` позволяет выбрать папку с файлами программ (например, `C:\Program Files`).
  - `%WINDIR%` позволяет выбрать папку, в которой находится система Windows (например, `C:\Windows`).

  Можно использовать другие переменные среды или их сочетание с текстом. Например, чтобы выбрать папку Java в папке Program Files, введите `%PROGRAMFILES%\Java`.

Правила выбора для Linux

- Полный путь к файлу или каталогу. Например, чтобы создать резервную копию файла `file.txt` в томе `/dev/hda3`, подключенном к каталогу `/home/usr/docs`, введите `/dev/hda3/file.txt` или `/home/usr/docs/file.txt`.
  - `/home` позволяет выбрать домашний каталог обычных пользователей.
  - `/root` позволяет выбрать домашний каталог привилегированного пользователя.
  - `/usr` позволяет выбрать каталог для всех пользовательских программ.
  - `/etc` позволяет выбрать каталог с конфигурационными файлами системы.
- Шаблоны
  - `[All Files]` позволяет выбрать все файлы во всех каталогах машины.
  - `[All Profiles Folder]` позволяет выбрать каталог **/home**. В этой папке по умолчанию размещены все профили пользователя.

Выбор дисков и томов

Резервная копия диска содержит копию диска или тома в запакованном виде. Из такой копии можно восстановить отдельные диски, тома или файлы. Резервная копия всей машины — это резервная копия со всеми ее несъемными дисками.

Есть два способа выбора дисков/томов: напрямую на каждой машине или с помощью правил политики. Исключить файлы из резервной копии можно с помощью *фильтров файлов*.

Выбор напрямую на машине

Возможность выбора дисков и томов напрямую доступна только для физических машин. Чтобы включить прямой выбор дисков и томов на виртуальной машине, необходимо установить агент Киберзащиты в ее гостевой операционной системе.

1. В области **Выбор данных** выберите вариант **Диски/тома**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Напрямую**.
4. Для каждой из машин, которая включена в план защиты, установите флажки рядом с дисками и томами, которые требуется скопировать.
5. Нажмите кнопку **Готово**.

Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Диски/тома**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **С использованием правил политики**.
4. Выберите готовые правила, введите собственные или используйте оба варианта.

   Правила политики будут применены ко всем машинам, которые входят в план защиты. Если на машине при запуске резервного копирования отсутствуют объекты, соответствующие хотя бы одному правилу, копирование завершится сбоем.
5. Нажмите кнопку **Готово**.

Правила для Windows и Linux

- `[All Volumes]` позволяет выбрать все тома машин с Windows и все подключенные тома машин с Linux.
- `[Fixed Volumes (physical machines)]` позволяет выбрать все тома физических машин, кроме съемных носителей. К фиксированным томам относятся тома на устройствах SCSI, ATAPI, ATA, SSA, SAS и SATA, а также RAID-массивы.
- `[BOOT+SYSTEM]` выбирает системный том и загрузочный том. Это сочетание соответствует минимальному набору данных, который необходим для восстановления операционной системы из резервной копии.
- `[Disk 1]` позволяет выбрать первый диск машины, включая все тома на нем. Чтобы выбрать другой диск, введите соответствующий номер.

Правила только для Windows

- Буква диска (например, **C:**) обозначает том с указанной буквой.
- `[ЗАГРУЗОЧНЫЙ+СИСТЕМНЫЙ ДИСК (физические машины)]` выбирает все тома диска, на котором расположены загрузочный и системный том. Если загрузочный том и системный том располагаются на разных дисках, ничего не будет выбрано. Это правило действует только для физических машин.

Правила только для Linux

- `/dev/hda1` обозначает первый том на первом жестком диске IDE.
- `/dev/sda1` обозначает первый том на первом жестком диске SCSI.
- `/dev/md1` обозначает первый жесткий диск в программном RAID-массиве.

Чтобы выбрать другие базовые тома, введите `/dev/xdyN`, где:

- x обозначает тип диска;
- y обозначает номер диска (a — первый, b — второй и т. д.);
- N обозначает номер тома.

Чтобы выбрать логический том, укажите путь к нему, отображаемый после выполнения команды `ls /dev/mapper` в учетной записи привилегированного пользователя. Пример:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

В выходных данных отображаются два логических тома, `lv1` и `lv2`, принадлежащие к группе томов `vg_1`. Для создания резервных копий этих томов введите:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Что содержится в резервных копиях томов или дисков

Резервная копия диска или тома хранит **файловую систему** целиком и включает всю информацию, необходимую для загрузки операционной системы. Из таких резервный копий можно восстанавливать целые диски или тома, а также отдельные папки и файлы.

Если включен параметр резервного копирования *посекторное копирование (бесформатный режим)*, то в резервной копии диска сохраняются все сектора диска. Посекторное резервное копирование может использоваться для резервного копирования дисков с неопознанными или неподдерживаемыми файловыми системами и другими нестандартными форматами данных.

Windows

Резервная копия тома хранит все файлы и папки выбранного тома независимо от их атрибутов (включая скрытые и системные файлы), загрузочную запись, таблицу размещения файлов (FAT), если она есть, а также корневую и нулевую дорожки жесткого диска с основной загрузочной записью (MBR).

Резервная копия диска сохраняет все тома выбранного диска (включая скрытые разделы, например

специальные скрытые разделы, предназначенные для хранения ПО поставщика) и нулевую дорожку жесткого диска с основной загрузочной записью (MBR).

Следующие элементы *не входят* в резервную копию диска или тома (а также в резервную копию на уровне файлов):

- Файл подкачки (pagefile.sys) и файл, в котором сохраняется содержимое ОЗУ, когда машина переходит в режим гибернации (hiberfil.sys). После восстановления эти файлы будут созданы повторно в соответствующем месте с нулевым размером.
- При выполнении резервного копирования в операционной системе (а не на загрузочном носителе или при резервном копировании виртуальных машин на уровне гипервизора):
  - Теневое хранилище Windows. Путь к нему определяется значением реестра **VSS Default Provider** в разделе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`. Это означает, что в ОС Windows резервное копирование Windows Restore Points не производится.
  - Файлы и папки, указанные в ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot`, если включен параметр резервного копирования **Volume Shadow Copy Service (VSS)** (см. *Служба теневого копирования томов (VSS)*).

Linux

Резервная копия тома хранит все файлы и папки выбранного тома независимо от их атрибутов, загрузочную запись и суперблок файловой системы.

Резервное копирование диска сохраняет все тома диска, а также нулевую дорожку с основной загрузочной записью.

Выбор конфигурации ESXi

Резервная копия конфигурации хоста ESXi позволяет восстановить хост ESXi на ”голое железо”. Восстановление выполняется с загрузочного носителя.

Виртуальные машины, которые выполняются на данном хосте, не включены в резервную копию. Создать для них резервную копию и восстановить их можно отдельно.

В резервную копию конфигурации хоста входят следующие элементы:

- Разделы загрузчика и активного загрузочного блока данного хоста.
- Состояние хоста (конфигурация виртуальной сети и хранилища данных, ключи SSL, сетевые настройки сервера и информация локального пользователя).

- Расширения и исправления, установленные или поэтапно устанавливаемые на хосте.
- Файлы журнала.

Предварительные требования

- В разделе **Профиль безопасности** конфигурации хоста ESXi должен быть включен SSH.
- Необходимо знать пароль учетной записи ”root” хоста ESXi.

Ограничения

- Резервное копирование конфигурации ESXi не поддерживается для VMware vSphere 7.0 и новее.
- Для корректной загрузки восстановленной конфигурации ESXi рекомендуется отключить параметр **Безопасная загрузка** (Secure boot) в настройках хоста.

Порядок выбора конфигурации ESXi

1. Щёлкните **Устройства** → **Физические и виртуальные машины**, после чего выберите хосты ESXi, для которых необходимо создать резервную копию.
2. Нажмите кнопку **Резервное копирование**.
3. В поле **Выбор данных**, выберите **Конфигурация ESXi**.
4. В поле **Пароль пользователя root ESXi** укажите пароль для учетной записи root на каждом выбранном хосте или примените один пароль ко всем хостам.

Выбор места сохранения

Для выбора хранилища резервных копий

1. Нажмите **Место сохранения резервной копии**.
2. Выполните одно из следующих действий:
    - Выберите использованное ранее или предопределенное хранилище резервных копий.
    - Нажмите **Добавить хранилище** и затем укажите новое хранилище резервных копий.

Поддерживаемые расположения

Виды поддерживаемых хранилищ резервных копий приведены в таблицах ниже.

Вид хранилища	СУБД			
	PostgreSQL	Microsoft SQL Server	MySQL	БД Microsoft Exchange Server
Локальная папка	+	+	+	+
Сетевая папка	+	+	+	+
Папка NFS	+	—	—	—
SFTP	+	—	—	—
Узел хранения	+	+	—	+
Кибер Инфраструктура или Кибер Хранилище	+	+	+	+
Зона безопасности	—	—	—	—
Ленты	+	+	—	+

Вид хранилища	Физические и виртуальные машины с установленным агентом		ESXi-конфигурация	Kubernetes
	Windows	Linux		
Локальная папка	+	+	+	+
Сетевая папка	+	+	+	+
Папка NFS	—	+	+	+
SFTP	+	+	+	+
Узел хранения	+	+	—	+
Кибер Инфраструктура или Кибер Хранилище	+	+	—	+
Зона безопасности	+	+	+	—
Ленты	+	+	—	+

Вид хранилища	Виртуальные машины, защищённые в безагентном режиме									
	VMware	Hyper-V	oVirt, zVirt, HOSTVM, ROSA Virtualization	OpenStack, VK Cloud	OpenNebula, ПК СВ ”Брест”	ECP VeiL, SpaceVM	Basis DynamiX Enterprise	Proxmox Virtual Environment	Кибер Инфраструктура	VM-manager
Локальная папка	+	+	+	—	—	—	—	—	—	—
Сетевая папка	+	+	+	+	+	+	+	+	+	+
Папка NFS	+	—	+	+	+	+	+	+	+	+
SFTP	+	+	+	+	+	+	+	+	+	—
Узел хранения	+	+	+	+	+	+	+	+	+	—
Кибер Инфраструктура или Кибер Хранилище	+	+	+	+	+	+	+	+	+	+
Зона безопасности	—	—	—	—	—	—	—	—	—	—
Ленты	+	+	+	+	+	+	+	+	+	—

Вид хранилища	Почтовые ящики				
	VK WorkMail	CommuniGate Pro	Mailion	Почтовые ящики Microsoft Exchange Server	RuPost
Локальная папка	+	+	+	+	+
Сетевая папка	+	+	+	+	+
Папка NFS	+	+	+	—	+
SFTP	+	+	+	—	+
Узел хранения	+	+	+	+	+
Кибер Инфраструктура или Кибер Хранилище	+	+	+	+	+
Зона безопасности	—	—	—	—	—
Ленты	+	—	—	—	+

- **Локальная папка**

  Если выбрана одна машина, перейдите на ней в соответствующую папку или введите путь.

  Если выбрано несколько машин (или их статическая или динамическая группа), введите путь к папке. Резервные копии будут сохраняться в этой папке на каждой из выбранных физических машин либо на машине, на которой установлен агент для виртуальных машин. Если папка не существует, она будет создана.

- **Сетевая папка**

  Это папка, общий доступ к которой предоставлен посредством SMB/CIFS/DFS.

  Также поддерживаются сетевые папки в хранилищах, работающих в режиме ”Только для добавления” (Append Only). Перед их использованием требуется *дополнительная настройка*.

  Перейдите к требуемой общей папке или введите путь к ней в следующем формате:

  - Для общих папок SMB/CIFS: `\\<имя_хоста>\<путь>` или `smb://<имя_хоста>/<путь>/`
  - Для папок DFS: `\\<полное доменное имя DNS>\<корневой каталог DFS>\<путь>`

    Например, `\\example.company.com\shared\files`

  После этого нажмите кнопку со стрелкой. Если потребуется, укажите имя пользователя и пароль для доступа к общей папке. Эти учетные данные можно изменить в любое время. Для этого щёлкните значок ключа рядом с именем папки.

Примечание

- Резервное копирование в папку с анонимным доступом не поддерживается.
- Перед выполнением резервного копирования в сетевую папку убедитесь, что на компьютере с агентом для Linux установлены необходимые пакеты. Подробнее см. в разделе *Модуль резервного копирования: памятка*.

- **Папка NFS** (доступна для машин под управлением Linux)

  Перейдите к требуемой папке NFS или введите путь к ней в следующем формате: `nfs://<имя хоста>/<экспортированная папка>:/<подпапка>`.

  После этого нажмите кнопку со стрелкой.

  Невозможно выполнить резервное копирование в папку NFS, защищенную паролем.

- **SFTP**

  Введите имя или IP-адрес сервера SFTP. Поддерживаются следующие форматы:

```
sftp://<сервер>
sftp://<сервер>/<папка>
```

  После введения имя пользователя и пароля вы можете просматривать папки на сервере.

  В любом формате также можно указать порт, имя пользователя и пароль:

```
sftp://<сервер>:<порт>/<папка>
sftp://<имя пользователя>@<сервер>:<порт>/<папка>
sftp://<имя пользователя>:<пароль>@<сервер>:<порт>/<папка>
```

  Если номер порта не указан, используется порт 22.

  Пользователи, для которых настроен доступ к SFTP без пароля, могут выполнять резервное копирование на SFTP.

  Резервное копирование на FTP-сервер не поддерживается.

- **Узел хранения**

  Узел хранения — это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается путем организации хранилищ и управления хранилищами, выделенными для корпоративных резервных копий (управляемыми хранилищами).

Выберите предварительно созданное хранилище или создайте новое, нажав **Добавить хранилище** → **Узел хранения**. Информацию о настройках см. в разделе *Добавление управляемого хранилища*.

Если потребуется, укажите имя пользователя и пароль для доступа к узлу хранения. Члены указанных ниже групп Windows на машине с установленным узлом хранения имеют доступ ко всем управляемым хранилищам на узле хранения:

- **Администраторы**
- **ASN Remote Users**

  Эта группа создается автоматически при установке узла хранения. По умолчанию эта группа пустая. Можно добавить пользователей в эту группу вручную.

- **Кибер Инфраструктура / Кибер Хранилище**

  Кибер Инфраструктура и Кибер Хранилище — это высоконадежные программно-определяемые хранилища данных с избыточностью данных и автоматическим самовосстановлением. Эти хранилища данных можно настроить как шлюз для хранения резервных копий в Yandex Cloud или в одном из ряда решений для хранения данных, совместимых с S3 или Swift. В хранилищах также может использоваться сервер NFS. Дополнительную информацию см. в разделе *О продуктах Кибер Инфраструктура и Кибер Хранилище*.

- **Зона безопасности** (доступно, если этот раздел присутствует на каждой из выбранных машин)

  Зона безопасности — это безопасный раздел на диске машины, для которой создана резервная копия. Перед настройкой резервной копии этот раздел необходимо создать вручную. Информацию о создании раздела Зона безопасности, его преимуществах и ограничениях см. в разделе *Информация о разделе Зона безопасности*.

- **Лента**

  Если ленточное устройство подключено к машине, для которой создается резервная копия, или к узлу хранения, в списке хранилищ указывается заданный по умолчанию пул лент. Этот пул создается автоматически.

  Выберите заданный по умолчанию пул или создайте новый, нажав **Добавить хранилище** → **Лента**. Информацию о настройках пула см. в *Создание пула*.

  Для хранения данных на лентах используйте подходящий тип ленты. Подробнее о типах лент в разделе *Типы ленточных носителей*.

- **Определяется сценарием** (доступно для машин под управлением Windows)

  Резервную копию каждой машины можно хранить в папке, определенной сценарием. Поддерживаются сценарии на языках JScript, VBScript или Python.

Примечание

Для использования сценариев Python на машины с агентами необходимо вручную установить Python версии 3.5 или новее.

При развертывании плана защиты на каждой машине будет выполнен заданный сценарий. Выходными данными сценария для каждой машины является путь к локальной или сетевой папке. Если папка не существует, она будет создана. Действует следующее ограничение: сценарии на языке Python не могут создавать папки в сетевых папках. На вкладке **Хранилища резервных копий** каждая папка показана в виде отдельного хранилища резервных копий.

В поле **Тип сценария** выберите тип сценария (**JScript**, **VBScript** или **Python**), а затем импортируйте или скопируйте и вставьте сценарий. Для сетевых папок укажите учетные данные доступа с правами чтения/записи

Например, следующий сценарий JScript выводит расположение хранилища резервных копий для машины в формате `\\bkpsrv\<имя_машины>`:

```
WScript.echo("\\\\bkpsrv\\" + WScript.CreateObject("WScript.Network").ComputerName);
```

В результате резервные копии каждой машины будут сохранены в папке с тем же именем на сервере **bkpsrv**.

О разделе Зона безопасности

Зона безопасности — это безопасный раздел на диске машины, для которой была создана резервная копия. В нем могут храниться резервные копии дисков или файлов этой машины.

Если на диске произойдет физический сбой, резервные копии в разделе Зона безопасности могут быть утрачены. Поэтому Зона безопасности не должна быть единственным хранилищем резервных копий. В корпоративных средах Зону безопасности можно представить как вспомогательное хранилище резервных копий, когда обычное хранилище временно недоступно или подключено через медленный или загруженный канал.

Зона безопасности:

- Обеспечивает восстановление диска на тот же диск, на котором находится резервная копия диска.
- Обеспечивает экономный и удобный метод защиты данных при неправильной работе программного обеспечения или ошибках, вызванных человеческим фактором.
- Устраняет необходимость в отдельном носителе или сетевом подключении для резервного копирования или восстановления данных.

- Может служить основным местом сохранения при использовании репликации резервных копий.

Ограничения:

- Зона безопасности — это раздел на базовом диске. Зону безопасности невозможно организовать на динамическом диске или создать как логический том (управляемый LVM).
- Файловая система раздела Зона безопасности имеет формат FAT32. Поскольку в FAT32 действует ограничение 4 ГБ на размер файлов, то резервные копии большего размера разбиваются на части при сохранении в Зону безопасности. Это не влияет на процедуру резервного копирования и его скорость.
- Зона безопасности не поддерживает формат одного файла резервной копии. При изменении места сохранения на Зону безопасности в плане защиты, который имеет схему резервного копирования **Всегда инкрементное**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

Преобразование диска в результате создания раздела Зона безопасности

- Зона безопасности всегда создается в конце жесткого диска.
- Если в конце диска нераспределенного пространства нет или недостаточно, но существует нераспределенное пространство между томами, то эти тома будут перемещены, чтобы добавить больше нераспределенного пространства в конец диска.
- Если все незанятое пространство собрано, но его не хватает, то программа заберет свободное пространство из томов по выбору, пропорционально уменьшив их размер.
- Тем не менее на томе должно быть свободное пространство для работы операционной системы и приложений, например для создания временных файлов. Программа не будет уменьшать размер тома, на котором свободное пространство меньше или равно 25 % общего объема тома. Только если все тома на диске будут иметь 25 % или меньше свободного пространства, программа продолжит пропорциональное уменьшение томов.

Как следует из приведенных выше соображений, не рекомендуется указывать максимальный возможный размер раздела Зона безопасности. Следствием этого будет отсутствие свободного пространства на любом томе, что может привести к нестабильной работе операционной системы или приложений либо даже к невозможности их запуска.

Важно

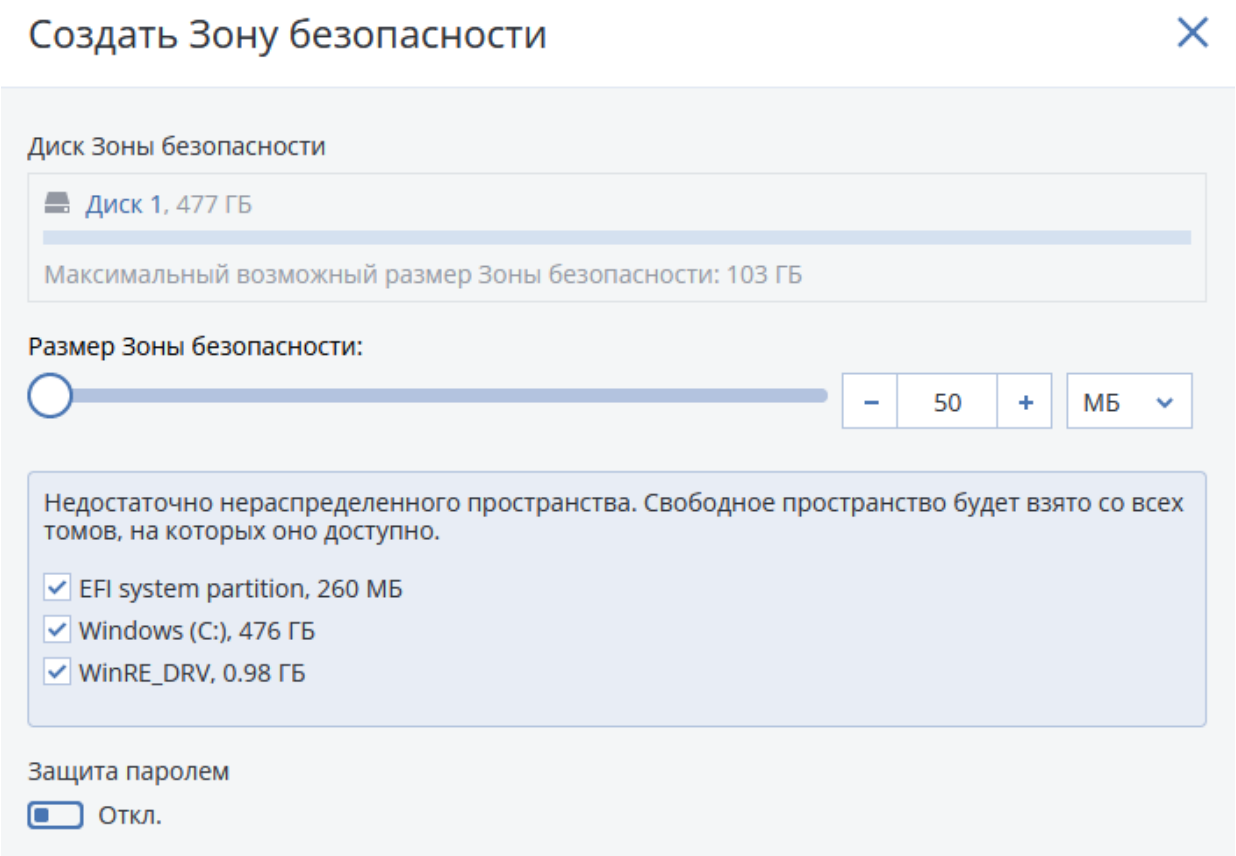
Для перемещения или изменения размера тома, с которого загружена операционная система, потребуется перезагрузка.

Порядок создания Зоны безопасности

1. Выберите машину, на которой необходимо создать Зону безопасности.
2. Щёлкните **Сведения** → **Создать Зону безопасности**.
3. В разделе **Диск Зоны безопасности** щёлкните **Выбрать**, выберите жесткий диск (если их несколько), на котором нужно создать Зону безопасности.

   Программа рассчитает максимальный возможный размер Зоны безопасности.
4. Введите размер Зоны безопасности или перетащите ползунок, чтобы выбрать любой размер в диапазоне между минимальным и максимальным.

   Минимальный размер составляет около 50 МБ в зависимости от геометрии жесткого диска. Максимальный размер складывается из размера нераспределенного пространства и суммарного свободного пространства всех томов диска.
5. Если всего нераспределенного пространства не хватает для указанного размера, то программа заберет свободное пространство от существующих томов. По умолчанию выбраны все тома. Чтобы исключить некоторые тома, щёлкните **Выбрать тома**. В противном случае пропустите этот шаг.



6. [Необязательно] Включите переключатель **Защита паролем** и укажите пароль.

   Этот пароль потребуется для доступа к резервным копиям, расположенным в Зоне безопасности.

Для резервного копирования в раздел Зона безопасности пароль не требуется, за исключением случая, когда резервное копирование выполняется в системе, загруженной с загрузочного носителя.

7. Нажмите кнопку **Создать**.

   Программа покажет предполагаемую структуру разделов. Нажмите кнопку **ОК**.

8. Подождите, пока программа создаст Зону безопасности.

После этого Зону безопасности можно выбрать в разделе **Место сохранения** при создании плана защиты.

Порядок удаления Зоны безопасности

1. Выберите машину с разделом Зона безопасности.
2. Нажмите **Сведения**.
3. Щёлкните значок шестерни рядом с разделом **Зона безопасности**, затем щёлкните **Удалить**.
4. [Дополнительно] Укажите тома, на которые будет добавлено пространство, которое занимала Зона безопасности. По умолчанию выбраны все тома.

   Пространство будет распределено между выбранными томами поровну. Если ни один том не выбран, освобожденное пространство становится нераспределенным.

   Для изменения размера тома, с которого загружена операционная система, потребуется перезагрузка.

5. Щёлкните **Удалить**.

В результате Зона безопасности будет удалена вместе со всеми содержащимися в ней резервными копиями.

О продуктах Кибер Инфраструктура и Кибер Хранилище

Кибер Бэкап поддерживает интеграцию с продуктами Кибер Инфраструктура (версии с 6.5.2 по 6.7.3) и Кибер Хранилище (версии 6.7 и новее).

Развертывание

Чтобы использовать продукт Кибер Инфраструктура или Кибер Хранилище, разверните его локально на вычислительном оборудовании без виртуализации. Чтобы воспользоваться всеми преимуществами данного продукта, необходимо по крайней мере пять физических серверов. Если нужна только функциональность шлюза резервного копирования (Backup Gateway), можно использовать один физический или виртуальный сервер либо настроить кластер шлюзов с максимально большим количеством серверов.

Убедитесь, что настройки времени синхронизированы между сервером управления Кибер Бэкапа и Кибер Инфраструктурой или Кибер Хранилищем. Настройки времени для Кибер Инфраструктуры или Кибер Хранилища можно задать при развертывании. Синхронизация времени по протоколу NTP включена по умолчанию.

Можно развернуть несколько экземпляров Кибер Инфраструктуры или Кибер Хранилища и зарегистрировать их на одном сервере управления.

Регистрация

Регистрация сервера управления Кибер Бэкап выполняется в веб-интерфейсе Кибер Инфраструктуры или Кибер Хранилища. Кибер Инфраструктуру или Кибер Хранилище могут зарегистрировать только администраторы организации и только в данной организации. После регистрации хранилище становится доступным всем отделам организации. Его можно добавить в качестве хранилища резервных копий в любой отдел или организацию.

Обратная операция (отмена регистрации) выполняется в интерфейсе Кибер Бэкап. Щёлкните **Настройки** → **Узлы хранения**, щёлкните требуемый экземпляр Кибер Инфраструктуры или Кибер Хранилища, а затем щёлкните **Удалить**.

Добавление хранилища резервных копий

В отдел или организацию можно добавить только по одному хранилищу резервных копий на каждый экземпляр Кибер Инфраструктуры или Кибер Хранилища. Хранилище, добавленное на уровне отдела, доступно в этом отделе и администраторам организации. Хранилище, добавленное на уровне организации, доступно только администраторам организации.

При добавлении хранилища вы создаете и вводите его имя. Если понадобится добавить существующее хранилище на новый или другой сервер управления, установите флажок **Использовать существующее хранилище в Кибер Инфраструктуре или Кибер Хранилище**, щёлкните **Обзор** и выберите хранилище в списке.

Если на сервере управления зарегистрировано несколько экземпляров Кибер Инфраструктуры или Кибер Хранилища, можно выбрать нужный экземпляр при добавлении хранилища.

Подробнее о добавлении хранилища в Кибер Бэкап см. в документации Кибер Хранилища и документации Кибер Инфраструктуры.

Ограничения для Кибер Инфраструктуры и Кибер Хранилища

- Доступ к Кибер Инфраструктуре или Кибер Хранилищу через интерфейс командной строки невозможен.
- Резервное копирование в Кибер Инфраструктуру или Кибер Хранилище недоступно для конфигураций ESXi.
- После окончания резервного копирования в некоторых случаях размер больших архивов может обновляться с задержкой.

Документация

Документация продуктов доступна по следующим ссылкам:

- Кибер Инфраструктура,
- Кибер Хранилище.

Поддержка хранилищ, работающих в режиме ”Только для добавления”

Кибер Бэкап поддерживает возможность сохранения резервной копии в хранилище, работающем в режиме ”Только для добавления” (Append Only). В качестве таких хранилищ поддерживаются сетевые папки InfoDiode (только локации типа CIFS).

В режиме ”Только для добавления” возможно добавление новых файлов резервных копий как при выполнении резервного копирования, так и при репликации, а изменение или удаление существующих файлов невозможно. Также в этом режиме всегда выполняется только полное резервное копирование. Дедупликация данных отключается автоматически.

Примечание

Скорость резервного копирования в сетевую папку InfoDiode ориентировочно в 6 раз ниже, чем при копировании в обычный сетевой ресурс. Это обусловлено аппаратными и архитектурными особенностями самого устройства InfoDiode и является штатным поведением системы.

Настройка поддержки InfoDiode

Для настройки взаимодействия Кибер Бэкап с сетевой папкой InfoDiode выполните следующие действия в зависимости от установленной ОС на машине с агентом:

- Для ОС Linux:

1. Откройте конфигурационный файл `/etc/Acronis/BackupAndRecovery.config`.
2. Внутри секции `<key name="ProductInformation" />` найдите блок `<key name="Settings">` и добавьте в него новую строку:

   ```
   <value name="WriteOnlyLocationHosts" type="TString">"<IP или имя_машины>"</value>
   ```

   В этом выражении `<IP или имя_машины>` — IP-адрес или доменное имя машины с сетевой папкой InfoDiode. Если машин несколько, укажите значения в общих кавычках, разделяя их запятыми без пробелов (например, "`192.168.10.12,192.168.10.13,diode-server.local`").
3. Перезапустите службу агента командой:

   ```
   systemctl restart acronis_mms.service
   ```

- Для ОС Windows:
  1. Откройте редактор реестра ОС Windows **Regedit**.
  2. Перейдите в раздел реестра: `HKLM\SOFTWARE\Acronis\BackupAndRecovery\Settings`.
  3. Создайте в этом разделе строковый параметр (REG_SZ) с именем `WriteOnlyLocationHosts`.

     В качестве значения созданного параметра укажите IP-адрес или доменное имя машины с сетевой папкой InfoDiode. Если машин несколько, укажите значения, разделяя их запятыми без пробелов (например, `192.168.10.12,192.168.10.13,diode-server.local`).
  4. Перезапустите службу агента, последовательно выполнив команды:

     ```
     net stop MMS
     net start MMS
     ```

После добавления параметра `WriteOnlyLocationHosts` в систему в файле `mms.log` появится соответствующая запись, например:

```
Write only location used for backup command.
Write only location used for replication command.
```

⚠ Предупреждение

Параметр `WriteOnlyLocationHosts` должен быть добавлен в систему до запуска резервного копирования. В противном случае резервное копирование или репликация в сетевую папку InfoDiode завершится сбоем в соответствии с настройками параметра *"Обработка ошибок"*.

Расписание

В расписании используются настройки времени (включая часовой пояс) операционной системы, в которой установлен агент. Инструкции по настройке агентов приведены в главе *Установка*.

Пример: если план защиты, который применен к нескольким машинам в разных часовых поясах, запланирован к запуску в 21:00, то процесс резервного копирования на каждой машине начнется в 21:00 по местному времени данной машины.

Схема резервного копирования

Можно выбрать одну из стандартных схем резервного копирования или создать собственную. Схема входит в состав плана защиты и содержит расписание и методы создания резервных копий.

В разделе **Схема резервного копирования** выберите один из перечисленных ниже вариантов.

- [Только резервные копии на уровне дисков] **Всегда инкрементное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска резервного копирования.

  Чтобы сменить частоту создания резервной копии, перетащите ползунок и задайте расписание резервного копирования.

  Для резервных копий используется новый формат резервной копии в виде одного файла.

  Эта схема недоступна при выполнении резервного копирования на SFTP-сервер или в зону безопасности.

- **Всегда полное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска резервного копирования.

  Чтобы сменить частоту создания резервной копии, перетащите ползунок и задайте расписание резервного копирования.

  Каждый раз создаются полные резервные копии.

- **Еженедельно полное, ежедневно инкрементное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Дни недели и время запуска резервного копирования можно изменить.

  Раз в неделю создается полная резервная копия. Остальные копии будут инкрементными. Время создания полной резервной копии определяется параметром **Еженедельное резервное копирование** (щёлкните значок шестеренки и выберите **Параметры резервного копирования** → **Еженедельное**

резервное копирование).

- **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)**

  Схема GFS (Grandfather-Father-Son) или ”дед-отец-сын” — иерархическая политика резервного копирования, при которой для разных типов резервных копий определяются различные периодичность создания и сроки хранения. Например: резервные копии уровня ”сын” (инкрементные) создаются ежедневно и хранятся одну неделю, резервные копии уровня ”отец” (дифференциальные) создаются каждую неделю и хранятся один месяц, резервные копии уровня ”дед” (полные) создаются ежемесячно и хранятся год.

  По умолчанию инкрементное резервное копирование выполняется ежедневно с понедельника по пятницу; дифференциальное резервное копирование выполняется каждую субботу; полное резервное копирование выполняется в первый день каждого месяца. Это расписание и время запуска резервного копирования можно изменить. Для установки сроков хранения требуется настроить правила хранения (см. раздел *Правила хранения*).

  Данная схема резервного копирования отображается как схема **Пользовательская** на панели плана защиты.

  > **Примечание**
  >
  > При выборе этой схемы при создании резервных копий на лентах рекомендуется включить параметр **Использовать наборы лент в пуле лент, выбранных для резервного копирования** в окне **Параметры резервного копирования** → **Управление лентами** (см. *Управление лентами*). Рекомендуется выбрать **Использовать отдельный набор лент** с шаблоном **День недели**.
  >
  > В таком случае для каждого дня недели будет использоваться отдельная лента. Резервные копии, созданные в понедельник, будут храниться на одной ленте. Резервные копии, созданные во вторник, будут храниться на другой ленте. И так далее.

- **Другое**

  Задайте расписания для полных, дифференциальных и инкрементных резервных копий.

  Дифференциальное резервное копирование не выполняется для данных SQL и Exchange.

Для любой схемы резервного копирования можно запланировать резервное копирование по событиям, а не по времени. Для этого выберите тип события в настройках расписания. Дополнительную информацию см. в разделе *Расписание по событиям*.

Дополнительные параметры расписания

Для каждого места сохранения можно выполнить следующие действия:

- Задайте условия запуска резервного копирования так, чтобы запланированное резервное копирование выполнялось только при соблюдении этих условий. Дополнительную информацию см. в разделе *Условия запуска*.
- Задать интервал дат, в течение которого будет использоваться указанное расписание. Установите флажок **Выполнять план в диапазоне дат** и укажите диапазон дат.
- Отключить расписание. Когда расписание отключено, правила хранения не применяются за исключением случая, при котором резервное копирование запущено вручную.
- Настроить задержку с момента запланированного времени. Значение задержки для каждой машины выбирается случайно и находится в диапазоне от нуля до максимального значения, которое вы укажете. Параметр может быть полезен для резервного копирования нескольких машин в сетевое хранилище, чтобы избежать чрезмерной загрузки сети.

  Щёлкните значок шестеренки, затем последовательно выберите пункты **Параметры резервного копирования** → **Планирование задач**. Установите флажок **Распределять время запуска резервного копирования по доступному времени**, затем укажите максимальную задержку. Продолжительность задержки для каждой машины определяется при применении плана защиты к машине и остается неизменной до тех пор, пока в плане защиты не будет изменено максимальное значение задержки.
- Щёлкните **Подробнее**, чтобы получить доступ к указанным ниже параметрам:
  - **Если машина выключена, выполнить пропущенные задания при ее загрузке** (по умолчанию отключено)
  - **Отключить переход в спящий режим или режим гибернации при выполнении резервного копирования** (по умолчанию включено)

    Этот параметр действует только для машин с ОС Windows.
  - **Выйти из спящего режима или режима гибернации для запуска запланированного резервного копирования** (отключено по умолчанию)

    Этот параметр действует только для машин с ОС Windows. Этот параметр не действует, когда машина выключена, т. е. данный параметр не использует функциональность Wake-on-LAN.

Планирование по событиям

При составлении расписания для плана защиты выберите тип события в настройках расписания. Резервное копирование будет запущено, как только произойдет событие.

Можно выбрать одно из следующих событий:

- **С заданной периодичностью**

  Через определенное время после завершения последнего успешного резервного копирования в рамках одного плана защиты. Укажите период времени.

  > **Примечание**
  >
  > Расписание составляется на основе успешно выполненных операций резервного копирования. При сбое операции резервного копирования планировщик не будет запускать задание заново, пока оператор не запустит план вручную, и он не будет выполнен без сбоев.

- **При входе пользователя в учетную запись**

  По умолчанию резервное копирование запустится при входе в учетную запись любого пользователя. Вместо любого пользователя можно указать конкретную учетную запись.

- **При выходе пользователя из учетной записи**

  По умолчанию резервное копирование запустится при выходе из учетной записи любого пользователя. Вместо любого пользователя можно указать конкретную учетную запись.

  > **Примечание**
  >
  > Резервное копирование не будет запущено при завершении работы системы, поскольку завершение работы не эквивалентно выходу из учетной записи.

- **При запуске системы**
- **При завершении работы системы**
- **По событию в журнале событий Windows**

  Вы должны указать *свойства события*.

В следующей таблице перечислены события, доступные для различных данных в ОС Windows и Linux.

Элементы для резервного копирования	С заданной периодичностью	При входе пользователя в учетную запись	При выходе пользователя из учетной записи	При запуске системы	При завершении работы системы	По событию в журнале событий Windows
Диски/тома или файлы (физические машины)	Windows, Linux	Windows	Windows	Windows, Linux	Windows	Windows
Диски/тома (виртуальные машины)	Windows, Linux	–	–	–	–	–
Конфигурация ESXi	Windows, Linux	–	–	–	–	–
Базы данных и почтовые ящики Exchange	Windows	–	–	–	–	Windows
Базы данных SQL	Windows	–	–	–	–	Windows

По событию в журнале событий Windows

Можно запланировать запуск резервного копирования в случае записи определенного события в один из журналов событий Windows (**журнал приложения**, **журнал безопасности** или **системный журнал**).

Например, можно задать план защиты, по которому аварийное полное резервное копирование данных будет запускаться автоматически, как только ОС Windows обнаружит вероятность отказа жесткого диска.

Для обзора событий и просмотра свойств событий используйте встраиваемое **Средство просмотра событий**, доступное в консоли **Управление компьютером**. Журнал **Безопасность** может быть открыт только из-под учетной записи, которая входит в группу **Администраторы**.

Свойства событий

Имя журнала

Указывает имя журнала. Выберите имя стандартного журнала (**Приложение**, **Безопасность** или **Система**) из списка или введите имя журнала. Пример: **Microsoft Office Sessions**

Источник события

Указывает источник события. Как правило, это программа или компонент системы, который вызвал событие. Пример: **диск**.

Любой источник событий с указанной строкой запустит запланированное резервное копирование. Этот параметр не является регистрозависимым. Таким образом, если указана строка ”служб”, то источники событий **Диспетчер служб** и **Служба времени** вызовут резервное копирование.

Тип события

Указывает тип события: **Ошибка**, **Предупреждение**, **Информация**, **Успех аудита** или **Ошибка аудита**.

Идентификатор события

Указывает номер события, который обычно определяет тип событий среди событий из одного источника.

Например, событие **Ошибка** с источником события **диск** и идентификатором события **7** происходит в случае, если ОС Windows обнаруживает плохой блок на диске, а событие **Ошибка** с источником события **диск** и идентификатором события **15** — в случае, если диск еще недоступен.

Пример. Аварийное резервное копирование при обнаружении ”плохого блока”

Появление одного или нескольких плохих блоков на жестком диске обычно означает, что диск скоро выйдет из строя. Предположим, требуется план защиты, который создаст резервную копию данных жесткого диска в такой ситуации.

Если ОС Windows обнаруживает плохой блок на жестком диске, это событие записывается в журнал **Система** с источником события **диск** и номером события **7**, тип этого события — **ошибка**.

Во время создания плана введите или выберите следующее в разделе **Расписание**.

- Имя журнала: **Система**
- Источник события: **диск**
- Тип события: **Ошибка**
- Идентификатор события: **7**

Важно

Чтобы убедиться в том, что резервное копирование будет выполнено несмотря на присутствие плохих блоков, необходимо настроить резервное копирование на пропуск плохих блоков. Для этого в разделе **Параметры резервного копирования** выберите **Обработка ошибок** и установите флажок **Пропуск поврежденных секторов**.

Условия запуска

Такие настройки делают планировщик более гибким, позволяя выполнять резервное копирование в соответствии с определенными условиями. Если условий несколько, для запуска резервного копирования все они должны выполняться одновременно. Начальные условия не действуют, если резервная копия запущена вручную.

Для доступа к этим настройкам щёлкните **Показать больше** при настройке расписания для плана защиты.

Поведение планировщика заданий в случае, если событие происходит, а одно или несколько условий не выполнено, определяется параметром резервного копирования *Условия запуска резервного копирования*. Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка резервного копирования становится рискованной, можно установить временной промежуток, после которого задание запустится независимо от условия.

В следующей таблице перечислены условия запуска, доступные для различных данных в ОС Windows и Linux.

Элементы для резервного копирования	**Диски/тома или файлы (физические машины)**	**Диски/тома (виртуальные машины)**	**Конфигурация ESXi**	**Базы данных и почтовые ящики Exchange**	**Базы данных SQL**
Пользователь неактивен	Windows	–	–	–	–
Хост хранилища резервных копий доступен	Windows, Linux	Windows, Linux	Windows, Linux	Windows	Windows
Пользователи завершили сеанс	Windows	–	–	–	–
В интервале времени	Windows, Linux	Windows, Linux	–	–	–
Сэкономить заряд батареи	Windows	–	–	–	–
Не запускать при работе на лимитном подключении	Windows	–	–	–	–
Не запускать при подключении к следующим сетям Wi-Fi	Windows	–	–	–	–

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Элементы для резервного копирования	Диски/тома или файлы (физические машины)	Диски/тома (виртуальные машины)	Конфигурация ESXi	Базы данных и почтовые ящики Exchange	Базы данных SQL
Проверить IP-адрес устройства	Windows	–	–	–	–

Пользователь неактивен

”Пользователь неактивен” означает, что машина заблокирована или на экране отражается заставка.

Пример

Запускать резервное копирование на машине каждый день в 21:00 — желательно, когда пользователь неактивен. Если в 23:00 пользователь все еще активен, все равно запустить резервное копирование.

- Расписание: Ежедневно, запускать каждый день. Запускать в: **21:00**.
- Условие: **Пользователь неактивен**.
- Условия запуска резервного копирования: **Ждать выполнения условий, все равно запустить резервное копирование через 2 часа**.

В результате:

- Если пользователь становится неактивным до 21:00, резервное копирование начинается в 21:00.
- Если пользователь становится неактивным между 21:00 и 23:00, резервное копирование выполняется сразу после того, как пользователь стал неактивным.
- Если пользователь все еще активен в 23:00, резервное копирование начинается в 23:00.

Хост хранилища резервных копий доступен

Строка ”Хост хранилища резервных копий доступен” означает, что машина, служащая назначением для хранения резервных копий, доступна в сети.

Данное условие эффективно для сетевых папок и хранилищ под управлением узла хранения.

Данное условие перекрывает доступность хоста, а не доступность самого хранилища. Например, если хост доступен, но отсутствует доступ к сетевой папке на хосте или учетные данные для доступа к папке недействительны, условия все еще считаются соблюденными.

Пример

Резервное копирование данных в сетевую папку выполняется каждый рабочий день в 21:00. Если машина, на которой находится папка, в это время недоступна (например, из-за профилактических работ), вам необходимо пропустить резервное копирование и ждать запланированного запуска на следующий рабочий день.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: **21:00**.
- Условие: **Хост хранилища резервных копий доступен**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

- Если в 21:00 хост местоположения доступен, резервное копирование начнет выполняться вовремя.
- Если в 21:00 хост с хранилищем недоступен, резервное копирование будет выполнено в следующий рабочий день, когда хост будет доступен.
- Если хост с хранилищем вообще недоступен по рабочим дням в 21:00, задание вообще не будет выполняться.

Пользователи завершили сеанс

Позволяет поставить выполнение резервного копирования на ожидание до тех пор, пока все пользователи не выйдут из системы Windows.

Пример

Запуск резервного копирования в 20:00 каждую пятницу, желательно, когда все пользователи завершили сеанс. Если один из пользователей все еще находится в системе в 23:00, все равно запустить резервное копирование

- Расписание: Еженедельно, по пятницам. Запускать в: **20:00**.
- Условие: **Пользователи завершили сеанс**.
- Условия запуска резервного копирования: **Ждать выполнения условий, все равно запустить резервное копирование через 3 часа**.

В результате:

- Если все пользователи выходят из системы к 20:00, резервное копирование начинает выполняться в 20:00.
- Если последний пользователь выходит из системы между 20:00 и 23:00, резервное копирование

начинает выполняться сразу после выхода пользователя из системы.

- Если хотя бы один пользователь все еще активен в 23:00, резервное копирование начинается в 23:00.

В интервале времени

Ограничивает время запуска резервного копирования определенным интервалом.

Пример

Для резервного копирования данных пользователей и серверов компания использует разные области на одном и том же сетевом устройстве хранения. Рабочий день начинается в 8:00 и заканчивается в 17:00. Копирование данных пользователя должно начинаться, как только пользователи выйдут из системы, но не раньше 16:30. Каждый день в 23:00 начинается резервное копирование серверов компании. К этому времени резервное копирование пользовательских данных должно закончиться, чтобы освободить пропускную способность сети. Считается, что резервное копирование данных пользователей занимает не больше часа, так что самое позднее время начала резервного копирования — 22:00. Если в заданный период времени пользователь все еще находится в системе или выходит из системы в любое другое время, резервное копирование пользовательских данных не производится, то есть, резервное копирование пропускается.

- Событие: **При выходе пользователя из системы**. Укажите учетную запись пользователя: **Любой пользователь**.
- Условие: **В интервале времени** от **16:30** до **22:00**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

- Если пользователь выходит из системы между 16:30:00и 22:00:00, задание резервного копирования запускается сразу после выхода пользователя из системы.
- Если пользователь выходит из системы в любое другое время, резервное копирование пропускается.

Сэкономить заряд батареи

Предотвращает резервное копирование, если устройство (ноутбук или планшетный ПК) не подключено к источнику питания. В зависимости от значения параметра резервного копирования *Условия запуска резервного копирования* пропущенное резервное копирование запускается или не запускается после подключения устройства к источнику питания. Доступны следующие параметры:

- **Не запускать при работе от батареи**

  Резервное копирование запускается, только если устройство подключено к источнику питания.

- **Запускать при работе от батареи, если уровень ее заряда больше**

  Резервное копирование запускается, если устройство подключено к источнику питания или если уровень заряда аккумуляторной батареи больше указанного значения.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство не подключено к источнику питания (например, пользователь допоздна задерживается на собрании), уместно не выполнять резервное копирование до тех пор, пока устройство не будет подключено к источнику питания. Это позволит сэкономить заряд батареи.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Сэкономить заряд батареи**, **Не запускать при работе от батареи**.
- Условия запуска резервного копирования: **Ожидайте выполнения условий**.

В результате:

- Если в 21:00 устройство подключено к источнику питания, резервное копирование начнется немедленно.
- Если в 21:00 устройство работает от аккумуляторной батареи, резервное копирование начнется как только устройство будет подключено к источнику питания.

Не запускать при работе на лимитном подключении

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к Интернету через лимитное подключение в Windows. Дополнительную информацию о лимитных подключениях в Windows см. в документации Microsoft.

Дополнительная мера предотвращения резервного копирования через мобильные точки доступа: если включено условие **Не запускать при работе на лимитном подключении**, условие **Не запускать при подключении к следующим сетям Wi-Fi** включается автоматически. По умолчанию указаны следующие сетевые имена: ”android”, ”phone”, ”mobile” и ”modem”. Эти имена можно удалить из списка, щёлкнув значок **X**.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к Интернету через лимитное подключение (например, пользователь в командировке), возможно, предпочтительнее будет не выполнять резервное копирование, дождавшись запланированного запуска на следующий рабочий день. Это позволит сэкономить сетевой трафик.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: **21:00**.
- Условие: **Не запускать при работе на лимитном подключении**
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

- Если в 21:00 устройство не подключено к Интернету через лимитное подключение, резервное копирование начнется немедленно.
- Если в 21:00 устройство подключено к Интернету через лимитное подключение, резервное копирование начнется на следующий рабочий день.
- Если устройство всегда подключено к Интернету через лимитное подключение по рабочим дням 21:00, то резервное копирование вообще не запускается.

Не запускать при подключении к следующим сетям Wi-Fi

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к любой указанной беспроводной сети. Можно указать имена сети Wi-Fi, также известные как идентификаторы беспроводной сети (SSID).

Это ограничение применяется ко всем сетям, которые содержат указанное имя (с учетом регистра) как подстроку в своем имени. Например, если в качестве сетевого имени указать ”phone”, резервная копия не запустится, если устройство подключено к любой из указанных ниже сетей: ”John’s iPhone”, ”phone_wifi”, или ”my_PHONE_wifi”.

Это условие полезно, чтобы предотвратить резервное копирование, когда устройство подключено к Интернету через мобильную точку доступа.

Дополнительная мера предотвращения резервного копирования через мобильные точки доступа: условие **Не запускать при подключении к следующим сетям Wi-Fi** включается автоматически при включении условия **Не запускать при работе на лимитном подключении**. По умолчанию указаны следующие сетевые имена: ”android”, ”phone”, ”mobile” и ”modem”. Эти имена можно удалить из списка, щёлкнув значок X.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к Интернету через мобильную точку доступа (например, ноутбук подключен через мобильный телефон в режиме модема), возможно, предпочтительнее будет не выполнять резервное копирование, дождавшись запланированного запуска на следующий рабочий день.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: **21:00**.
- Условие: **Не запускать при подключении к следующим сетям**, **Сетевое имя: <SSID сети доступа>**.
- Условия запуска резервного копирования: **Пропустить запланированное резервное копирование**.

В результате:

- Если в 21:00 машина не подключена к указанной сети, резервное копирование начнется немедленно.
- Если в 21:00 машина подключена к указанной сети, резервное копирование начнется на следующий рабочий день.
- Если машина всегда подключено к указанным сетям по рабочим дням 21:00, то резервное копирование вообще не запускается.

Проверить IP-адрес устройства

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если любой из IP-адресов устройства находится в указанном диапазоне IP-адресов или вне этого диапазона. Доступны следующие параметры:

- **Запустить, если вне диапазона IP-адресов**
- **Запустить, если в диапазоне IP-адресов**

В обоих параметрах можно указать разные диапазоны. Поддерживаются только адреса IPv4.

Это условие позволяет избежать затрат на передачу больших объемов данных, если пользователь физически находится на большом расстоянии. Кроме того, оно помогает предотвратить резервное копирование через подключение VPN.

Пример

Резервное копирование данных выполняется каждый рабочий день в 21:00. Если устройство подключено к корпоративной сети через VPN-туннель (например, пользователь работает из дома), уместно не выполнять резервное копирование до тех пор, пока устройство не будет в офисе.

- Расписание: ежедневно, запускать с понедельника по пятницу. Запускать в: 21:00.
- Условие: **Проверить IP-адрес устройства**, **Запустить, если вне диапазона IP-адресов**, **От: <начало диапазона IP-адресов VPN>**, **До: <конец диапазона IP-адресов VPN>**.
- Условия запуска резервного копирования: **Ожидайте выполнения условий**.

В результате:

- Если в 21:00 IP-адрес машины не будет находится в указанном диапазоне, резервное копирование запустится немедленно.
- Если в 21:00 IP-адрес машины будет находится в указанном диапазоне, резервное копирование запустится как только устройство получит IP-адрес вне диапазона IP-адресов VPN.
- Если IP-адрес машины всегда находится в указанном диапазоне по рабочим дням в 21:00, резервное копирование вообще не будет выполняться.

Правила хранения

Для настройки правил хранения резервных копий выполните следующие действия:

1. Нажмите **Срок хранения**.
2. В разделе **Очистка** выберите один из перечисленных ниже вариантов:
   - **По сроку хранения** (по умолчанию)

     Укажите, в течение какого срока нужно хранить резервные копии, созданные планом защиты. По умолчанию правила хранения задаются отдельно для каждого набора резервных копий. Чтобы использовать одно правило для всех резервных копий, щёлкните **Переключиться на одно правило для всех наборов резервных копий**.
   - **По числу резервных копий**

     Укажите максимальное количество хранимых резервных копий.
   - **По общему размеру резервных копий**

     Укажите максимальный общий размер резервных копий.

     Данная настройка доступна только для формата резервных копий ”Версия 11” (см. раздел

Формат резервной копии).

Данная настройка недоступна в схеме резервного копирования **Всегда инкрементное** или при резервном копировании на сервер SFTP или на ленточное устройство.

- **Хранить резервные копии неограниченное время**

3. Выберите время для запуска очистки:
   - **После резервного копирования** (по умолчанию)

     Правила хранения будут применены после создания новой резервной копии.
   - **До резервного копирования**

     Правила хранения будут применены до создания новой резервной копии.

     Эта настройка недоступна при резервном копировании кластеров Microsoft SQL Server или сервера Microsoft Exchange.
4. Нажмите **Готово**.

В результате правила хранения резервных копий будут установлены.

Особенности:

- Последняя резервная копия, созданная согласно плану защиты, сохраняется в любом случае, даже если это нарушает правило хранения. Не пытайтесь удалить единственную резервную копию, применяя правила хранения перед резервным копированием.
- Резервные копии, которые хранятся на ленточном накопителе, не удаляются физически до перезаписи данных на ленте.
- Если в соответствии со схемой резервного копирования и форматом резервного копирования каждая резервная копия хранится в отдельном файле, этот файл не может быть удалён до окончания времени существования всех зависимых от него резервных копий (инкрементных и дифференциальных). Для хранения резервных копий, удаление которых отложено, требуется дополнительное место на диске. Кроме того, возраст, количество или размер резервных копий могут превышать указанные вами значения.

  Это поведение можно изменить, используя параметр резервного копирования *Консолидация резервной копии*.
- Правила хранения — составная часть плана защиты. Они прекращают действовать для резервных копий машины, как только с неё отозван или удалён план защиты или когда сама машина удалена с сервера управления. Если вам больше не нужны резервные копии, созданные данным планом, удалите их, как описано в разделе *Удаление резервных копий*.

Защита паролем

Важно

Если пароль утерян, восстановить защищённые резервные копии будет невозможно.

Настройка защиты паролем в планах защиты

Чтобы включить защиту паролем, укажите соответствующие параметры при создании плана защиты. После применения плана защиты изменить их будет невозможно. Чтобы использовать другие настройки защиты паролем, создайте новый план защиты.

Определение настроек защиты паролем в планах защиты

1. На панели плана защиты переведите переключатель **Защита паролем** в положение **Включено**.
2. Укажите и подтвердите пароль.
3. Выберите один из следующих уровней защиты паролем:
   - **Базовый** — резервные копии будут защищены паролем с уровнем защиты **Базовый**.
   - **Средний** — резервные копии будут защищены паролем с уровнем защиты **Средний**.
   - **Высокий** — резервные копии будут защищены паролем с уровнем защиты **Высокий**.
4. Нажмите кнопку **ОК**.

Особенности защиты паролем

Чем выше уровень защиты паролем, тем дольше выполняется план защиты.

Пароль не сохраняется на диске или в резервных копиях. Это позволяет обезопасить данные резервной копии от несанкционированного доступа, но восстановление утраченного пароля невозможно.

Преобразование в виртуальную машину

Преобразование в виртуальную машину возможно только для резервных копий на уровне дисков. Если в резервной копии есть системный том и вся информация, необходимая для запуска операционной системы, то созданная виртуальная машина может запускаться без стороннего содействия. В противном случае можно добавить ее виртуальные диски на другую виртуальную машину.

Методы преобразования:

- Регулярное преобразование.

Есть два способа настроить регулярное преобразование:

- *Включить преобразование в план защиты*

  Преобразование будет выполняться после каждого резервного копирования (если настроено для первичного хранилища) или после каждой репликации (если настроено для второго и последующих хранилищ).

- *Создать отдельный план преобразования*

  Этот метод позволяет указать отдельное расписание преобразования.

- *Восстановление в новую виртуальную машину*

  Этот метод позволяет выбрать диски для восстановления и задать настройки для каждого виртуального диска. Этот метод позволяет выполнять преобразование только один раз или время от времени, например, для выполнения *миграции с физической машины на виртуальную*.

Поддерживаемые типы виртуальных машин

Преобразование резервной копии в виртуальную машину можно выполнить в том же агенте, который использовался для ее создания, или в другом агенте.

Чтобы выполнить преобразование в VMware ESXi или Hyper-V, необходимо иметь хост ESXi или Hyper-V и агент защиты (агент для VMware или агент для Hyper-V), который управляет этим хостом.

Преобразование в файлы VHDX предполагает, что файлы будут подключаться к виртуальной машине Hyper-V как виртуальные диски.

В следующей сводной таблице указаны типы виртуальных машин, которые могут быть созданы теми или иными агентами:

Тип ВМ	Агент для VMware	Агент для Hyper-V	Агент для Windows	Агент для Linux
VMware ESXi	+			
Microsoft Hyper-V		+		
VMware Workstation	+	+	+	+
Файлы VHDX	+	+	+	+

Ограничения

- Агент для Windows, агент для VMware (Windows) и агент для Hyper-V не могут преобразовать резервные копии, которые хранятся в системе NFS.
- Резервные копии, которые хранятся в системе NFS или на сервере SFTP, невозможно преобразовать в рамках *отдельного плана преобразования*.

- Резервные копии, которые хранятся в Зоне безопасности, могут быть преобразованы только агентом, который выполняется на той же машине.
- Резервные копии с логическими томами Linux (LVM) можно преобразовать, только если они созданы агентом для VMware или агентом для Hyper-V и ориентированы на один гипервизор. Преобразование между различными гипервизорами не поддерживается.
- При преобразовании резервных копий машины Windows в файлы VMware Workstation или VHDX полученная виртуальная машина наследует тип ЦП от машины, которая выполняет преобразование. В результате этого в гостевой операционной системе устанавливаются соответствующие драйверы ЦП. Если гостевая система запускается на хосте с ЦП другого типа, в гостевой системе отображается ошибка драйвера. Обновите этот драйвер вручную.

Регулярное преобразование в ESXi и Hyper-V по сравнению с запуском виртуальной машины с резервной копии

Обе операции предоставляют в ваше распоряжение виртуальную машину, которую можно запустить за считанные секунды в случае сбоя оригинальной машины.

Для регулярного преобразования требуются ресурсы ЦП и памяти. Файлы виртуальной машины постоянно занимают место в хранилище данных. Если рабочий хост используется для преобразования, это может быть непрактично. Однако производительность виртуальной машины ограничена только ресурсами хоста.

Во втором случае ресурсы потребляются только в том случае, когда виртуальная машина запущена. Место на хранилище данных требуется только для того, чтобы сохранить изменения в виртуальных дисках. Однако виртуальная машина может работать медленно, поскольку хост работает с виртуальными дисками не напрямую, а через агент, который считывает данные с резервной копии. Кроме того, виртуальная машина является временной. Сделать машину постоянной можно только для ESXi.

Преобразование в виртуальную машину в плане защиты

Можно настроить преобразование в виртуальную машину с любой резервной копии или хранилища репликации, указанных в плане защиты. Преобразование будет выполняться после каждого резервного копирования или репликации.

Информацию о предварительных требованиях и ограничениях см. в разделе *Преобразование в виртуальную машину*.

Порядок настройки преобразования в виртуальную машину в плане защиты

1. Определите, с какого хранилища резервных копий необходимо выполнить преобразование.
2. На панели плана защиты для этого хранилища щёлкните **Преобразовать в виртуальную машину**.
3. Включите параметр **Преобразование**.
4. В поле **Преобразовать в** выберите тип целевой виртуальной машины. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:
   - VMware ESXi,
   - Microsoft Hyper-V,
   - VMware Workstation,
   - Файлы VHDX.
5. Выполните одно из следующих действий:
   - Для VMware ESXi и Hyper-V: щёлкните **Хост**, выберите целевой хост, а затем укажите новый шаблон имени машины.
   - Для виртуальных машин других типов: в поле **Путь** укажите расположение для сохранения файлов виртуальной машины и шаблон имени файла.

   Имя по умолчанию — **[Имя машины]_converted**.
6. [Необязательно] Щёлкните **Агенты, которые будут выполнять преобразование** и выберите агент.

   Это может быть агент, который выполняет резервное копирование (по умолчанию), или агент, установленный на другой машине. В последнем случае необходимо сохранить резервные копии в общем хранилище, например в сетевой папке, чтобы другая машина могла получить к нему доступ.
7. [Необязательно] Для VMware ESXi и Hyper-V можно также выполнить следующие действия:
   - Щёлкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
   - Измените режим распределения ресурса дисков. По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щёлкните **Настройки ВМ**.
8. Нажмите кнопку **Готово**.

Как работает обычное преобразование в виртуальную машину

То, как выполняются повторные преобразования, зависит от того, где нужно создать виртуальную машину.

- **Если нужно сохранить виртуальную машину как набор файлов:** при каждом преобразовании виртуальная машина будет повторно создаваться с нуля.
- **Если нужно создать виртуальную машину на сервере виртуализации:** при преобразовании инкрементной или дифференциальной резервной копии программа обновляет существующую виртуальную машину, а не создает ее заново. Обычно такое преобразование происходит быстрее. Таким образом снижается загруженность сети и потребление ресурсов ЦП хоста, на котором выполняется преобразование. Если обновление виртуальной машины невозможно, программа воссоздает ее с нуля.

Ниже подробно описаны оба случая.

Сохранение виртуальной машины в виде набора файлов

В результате первого преобразования будет создана новая виртуальная машина. При каждом последующем преобразовании эта машина будет повторно создаваться с нуля. Сначала старая машина временно переименовывается. Затем создается новая виртуальная машина с предыдущим именем старой машины. Если эта операция завершается успешно, старая машина удаляется. При сбое операции новая машина удаляется, а старой машине возвращается предыдущее имя. Таким образом, после преобразования всегда остается одна машина. Однако на время преобразования необходимо дополнительное дисковое пространство для размещения временной машины.

Создание виртуальной машины на сервере виртуализации

В результате первого преобразования создается новая виртуальная машина. Все последующие преобразования выполняются следующим образом.

- Если с момента последнего преобразования выполнялось *полное резервное копирование*, виртуальная машина создается заново с нуля, как описано ранее в этом разделе.
- В противном случае существующая виртуальная машина обновляется в соответствии с изменениями, которые произошли после последнего преобразования. Если обновление невозможно (например, удалены промежуточные моментальные снимки, см. ниже), виртуальная машина создается заново.

Промежуточные моментальные снимки

Чтобы иметь возможность обновить виртуальную машину, программа хранит несколько ее промежуточных моментальных снимков Эти моментальные снимки имеют имена **Backup...** и **Replica...**; их необходимо хранить. Ненужные моментальные снимки удаляются автоматически.

Последний моментальный снимок **Replica...** соответствует результату последнего преобразования. Можно перейти к этому моментальному снимку, чтобы вернуть машину в это состояние, например если после работы с машиной нужно отменить внесенные изменения.

Другие моментальные снимки предназначены для внутреннего использования программой.

Репликация

В данном разделе описана репликация резервных копий, которая включена в план защиты. Информацию о создании отдельного плана репликации см. в разделе *Обработка данных вне хоста (off-host)*.

Если включить репликацию резервных копий, то каждая резервная копия копируется в другое хранилище сразу же после создания. Если более ранние резервные копии не были реплицированы (например, из-за сбоя сетевого подключения), программа также реплицирует все резервные копии, появившиеся после последней успешной репликации.

Реплицированные резервные копии не зависят от резервных копий, оставшихся в исходном хранилище и наоборот. Можно восстановить данные из любой резервной копии без доступа к другим хранилищам.

Примеры использования

- **Надежное аварийное восстановление**

  Храните резервные копии локально (для немедленного восстановления) и удаленно (чтобы защитить резервные копии при отказе локального хранилища данных или стихийных бедствиях).

- **Сохранение только последних точек восстановления**

  Удалите старые резервные копии из быстродействующего запоминающего устройства в соответствии с правилами резервного копирования, чтобы без необходимости не использовать емкость хранения данных.

Поддерживаемые расположения

Возможные расположения источников и целевых хранилищ резервных копий при репликации приведены в таблице.

Источник репликации	**Целевое хранилище репликации**									
	Локальная папка	**Сетевая папка**	**Папка NFS**	**SFTP-сервер**	**Зона безопасности**	**Ленточное устройство**	**Хранилище под управлением узла хранения**			**Кибер Инфраструктура или Кибер Хранилище**
							с дедупликацией	**без дедупликации**	**с лентами**	
Локальная папка	+	+	+[2]	+	+	Локальные ленты	+[3]	+	+	+
Сетевая папка	+	+	+[с. 360, 2]	+	+	+	+[с. 360, 3]	+	+	+
Папка NFS	+	+	+[с. 360, 2]	+	+	+	+[с. 360, 3]	+	+	+
SFTP-сервер	+	+	+[с. 360, 2]	+	+	+	+[с. 360, 3]	+	+	+
Зона безопасности	+	+	+[с. 360, 2]	+	+	+	+[с. 360, 3]	+	+	+
Ленточное устройство	—	—	—	—	—	—	—	—	—	—
Хранилище под управлением узла хранения с дедупликацией	+[1]	+	+[с. 360, 2]	+	+	+	+[с. 360, 3]	+	+	+

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Источник репликации	Целевое хранилище репликации									
	Локальная папка	Сетевая папка	Папка NFS	SFTP-сервер	Зона безопасности	Ленточное устройство	Хранилище под управлением узла хранения			Кибер Инфраструктура или Кибер Хранилище
							с дедупликацией	без дедупликации	с лентами	
Хранилище под управлением узла хранения без дедупликации	+[1]	+	+[2]	+	+	+	+[3]	+	+	+
Хранилище под управлением узла хранения с лентами	—	—	—	—	—	—	—	—	—	—
Кибер Инфраструктура или Кибер Хранилище	+	+	+[2]	+	+	+	+[3]	+	+	+

[2] Только для ОС Linux.

[3] Только для резервных копий формата ”Версия 11”. Подробнее о форматах резервных копий см. раздел *Формат резервной копии*.

[1] Репликация резервных копий из хранилища, управляемого узлом хранения, возможна только в локальную папку на той же машине, где находится узел хранения.

Примечание

Хранилище под управлением узла хранения с включённой дедупликацией не рекомендуется использовать для постоянной репликации. Дедупликация является длительным и ресурсоёмким процессом, который может привести к снижению скорости репликации, если в качестве источника реплицируемых данных используется хранилище под управлением узла хранения с дедупликацией.

Дополнительные условия использования хранилища под управлением узла хранения см. в разделе *Замечания по использованию узла хранения*.

Включение репликации резервных копий

Для включения репликации резервных копий выполните следующие действия:

1. На панели плана резервного копирования щёлкните **Добавить хранилище**.

   Элемент управления **Добавить хранилище** отображается только в том случае, если поддерживается репликация *из* последнего выбранного хранилища.

2. Укажите хранилище, в которое будет проведена репликация резервных копий.
3. [Необязательно] В поле **Срок хранения** измените правила хранения для указанного хранилища, как описано в разделе *Правила хранения*.
4. [Необязательно] В поле **Преобразовать в VM** укажите настройки преобразования в виртуальную машину, как описано в разделе *Преобразование в виртуальную машину*.
5. [Необязательно] Щёлкните значок шестерни > **Производительность и окно резервного копирования**, затем задайте окно резервного копирования для выбранного расположения, как описано в разделе *Производительность и окно резервного копирования*. Эти настройки определят производительность репликации.
6. [Необязательно] Повторите шаги 1–5 для всех хранилищ, где необходимо реплицировать резервные копии. Можно использовать до пяти последовательных хранилищ (включая основное).

Замечания по использованию узла хранения

Репликация резервных копий между управляемыми хранилищами

Репликация резервной копии из одного управляемого хранилища в другое выполняется узлом хранения.

Ограничения

- Репликация резервных копий *из* ленточного устройства, подключенного к узлу хранения, не поддерживается.
- Репликация резервных копий *из* хранилища, управляемого узлом хранения, в Зону безопасности не поддерживается.
- Репликация резервных копий *в* управляемое хранилище с включенной дедупликацией не поддерживается для резервных копий, имеющих *формат резервной копии* **Версии 12**.

  > **Примечание**
  >
  > Не рекомендуется использовать для постоянной репликации. Дедупликация является длительным и ресурсоёмким процессом, который может привести к снижению скорости репликации, если в качестве источника реплицируемых данных используется хранилище под управлением узла хранения с дедупликацией.

- Репликация резервных копий из хранилища, управляемого узлом хранения, возможна только в локальную папку на той же машине, где находится узел хранения.

Место выполнения операции

Репликация резервной копии *из* любого хранилища инициируется агентом, создавшим резервную копию, и выполняется:

- этим агентом, если хранилище *не* управляется узлом хранения;
- соответствующим узлом хранения, если хранилище является управляемым.

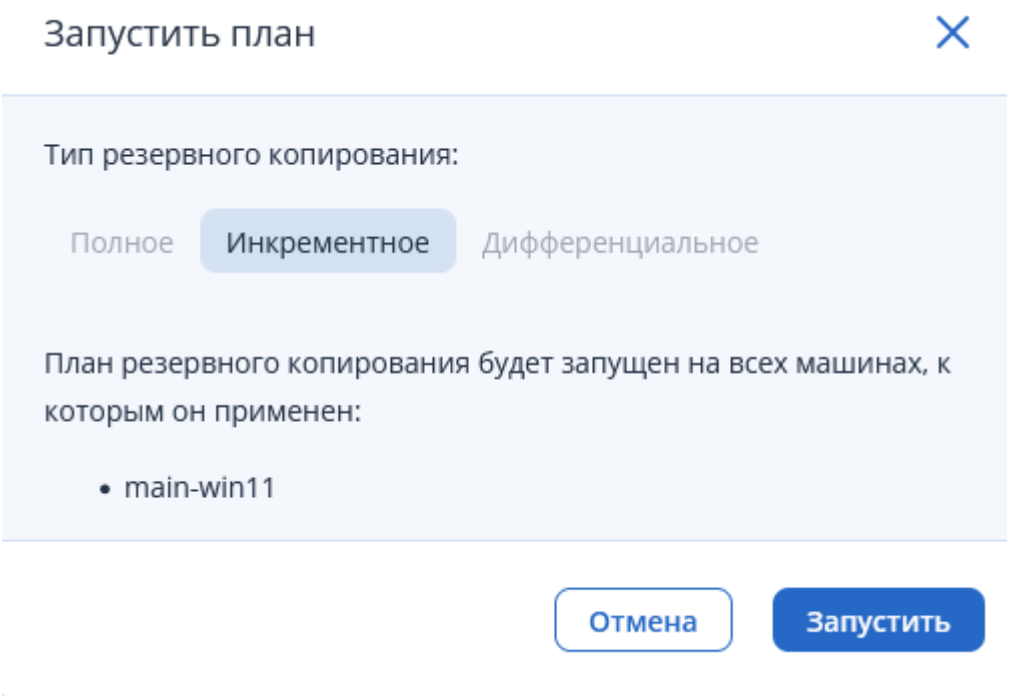
Как следует из вышеуказанного, операция будет выполнена только в том случае, если машина с агентом включена.

Запуск резервного копирования вручную

Можно не дожидаться запуска резервного копирования по расписанию и запустить его немедленно. Немедленный запуск резервного копирования можно осуществить несколькими способами.

Запуск резервного копирования из меню действий с планом

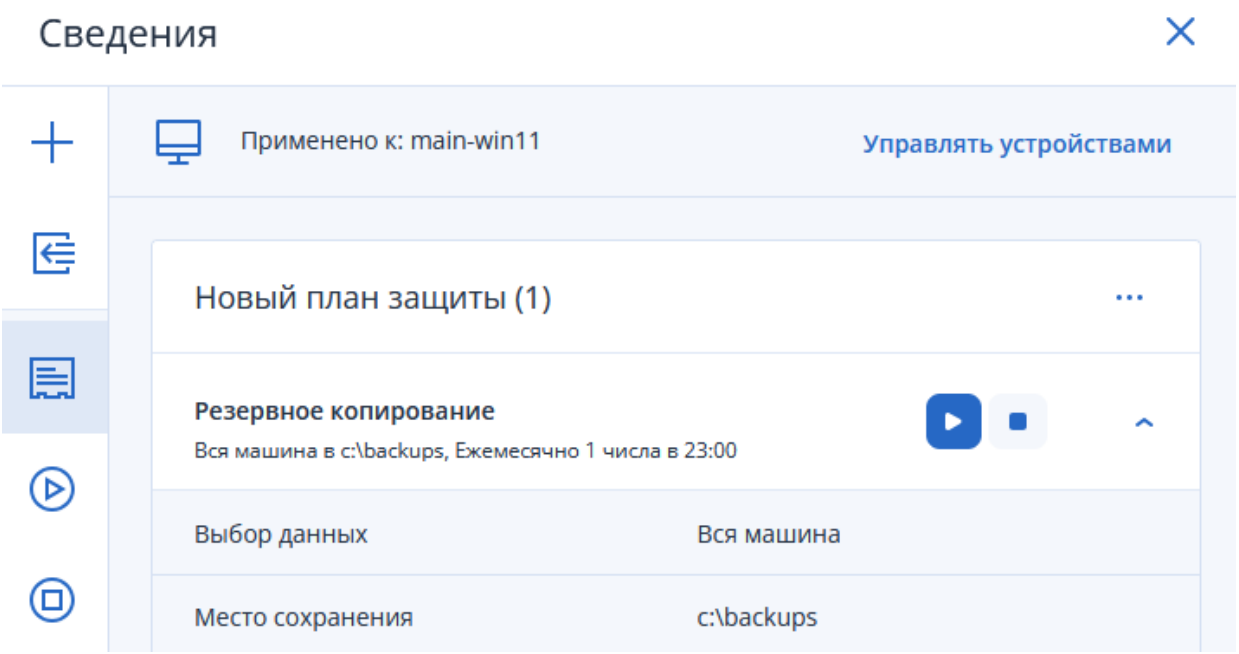
1. Во вкладке **Планы** → **Защита** отметьте план в списке.
2. Щёлкните **Запуск резервного копирования** в меню действий с планом.
3. Выберите тип резервного копирования (доступно, если в плане предусматривается резервное копирование с сочетанием разных его типов).



4. Нажмите кнопку **Запустить**. Дождитесь окончания резервного копирования.

Запуск резервного копирования из вкладки ”Сведения”

1. Отметьте план в списке и в меню действий с планом перейдите на вкладку **Сведения**.

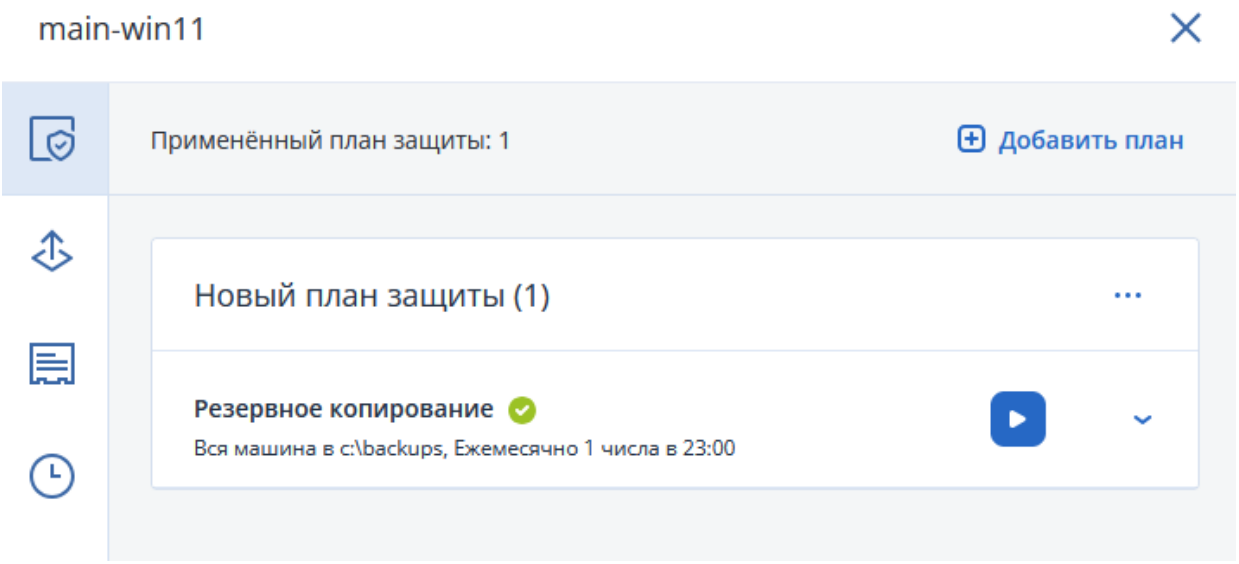


2. Нажмите кнопку с символом воспроизведения.
3. Выберите тип резервного копирования (доступно, если в плане предусматривается резервное копирование с сочетанием разных его типов).
4. Нажмите кнопку **Запустить**. Дождитесь окончания резервного копирования.

Запуск резервного копирования из меню ”Устройства”

1. Перейдите в меню **Устройства**.
2. Отметьте в списке одну машину или несколько машин и нажмите в меню справа **Защитить**.
3. Выберите нужный план и нажмите кнопку с символом воспроизведения.

> **Примечание**
>
> При выборе нескольких машин в списке будут отображены только те планы, которые являются общими для всех выбранных машин.



Если к машине применено несколько планов, нажмите кнопку запуска у каждого из тех, которые необходимо выполнить сейчас.

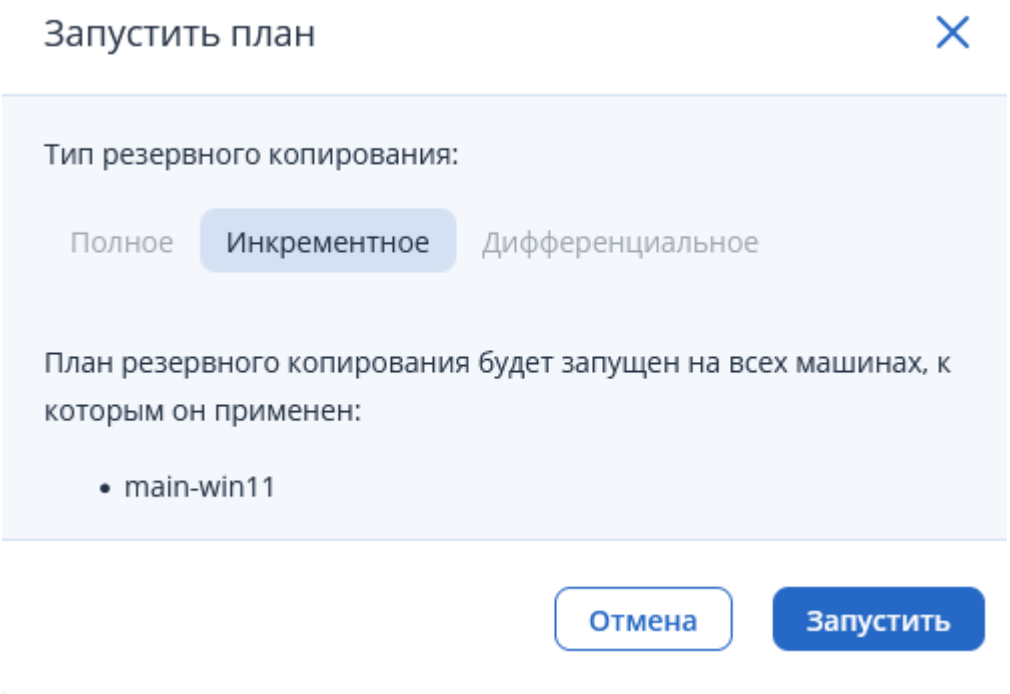
Примечание

Одновременный запуск большого количества планов может приводить к снижению производительности резервного копирования. Во избежание этого запускайте планы небольшими группами.

Важно

Запуск по требованию нескольких планов одновременно требует включения одновременного резервного копирования. Для включения одновременного файлового и дискового резервного копирования необходимо настроить конфигурационный файл (см. *Одновременное резервное копирование*).

4. Выберите тип резервного копирования (доступно, если в плане предусматривается резервное копирование с сочетанием разных его типов).



5. Нажмите кнопку **Запустить**. Дождитесь окончания резервного копирования.

Первая резервная копия, созданная планом защиты, всегда является полной.

Прогресс выполнения резервного копирования отображается в столбце **Действия** для выбранной машины или на вкладке **Панель мониторинга** → **Действия** основного меню.

Пока выполняется план, кнопка запуска будет неактивна. Остановка выполняющегося в данный момент резервного копирования в рамках плана описана в разделе *Операции с планами защиты*.

Одновременное резервное копирование

Одновременное резервное копирование одним агентом позволяет нескольким планам защиты выполняться параллельно в том случае, когда они работают с одним и тем же типом данных. Одновременное резервное копирование является реализацией многозадачности агента в резервном копировании Кибер Бэкап (см. *Агент*). Это способно значительно ускорить выполнение операций.

В Кибер Бэкап одновременное резервное копирование доступно для следующих элементов:

- локальные диски, файлы и папки;
- сетевые файлы и папки;
- виртуальные машины;
- почтовые ящики Microsoft Exchange;
- экземпляры баз данных PostgreSQL.

В Кибер Бэкап, начиная с версии 17.3, доступно одновременное файловое (см. *Выбор файлов и папок*) и дисковое (см. *Выбор дисков и томов*) резервное копирование, выполняемое одним агентом.

По умолчанию эта функция отключена.

Условия для выполнения одновременного резервного копирования

В таблице ниже представлены условия одновременного резервного копирования данных различных элементов в зависимости от их типа.

Элементы для резервного копирования	**Особенности**	**Количество планов защиты**	**Возможность одновременного резервного копирования**	**Необходимость включения одновременного резервного копирования**
Почтовые ящики	Разные почтовые ящики	Один или несколько	Да	Нет
Экземпляры баз данных PostgreSQL	Разные экземпляры	Один или несколько	Да	Нет
Виртуальные машины	Разные ВМ	Один или несколько	Да	Нет
	Разные диски одной ВМ	Несколько	Нет	Нет
Локальные диски	Разные диски одной машины	Несколько	Да	Да
	Один диск одной машины	Да		
Локальные файлы и папки	Разные диски одной машины	Несколько	Да	Да
	Один диск одной машины	Да		
Сетевые файлы и папки (SMB/CIFS и NFS)	Разные файлы одного ресурса	Несколько	Да	Да

Для того, чтобы иметь возможность выполнять одновременное файловое и дисковое резервное копирование, необходимо включить его, выполнив настройку конфигурационного файла Кибер Бэкап.

Включение одновременного резервного копирования

Конфигурационный файл по умолчанию расположен на машине с агентом по адресу: `C:\Program Files\Acronis\BackupAndRecovery\settings.config` (для Windows) и `/usr/lib/Acronis/BackupAndRecovery/settings.config` (для Linux). Добавьте в него значение `simultaneous_backups` как показано далее:

```
<mms>

  <default>

      <backup>
        <simultaneous_backups>10</simultaneous_backups>
...
```

Число в конфигурационном файле (в этом примере 10) — это параметр, задающий максимальное количество одновременно выполняемых планов. По умолчанию параметр `simultaneous_backups` не внесен в конфигурационный файл, что соответствует его значению, равному 1. Установка ограничения на число одновременно выполняемых планов для различных типов данных описана далее в соответствующих разделах.

Важно

- После внесения изменений в конфигурацию агента его необходимо перезапустить.
- При обновлении агента пользовательское значение параметра `simultaneous_backups` не сохраняется. После обновления его нужно задать повторно.

Запуск одновременного резервного копирования

Включение одновременного резервного копирования позволяет планам с файловым и дисковым резервным копированием выполняться одновременно.

Вы также можете запустить одновременное резервное копирование вручную. Запуск вручную выполняется в веб-консоли (см. *Запуск резервного копирования вручную*).

Перед запуском создайте необходимые планы (см. *Создание плана защиты*) с дисковым или файловым резервным копированием или убедитесь, что такие планы уже созданы (см. *Вкладка "Планы"*).

Ограничение общего количества планов для файлового и дискового резервного копирования

Конфигурационный файл по умолчанию расположен по адресу: `C:\Program Files\Acronis\BackupAndRecovery\settings.config` (для Windows) и `/usr/lib/Acronis/BackupAndRecovery/settings.config` (для Linux). Укажите в нем необходимое значение параметра `simultaneous_backups`, задающего максимальное количество одновременно выполняемых планов:

```
<mms>

  <default>

      <backup>
        <simultaneous_backups>10</simultaneous_backups>

.....
```

В этом примере число указано равным 10. Если это число указано достаточно большим и ресурсов агента для одновременного резервного копирования не хватает, количество одновременно выполняемых планов будет автоматически скорректировано агентом.

Важно

- После внесения изменений в конфигурацию агента его необходимо перезапустить.
- При обновлении агента пользовательское значение параметра `simultaneous_backups` не сохраняется. После обновления его нужно задать повторно.

Ограничение общего количества виртуальных машин

Параметр резервного копирования *Планирование* определяет количество виртуальных машин, для которых агент может одновременно создавать резервные копии при выполнении данного плана защиты.

Если несколько планов защиты пересекаются по времени, указанные в их параметрах числа суммируются. Хотя суммарное количество программным образом ограничено до 10, пересечение планов может влиять на производительность резервного копирования, а также оказывать избыточную нагрузку на хранилище хоста и виртуальной машины.

Вы можете дополнительно ограничить общее количество виртуальных машин, для которых агенты для систем управления виртуализацией (например, VMware или Hyper-V) могут одновременно создавать

резервные копии.

Примечание

Одновременное резервное копирование виртуальных машин для VMware/Hyper-V работает в том числе при размещении агента на физическом сервере.

Установка ограничения на общее количество виртуальных машин, для которых может создавать резервные копии агент для VMware (Windows) или агент для Hyper-V

1. На машине, на которой запущен агент, создайте новый текстовый документ и откройте его в текстовом редакторе, например в Блокноте.
2. Скопируйте и вставьте в этот файл следующие строки:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\
↪SimultaneousBackupsLimits]
”MaxNumberOfSimultaneousBackups”=dword:00000001
```

3. Вместо `00000001` укажите нужное ограничение в шестнадцатеричном формате. Например `00000001` означает 1, а `0000000A` — 10.
4. Сохраните документ под именем `limit.reg`.
5. Запустите файл от имени администратора.
6. Подтвердите изменение реестра Windows.
7. Выполните указанные ниже действия, чтобы перезапустить агент.
    1. В меню **Пуск** выберите команду **Выполнить** и введите: `cmd`.
    2. Нажмите кнопку **ОК**.
    3. Выполните следующие команды:

```
net stop mms
net start mms
```

Установка ограничения на общее количество виртуальных машин, для которых может создавать резервные копии агент для VMware (виртуальное устройство) или агент для среды виртуализации (Linux)

Эта процедура применяется в отношении следующих агентов, предоставляемых в виде виртуального устройства:

- агент для VMware;
- агент для системы управления виртуализацией, используемый совместно с агентом для Linux.

Для установки ограничения выполните следующие действия.

1. На машине, на которой запущен агент, откройте консоль управления.
   - **Агент для VMware (виртуальное устройство)**: в пользовательском интерфейсе виртуального устройства нажмите клавиши `Ctrl` + `Shift` + `F2`.
   - **Агент для среды виртуализации (Linux)**: войдите с учетными данными пользователя `root` на машину, на которой запущено устройство Кибер Бэкап. Пароль совпадает с паролем для веб-консоли Кибер Бэкап.
2. Откройте файл `/etc/Acronis/MMS.config` в текстовом редакторе, например в **vi**.
3. Найдите следующий раздел:

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. Вместо `10` укажите нужное ограничение в десятичном формате.
5. Сохраните файл.
6. Перезапустите агент.
   - **Агент для VMware (виртуальное устройство)**: выполните команду `reboot`.
   - **Агент для среды виртуализации (Linux)**: выполните указанные ниже команды.

     ```
     sudo service acronis_mms restart
     ```

Ограничение общего количества планов для почтовых ящиков и баз данных PostgreSQL

Конфигурационный файл по умолчанию расположен по адресу: `/opt/acronis/etc/generic-backup-agent/generic-backup-agent.json`. В параметре `maxTasks` укажите максимальное количество одновременно выполняемых планов (по умолчанию 5):

```
”maxTasks”: 5
```

Важно

После внесения изменений в конфигурацию агента его необходимо перезапустить.

Резервное копирование виртуальных машин без использования локальной сети (LAN-free backup)

Резервное копирование без использования локальной сети — это метод передачи данных, при котором агент резервного копирования получает прямой доступ к хранилищу данных через сеть хранения (SAN), минуя общую локальную сеть (LAN) организации.

Ключевые преимущества метода:

- **Разгрузка сети**. Трафик резервного копирования не замедляет работу бизнес-приложений и пользователей в локальной сети.
- **Повышение производительности**. Прямое чтение данных из системы хранения данных (через iSCSI или Fibre Channel) значительно сокращает время создания резервных копий.
- **Минимальное влияние на среду**. Нагрузка на вычислительные узлы (хосты) виртуализации и гипервизор сводится к минимуму, данные передаются напрямую на виртуальное устройство защиты.
- **Повышение безопасности**. Изоляция трафика резервного копирования в SAN снижает риск перехвата данных по сравнению с передачей через общую сеть.

Этот метод наиболее эффективен для организаций, которые работают с большими объемами данных и имеют строгие требования к *окну резервного копирования*.

Резервное копирование без использования локальной сети (LAN-free backup) для oVirt

Резервное копирование без использования локальной сети в системах oVirt/zVirt поддерживается в следующих продуктах:

- Кибер Бэкап версии 17.3 и выше;
- oVirt версии 4.2 и выше;
- zVirt версии 4.2 и выше.

Схема резервного копирования без использования локальной сети



На этой схеме:

- **Виртуальное устройство** — виртуальное устройство для взаимодействия с Кибер Бэкап и oVirt/zVirt;

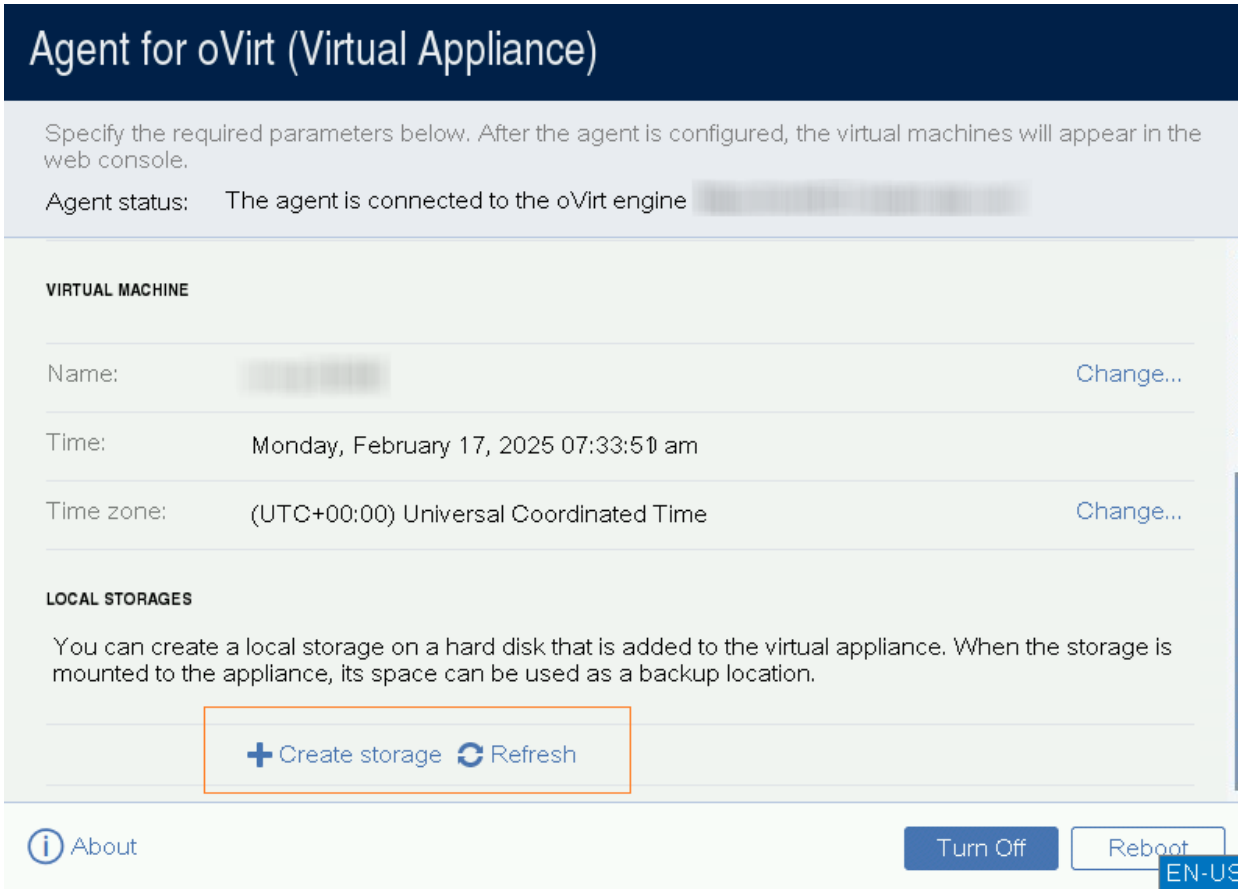
- **ВМ** — целевая виртуальная машина для выполнения резервной копии, расположена на системе виртуализации oVirt/zVirt;
- **Node** — вычислительный узел (хост) системы виртуализации oVirt/zVirt;
- **——** — отображает подключение сети управления;
- **<——->** — отображает направление трафика;
- **iSCSI,FC** — устройство хранения резервных копий;
- **Подключение диска к виртуальному устройству** — подключение диска к виртуальному устройству через настроенную сеть хранения данных на системе виртуализации (диск RDM (прямой LUN), диск, представленный через iSCSI или из локального хранилища).

Настройка и подключение диска к виртуальному устройству

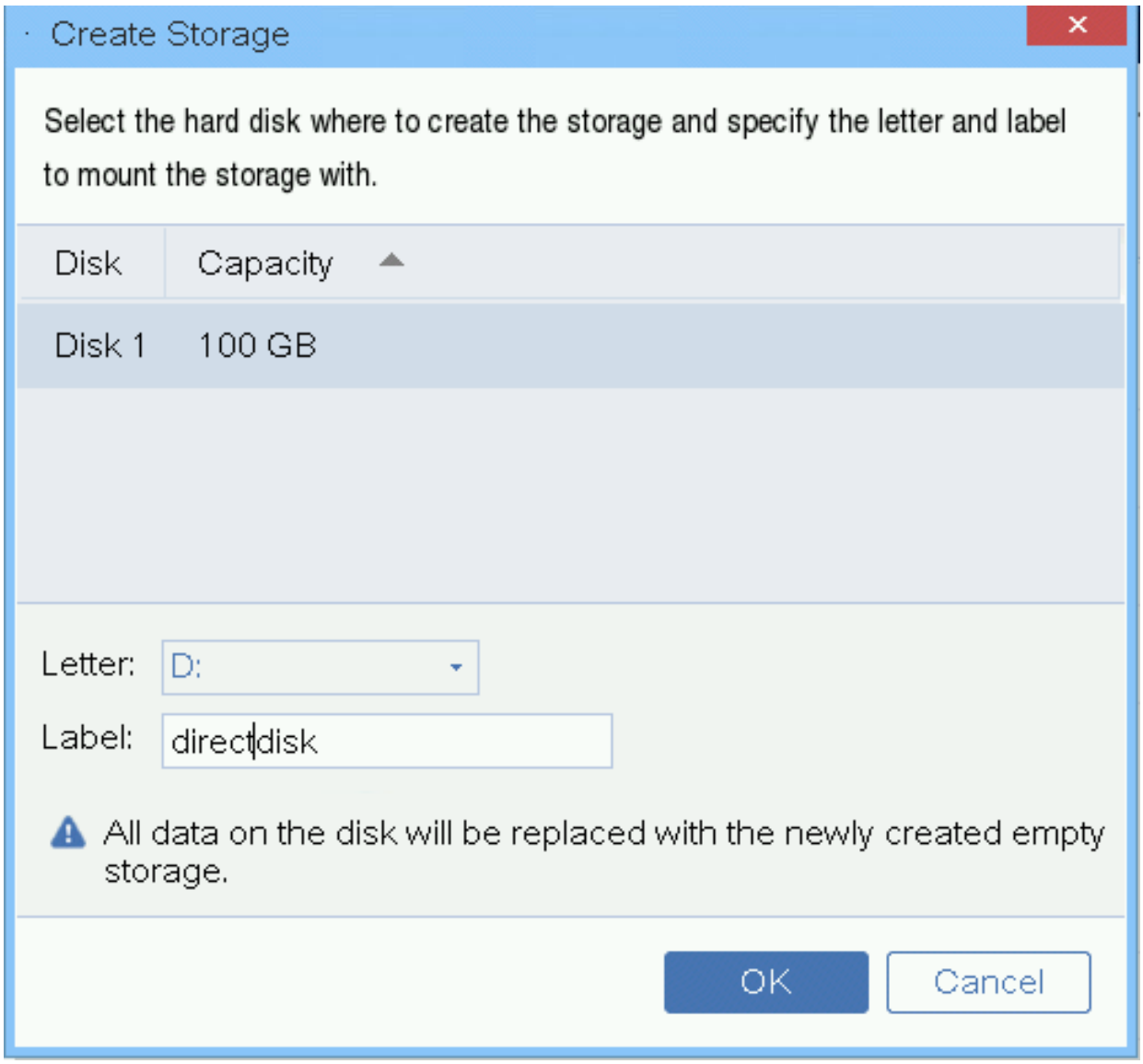
1. Установите виртуальное устройство (virtual appliance) для системы виртуализации oVirt/zVirt.
2. Убедитесь, что виртуальное устройство успешно подключено к системе виртуализации и серверу управления (CMS).
3. Добавьте новый диск к виртуальному устройству с помощью графического интерфейса oVirt/zVirt. Этот диск может быть представлен как диск iSCSI или FC. Размер диска должен составлять не менее 10 ГБ.

> **Важно**
>
> Для виртуального устройства (virtual appliance) любой подключенный к нему диск представляется как Local Storages. Этот термин следует отличать от локального хранилища zVirt, которое не рекомендовано к использованию в продуктовой среде.

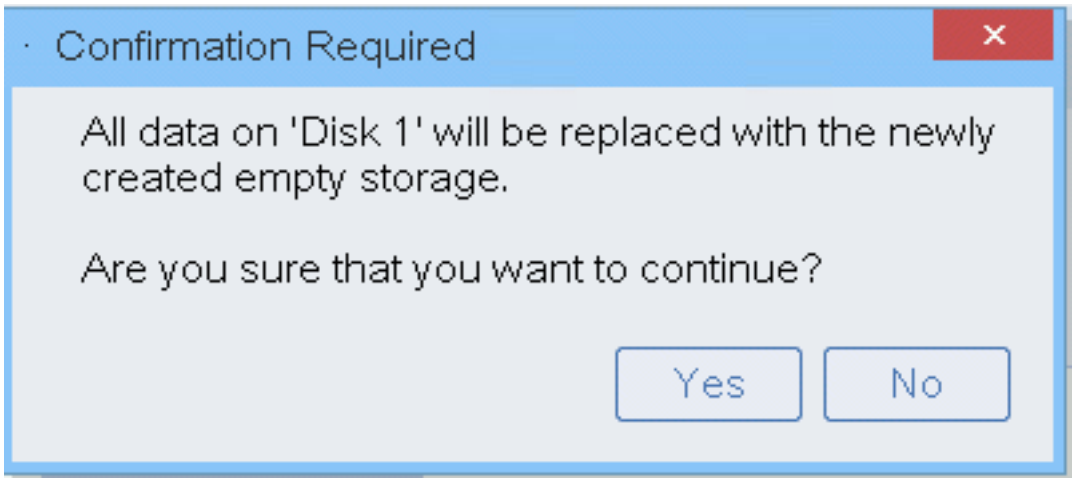
4. Перейдите в консоль виртуального устройства.
5. В веб-интерфейсе виртуального устройства в меню **Local Storages** нажмите на ссылку **Refresh**.



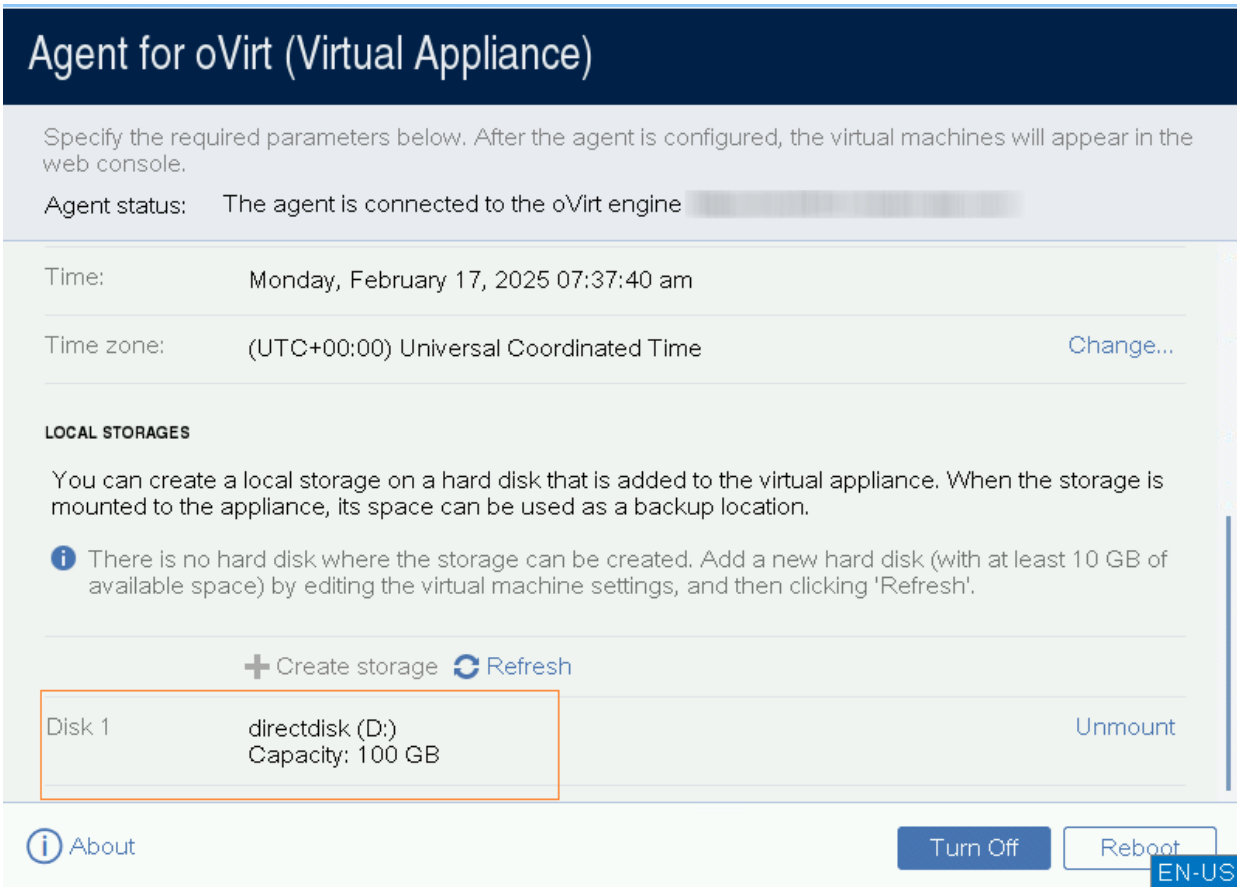
6. Ссылка **Create Storage** станет активной, нажмите на эту ссылку. Выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.



7. Подтвердите добавление диска.



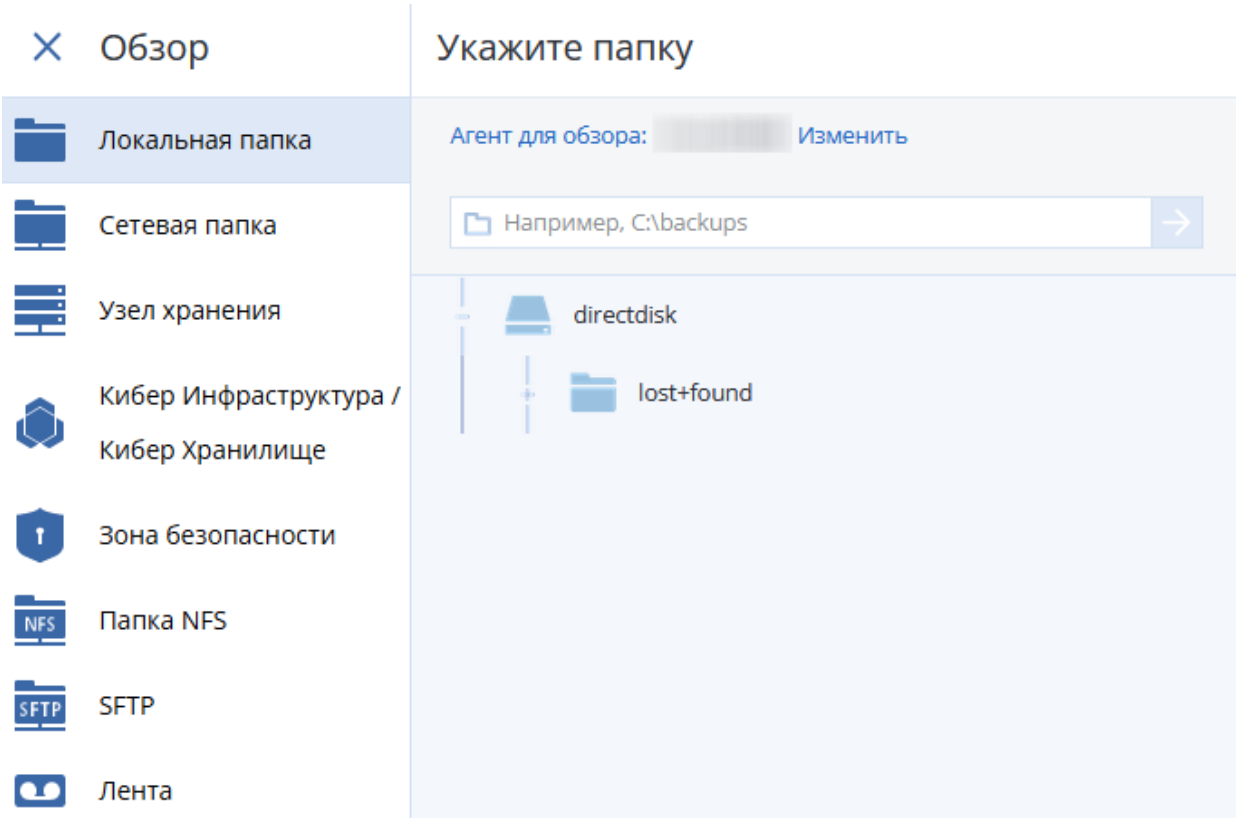
8. В интерфейсе виртуального устройства убедитесь, что диск был успешно добавлен к виртуальному устройству.



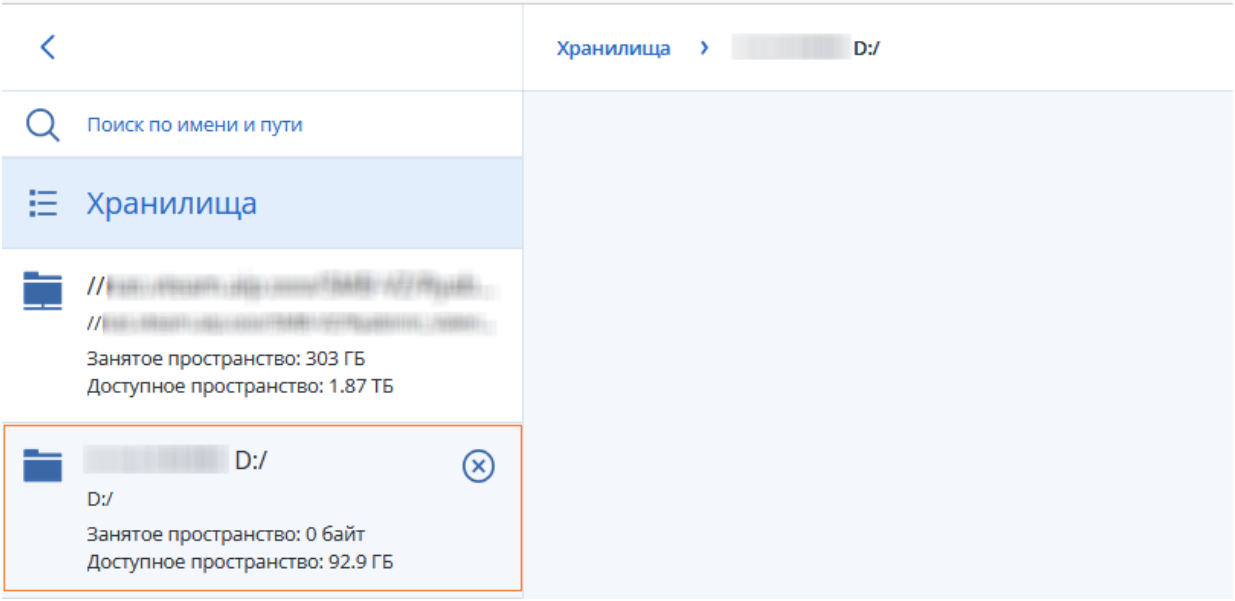
Подключение локального диска виртуального устройства в Кибер Бэкап

Для подключения выполните следующие действия:

1. Убедитесь, что виртуальное устройство (virtual appliance) установлено и подключено к oVirt/Zvirt.
2. В веб-консоли (Кибер Бэкап) перейдите в меню **Хранилище резервных копий** и на вкладке **Действия** выберите ссылку **Добавить хранилище**.
3. На вкладке **Обзор** рядом с **Агент для обзора** щёлкните **Изменить**, выберите нужное виртуальное устройство и нажмите **ОК**. Далее выберите **Локальная папка** и после отображения дерева подключенных дисков выберите необходимый диск на виртуальном устройстве.



4. После успешного добавления в разделе **Хранилище резервных копий** отобразится новое хранилище для резервных копий.



Новое хранилище можно добавить в планы резервного копирования и далее при использовании этого хранилища резервное копирование будет происходить без использования локальной сети (LAN-free backup).

Примечание

Резервное копирование в это хранилище может выполняться только тем виртуальным устройством (агентом), к которому подключен RDM-диск. Для других виртуальных устройств (агентов) хранилище недоступно.

Резервное копирование без использования локальной сети (LAN-free backup) для VMware

Резервное копирование виртуальных машин без использования локальной сети можно организовать с помощью *виртуального устройства для VMware* или *Windows-агента для VMware*. Подробные сведения см. в соответствующих подразделах.

Резервное копирование без использования локальной сети посредством виртуального устройства для VMware

Схема резервного копирования без использования локальной сети



На этой схеме:

- **ВМ CMS** — виртуальная машина с установленным сервером управления Кибер Бэкап (CMS);
- **Виртуальное устройство** — виртуальное устройство для взаимодействия с Кибер Бэкап и vCenter/ESXi;

- **ВМ** — целевая виртуальная машина для создания резервной копии, расположена в системе виртуализации VMware;
- **Узел** — ESXi-сервер;
- **——** — отображает подключение сети управления;
- **<——->** — отображает направление трафика;
- **iSCSI, FC** — устройство хранения резервных копий;
- **Подключение диска к ВУ** — подключение диска к виртуальному устройству через настроенную сеть хранения данных в системе виртуализации (диск RDM).

При использовании этой схемы виртуальное устройство создает резервные копии виртуальных машин, получая данные из хранилищ данных VMware, которые размещены в СХД и подключены к ESX-серверу виртуального устройства через сеть хранения данных. Резервные копии размещаются на локальном диске виртуального устройства, который представляет собой отдельный LUN, доступный через сеть хранения данных и подключенный к виртуальному устройству как RDM-диск.

Предварительные требования

- Развернута и настроена сеть хранения данных (SAN) на основе iSCSI или Fibre Channel; к этой сети подключена система хранения данных (СХД).
- Серверы ESXi, помимо сети управления, также подключены к сети хранения данных.
- Хранилища данных VMware (datastores) для дисков виртуальных машин размещены в СХД.
- Для хранения резервных копий виртуальных машин в СХД выделена и экспортирована в виде LUN часть дискового пространства.

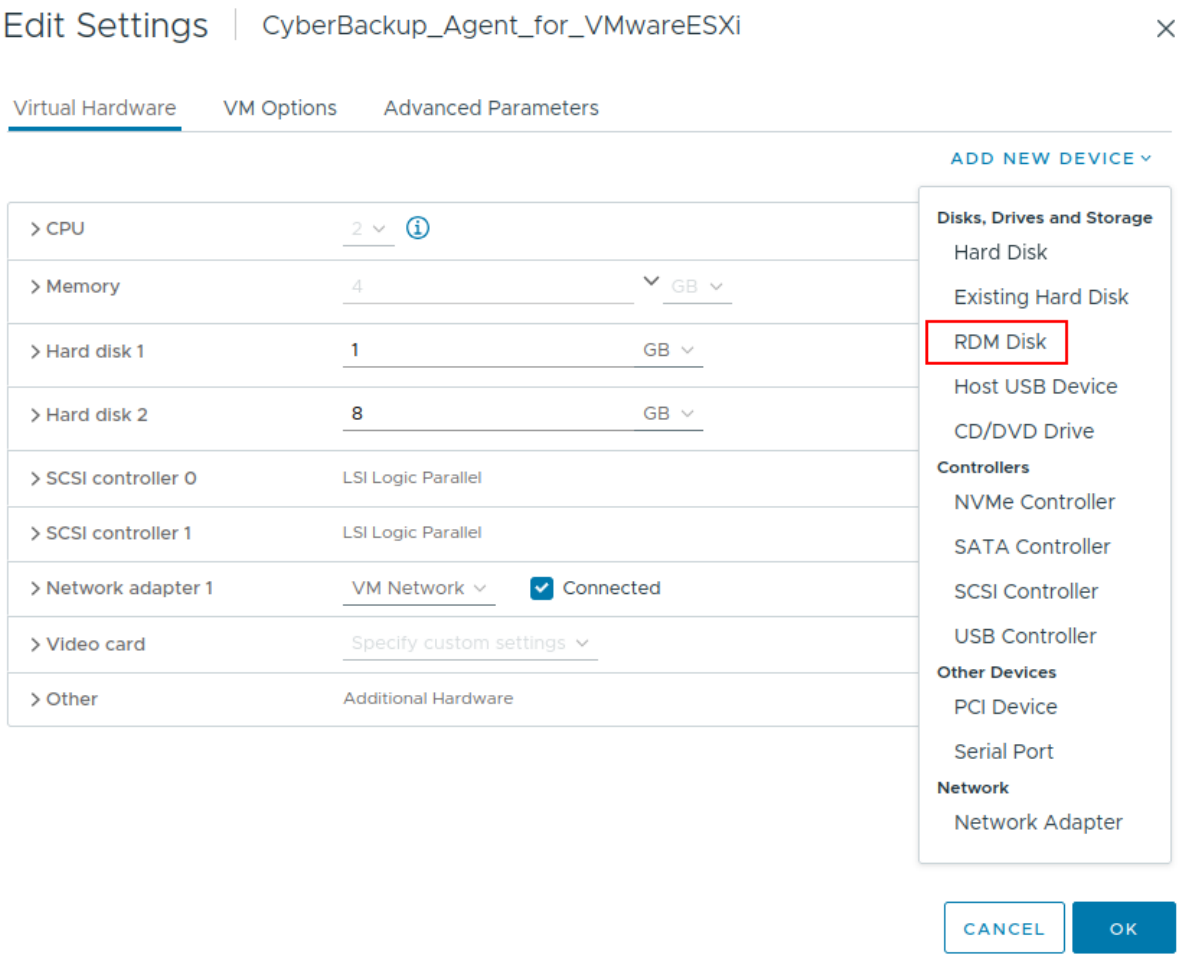
Настройка и подключение диска к виртуальному устройству

1. Создайте виртуальное устройство (virtual appliance) для системы виртуализации VMware.
2. Убедитесь, что виртуальное устройство успешно подключено к системе виртуализации и серверу управления (CMS).
3. Убедитесь, что ESX-сервер, на котором расположено виртуальное устройство, подключен к сети хранения данных.

> **Примечание**
>
> Для подключения к сети хранения данных на основе iSCSI на ESXi-сервере должен быть установлен программный iSCSI-адаптер, а для подключения к сети хранения данных на основе

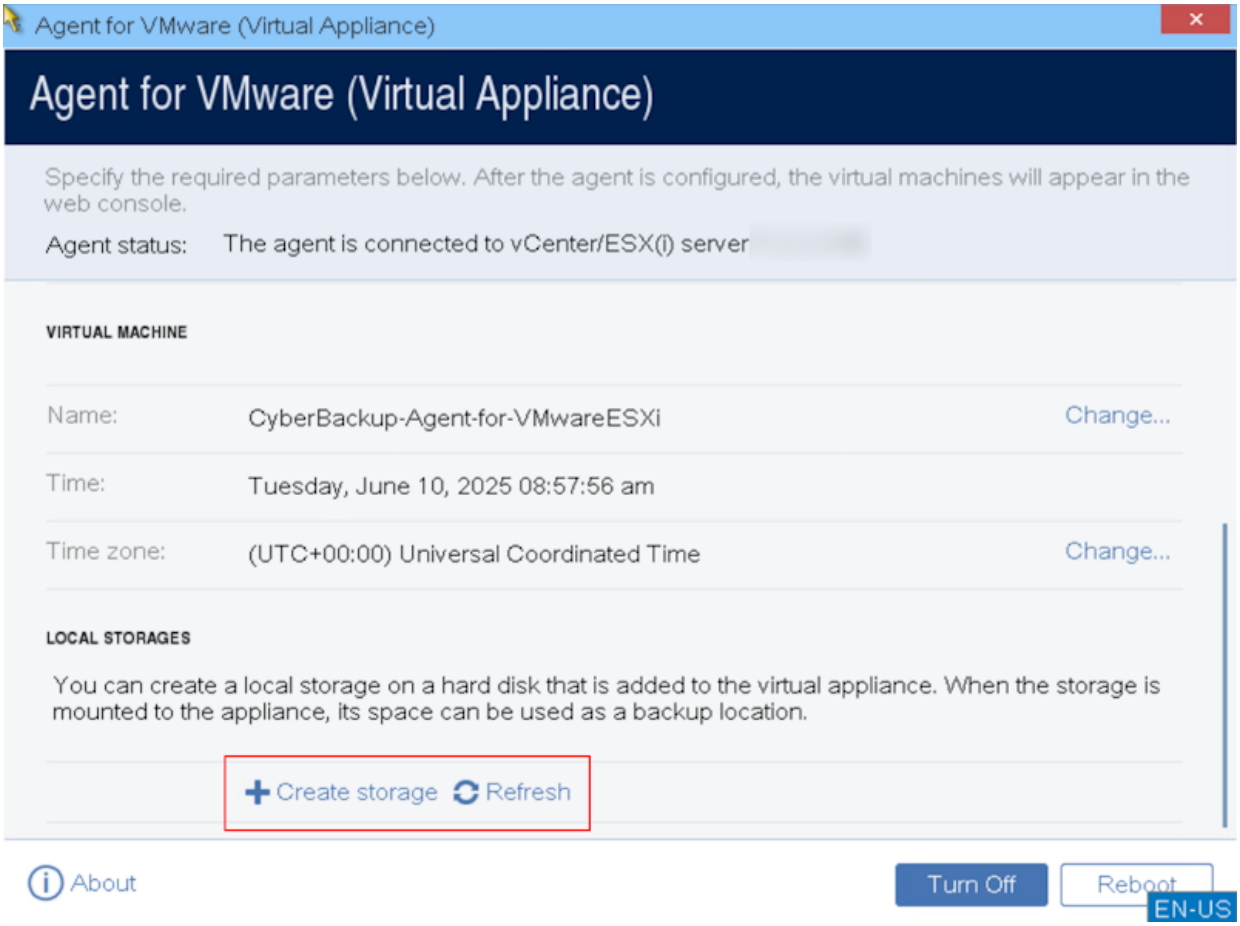
Fibre Channel — аппаратный HBA-адаптер.

4. Подключите LUN, предназначенный для хранения резервных копий, к виртуальному устройству как RDM-диск с помощью веб-интерфейса vCenter/ESXi.

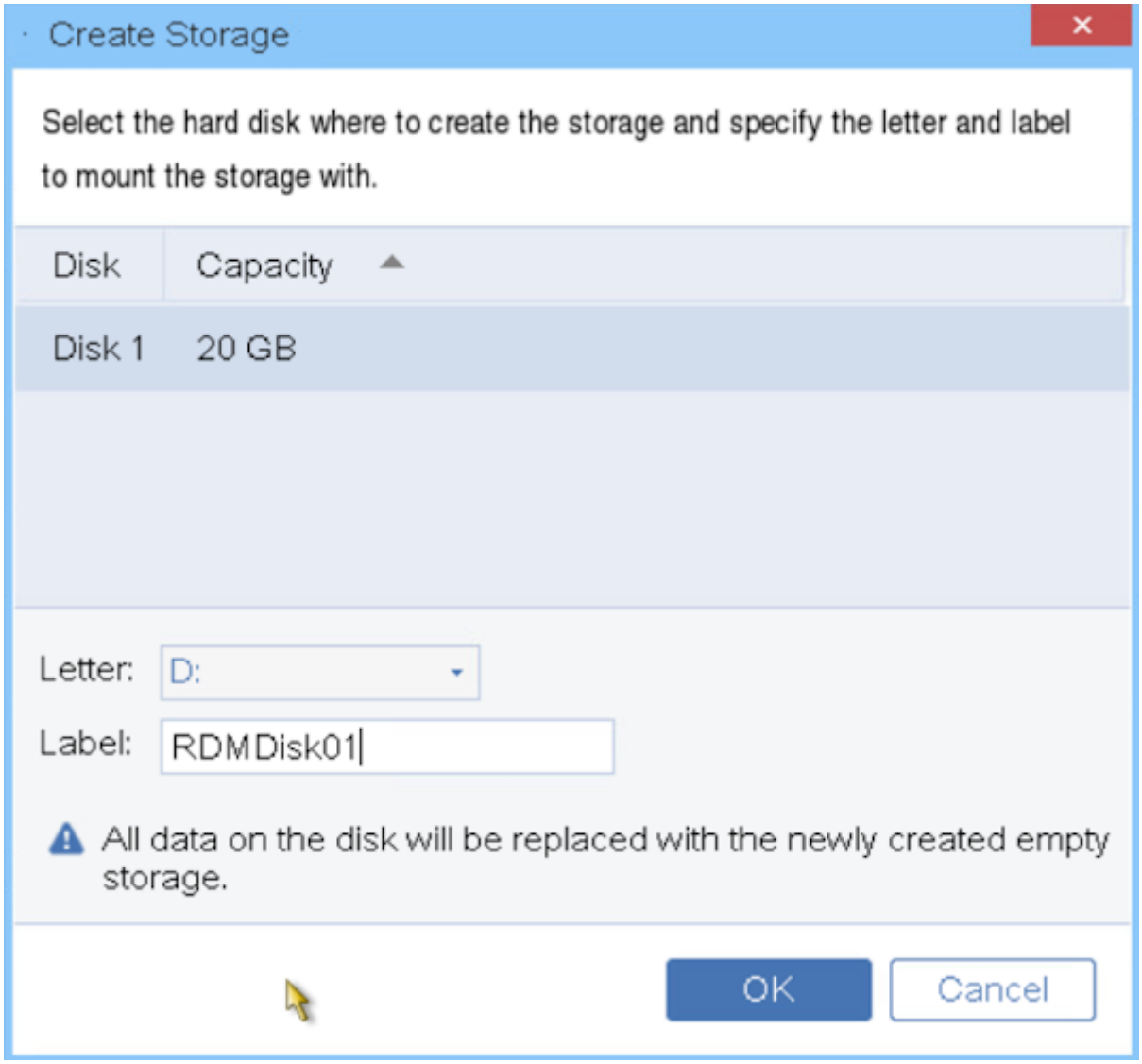


5. Перейдите в консоль виртуального устройства.

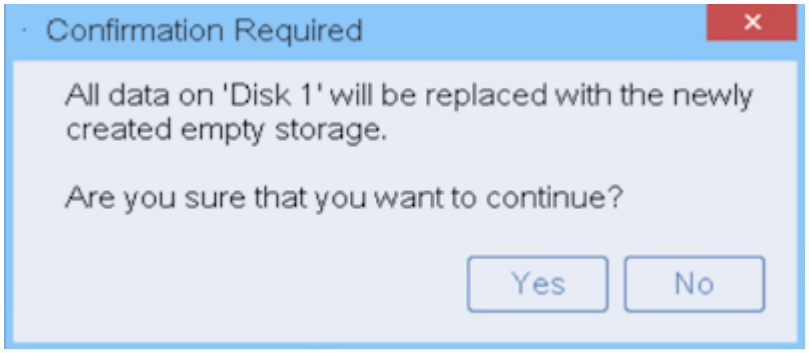
6. В интерфейсе виртуального устройства в разделе **Local Storages** нажмите **Refresh**.



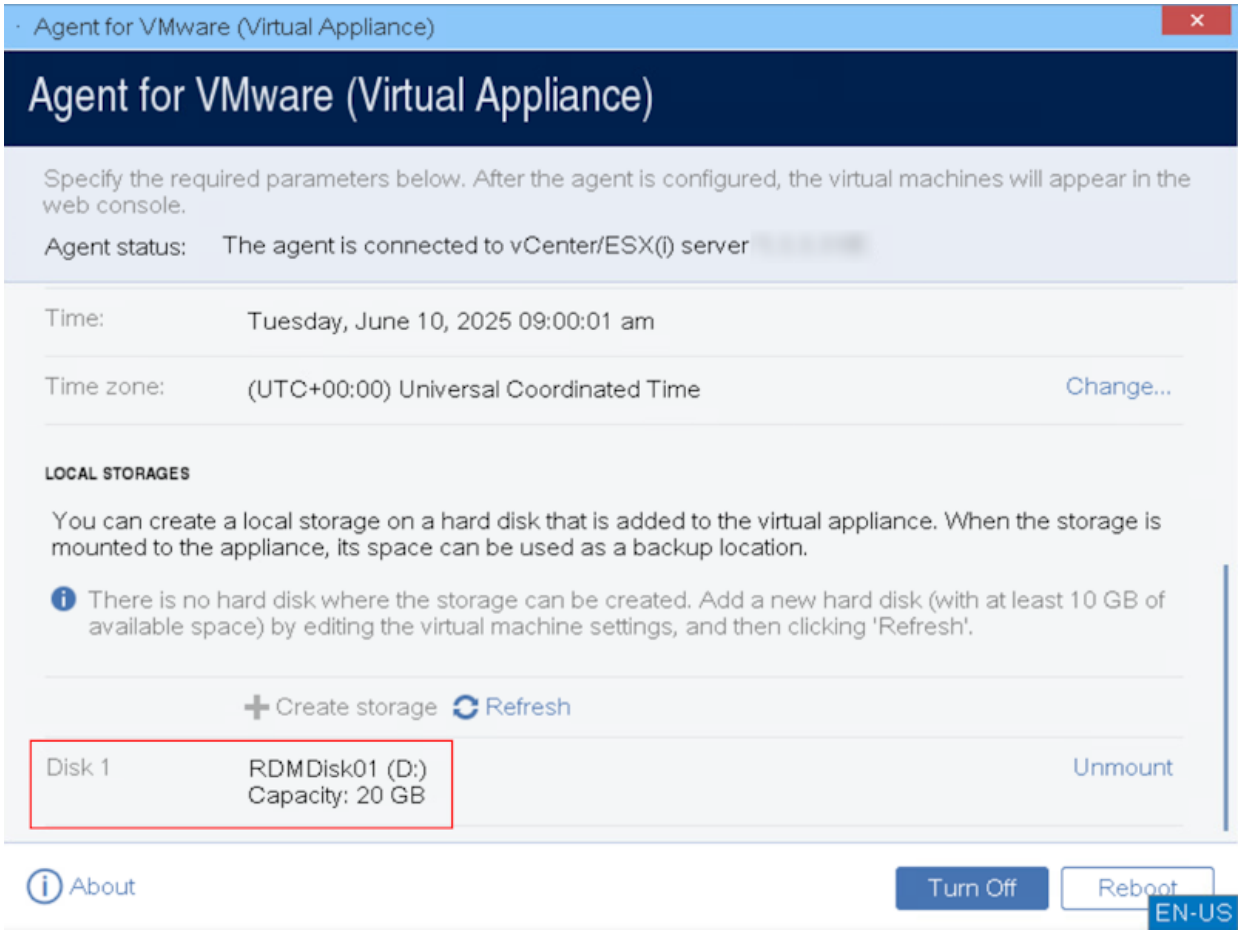
7. Когда ссылка **Create Storage** станет активной, нажмите на нее. Выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.



8. Подтвердите добавление диска.



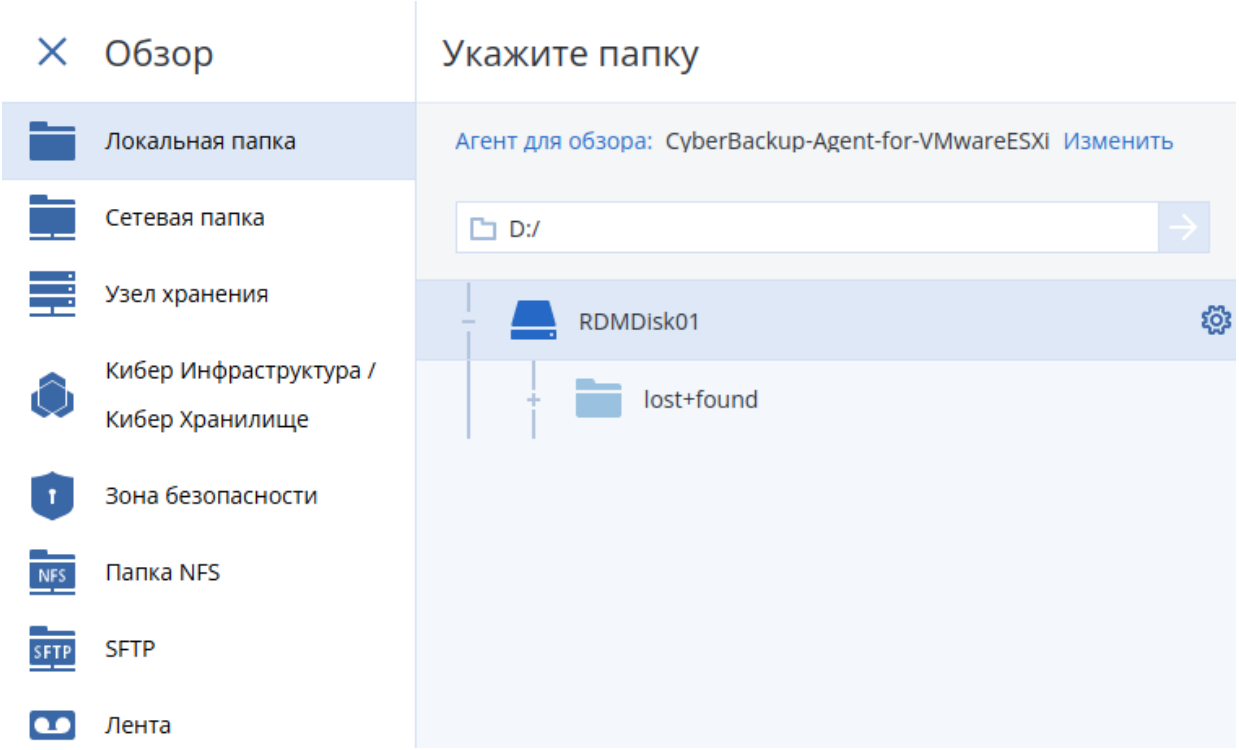
9. В интерфейсе виртуального устройства убедитесь, что диск был успешно добавлен к виртуальному устройству.



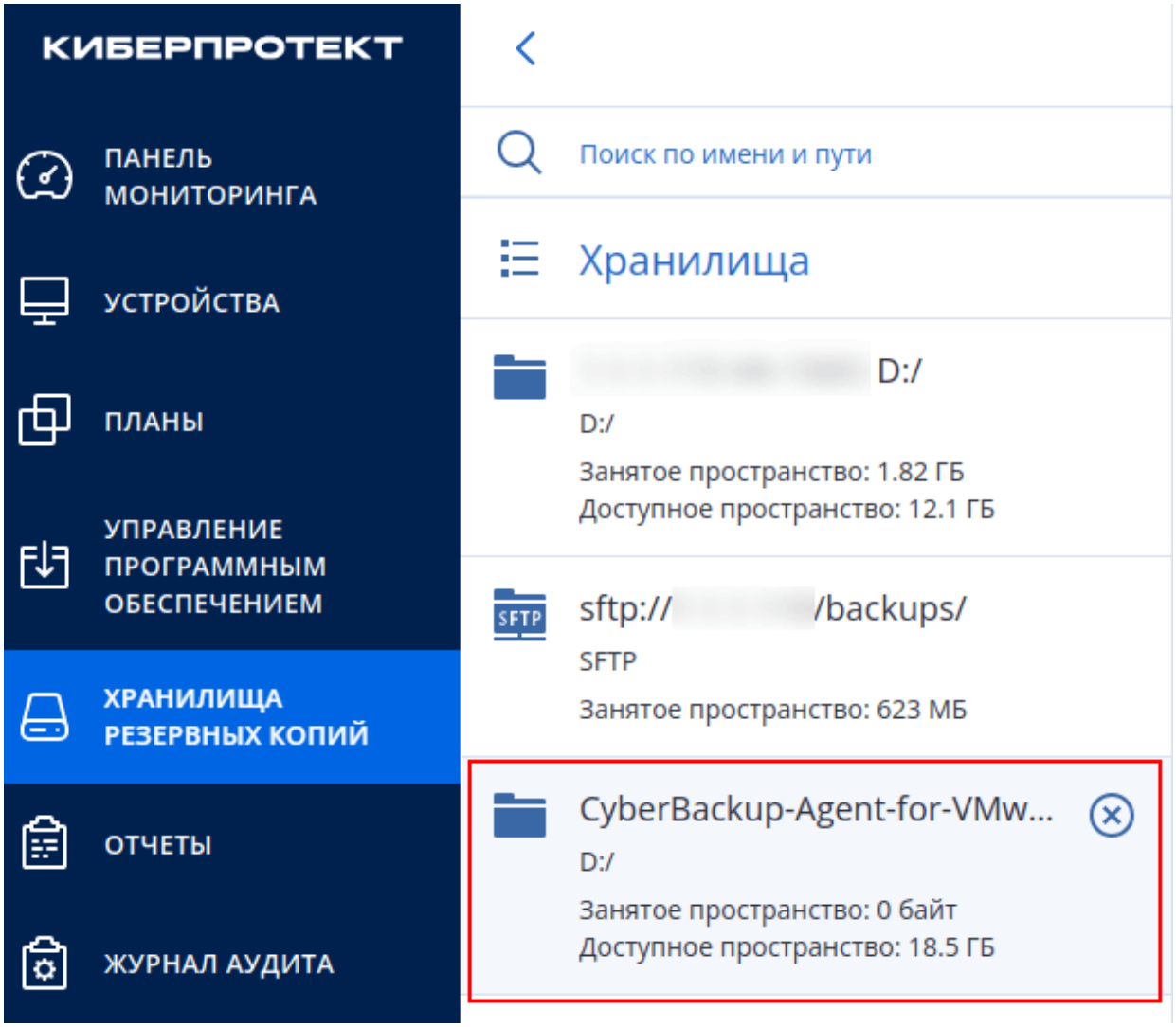
Подключение локального диска виртуального устройства в Кибер Бэкап

Для подключения выполните следующие действия:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Хранилища резервных копий** и на вкладке **Действия** щёлкните ссылку **Добавить хранилище**.
2. На вкладке **Обзор** рядом с **Агент для обзора** щёлкните **Изменить**, выберите нужное виртуальное устройство и нажмите **ОК**. Далее выберите **Локальная папка** и после отображения дерева подключенных дисков выберите необходимый диск виртуального устройства.



3. После успешного добавления в **Хранилища резервных копий** отобразится новое хранилище для резервных копий.



Добавленное хранилище можно будет использовать в плане резервного копирования виртуальных машин, при исполнении которого данные будут передаваться только через сеть хранения данных.

Примечание

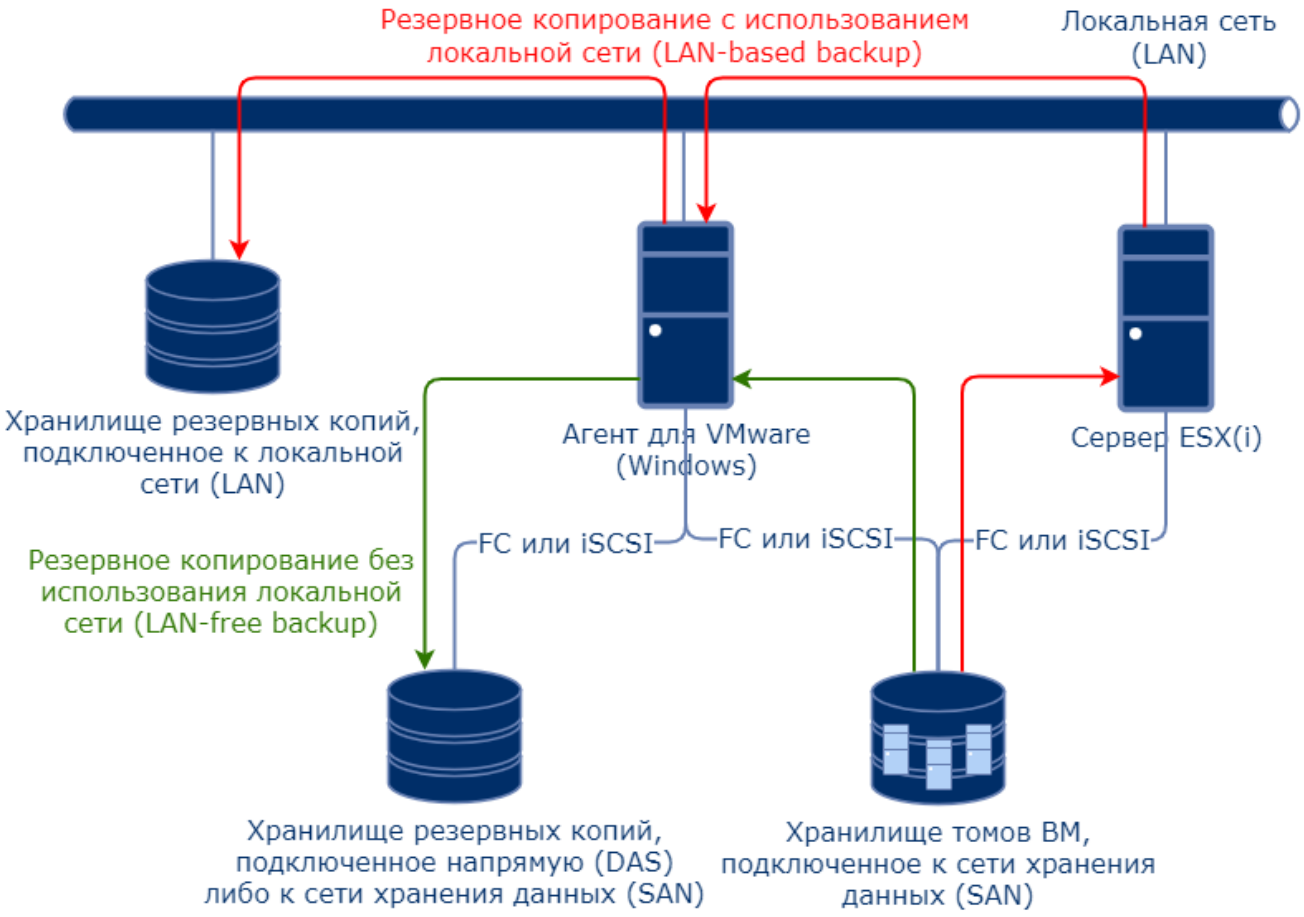
Резервное копирование в это хранилище может выполняться только тем виртуальным устройством (агентом), к которому подключен RDM-диск. Для других виртуальных устройств (агентов) хранилище недоступно.

Резервное копирование без использования локальной сети посредством Windows-агента для VMware

Если нагрузка на производственные хосты ESXi слишком велика и запуск виртуальных устройств нежелателен, можно установить агент для VMware (Windows) на физическую машину за пределами инфраструктуры ESXi.

Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Эта возможность называется резервным копированием без использования локальной сети.

На следующем рисунке показано резервное копирование с использованием и без использования локальной сети. Доступ к виртуальным машинам без использования локальной сети возможен при наличии оптоволоконного канала (FC) или сети хранения данных (SAN) iSCSI. Чтобы полностью исключить передачу резервных копий данных по локальной сети, храните резервные копии на локальном диске машины с установленным агентом или в присоединенном хранилище SAN.



Порядок включения прямого доступа к хранилищу данных для агента

1. Установите агент для VMware на машину Windows, на которой есть сетевой доступ к vCenter Server.
2. Подключите к машине логическое устройство, на котором расположено хранилище данных. Примите во внимание следующие соображения:
   - Используйте тот же протокол (iSCSI или FC), который использовался для подключения хранилища данных к ESXi.
   - Логическое устройство *не должно* инициализироваться. Вместо этого оно должно появиться

как ”автономный” диск в разделе **Управление дисками**. Если Windows инициализирует логическое устройство, оно может быть повреждено и стать нечитаемым для VMware vSphere.

Чтобы избежать инициализации логического устройства, для параметра **Политика SAN** автоматически устанавливается значение **Перевод в автономное состояние всех ресурсов** во время установки агента для VMware (Windows).

В результате агент будет использовать режим транспорта сети SAN для доступа к виртуальным дискам, т. е. он будет посекторно считывать секторы логического устройства по iSCSI/FC, не распознавая файловой системы VMFS (которая неизвестна для Windows).

Ограничения

- В vSphere агент не может использовать режим транспорта SAN, если одни диски ВМ расположены в VMware Virtual Volume (VVol), а другие — на других томах. Резервное копирование таких виртуальных машин приведет к сбою.
- Резервное копирование зашифрованных виртуальных машин (эта функциональная возможность представлена в VMware vSphere 6.5) будет выполняться по локальной сети, даже если настроен режим транспорта сети SAN для агента. Агент выполнит возврат из реплики, используя транспорт NBD, поскольку VMware не поддерживает транспорт сети SAN для резервного копирования зашифрованных виртуальных дисков.

Пример

Если используется сеть хранения данных (SAN) iSCSI, настройте инициатор iSCSI на машине с Windows, на которой установлен агент для VMware.

Настройка политики SAN

1. Войдите как администратор, откройте командную строку, введите `diskpart` и нажмите клавишу `Ввод`.
2. Введите `san` и нажмите клавишу `Ввод`. Убедитесь, что отображается **Политика SAN: Перевод в состояние ”вне сети” общих ресурсов**.
3. Если для политики SAN задано другое значение:
    1. Введите `san policy=offlineall`.
    2. Нажмите клавишу `Ввод`.
    3. Чтобы проверить правильность применения настройки, выполните шаг 2.
    4. Перезапустите машину.

Настройка инициатора iSCSI

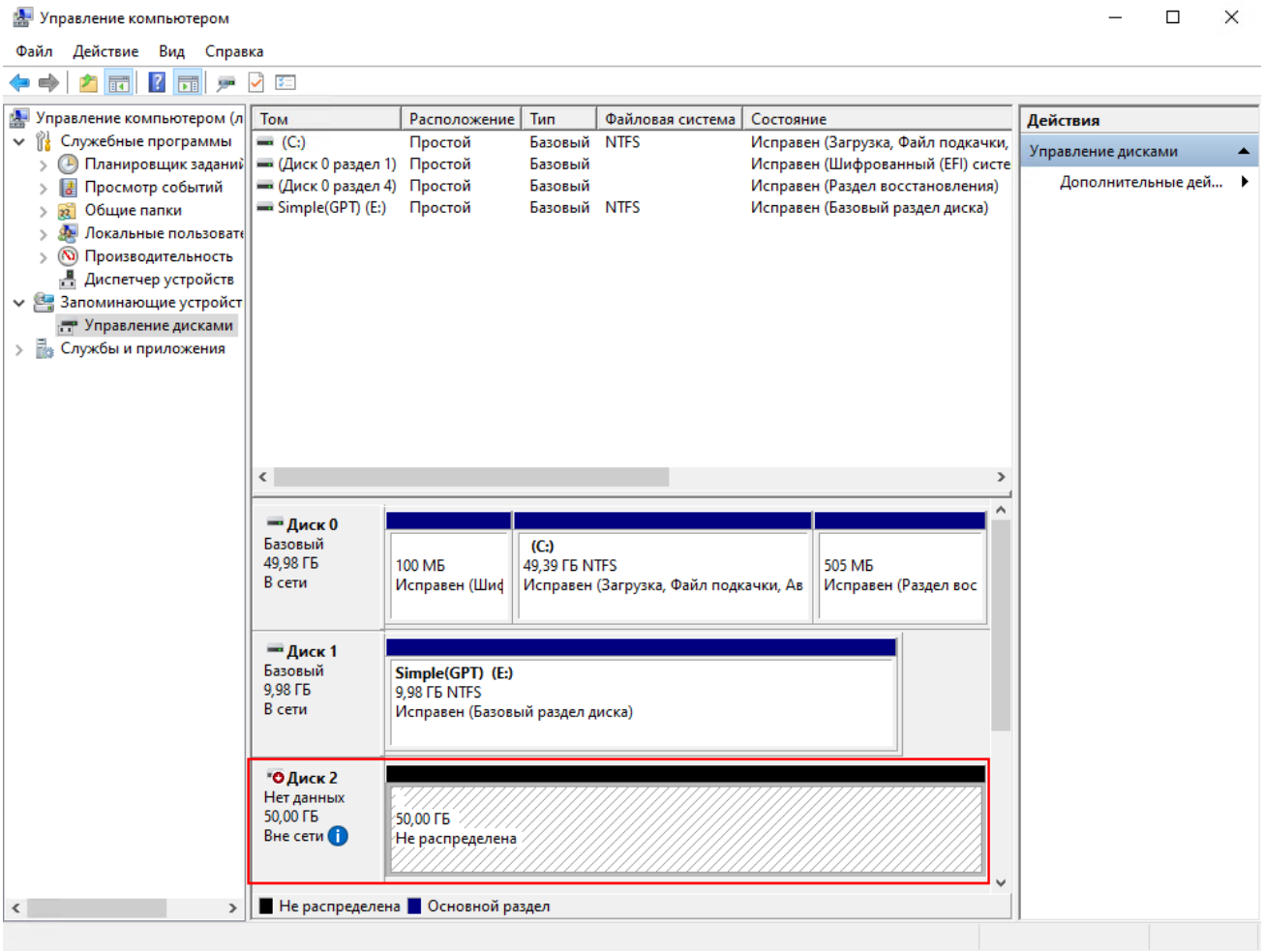
1. Последовательно выберите пункты **Панель управления** → **Администрирование** → **Инициатор iSCSI**.

   > **Примечание**
   >
   > Чтобы найти приложение **Администрирование**, возможно, необходимо будет изменить представление **панели управления** на отличное от **Главная** или **Категория** или воспользоваться поиском.

2. Если инициатор iSCSI Microsoft запускается впервые, подтвердите, что необходимо запустить службу инициатора iSCSI (Microsoft).
3. На вкладке **Цели** введите полное доменное имя или IP-адрес целевого устройства SAN и щёлкните **Быстрое подключение**.
4. Выберите логическое устройство, на котором расположено хранилище данных, и нажмите кнопку **Подключить**.

   Если логическое устройство не отображается, убедитесь, что распределение зон на целевом устройстве iSCSI позволяет машине, на которой выполняется агент, получить доступ к логическому устройству. Машину необходимо добавить в список разрешенных инициаторов iSCSI в этом целевом объекте.
5. Нажмите кнопку **ОК**.

Готовое логическое устройство SAN должно появиться в разделе **Управление дисками**, как показано на снимке экрана ниже.



Параметры резервного копирования

Чтобы изменить параметры резервного копирования, щёлкните **Изменить** в меню действий с планом, затем в блоке **Параметры резервного копирования** нажмите **Изменить**.

Доступность параметров резервного копирования

Набор доступных параметров резервного копирования зависит от следующих факторов:

- среда, в которой работает агент (Windows, Linux);
- тип данных, для которых выполняется резервное копирование (диски, файлы, виртуальные машины, данные приложения);
- место назначения резервной копии (локальная папка, сетевая папка и т. д.).

В следующей таблице представлены обобщенные сведения по доступности параметров резервного копирования.

Параметр резервного копирования	СУБД		
	PostgreSQL	MySQL	БД Microsoft Exchange Server
Функция Changed Block Tracking (CBT)	—	—	—
Быстрое инкрементное и дифференциальное резервное копирование	—	—	—
Действия при сбое задания	—	+	+
Деление	+	+	+
Еженедельное резервное копирование	+	+	+
Журнал событий Windows	—	+	+
Имя файла резервной копии	+	+	+
Команды до и после процедуры резервного копирования	+	+	+
Команды до и после захвата данных	—	—	—
Консолидация резервных копий	—	+	+
Многотомные моментальные снимки	—	—	—
Создание моментальных снимков LVM	—	—	—
Моментальные снимки оборудования SAN	—	—	—
Многопоточность	+	—	—
Обработка ошибок	—	+	+
Оповещения	—	+	+
Планирование	—	—	—
Посекторное резервное копирование	—	—	—
Проверка резервных копий	—	+	+
Производительность и окно резервного копирования	—	+	+
Служба теневого копирования томов (VSS)	—	—	—
Служба теневого копирования томов (VSS) для виртуальных машин	—	—	—
Уведомления по электронной почте	+	+	+
Уведомления в MAX	+	+	+
Уровень сжатия	+	+	+
Условия запуска задания	—	+	+
Фильтры файлов	—	—	—
Управление лентами	+	+	+
Способ резервного копирования кластера	+	—	+

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Параметр резервного копирования	СУБД		
	PostgreSQL	MySQL	БД Microsoft Exchange Server
Резервное копирование приложений	—	+	—
Кластер почтовых агентов	—	—	—
Преобразование в виртуальную машину	—	—	—

Параметр резервного копирования	Физические и виртуальные машины						
	VMware, Hyper-V	oVirt	OpenStack	OpenNebula	ECP VeiL, SpaceVM	VM-manager	Basis DynamiX Enterprise
Функция Changed Block Tracking (CBT)	+	+	+	+	+	—	+
Быстрое инкрементное и дифференциальное резервное копирование	+	+	+	+	+	+	+
Действия при сбое задания	+	+	+	+	+	+	+
Деление	+	+	+	+	+	+	+
Еженедельное резервное копирование	+	+	+	+	+	+	+
Журнал событий Windows	+	+	+	+	+	+	+
Имя файла резервной копии	+	+	+	+	+	+	+
Команды до и после процедуры резервного копирования	+	+	+	+	+	+	+
Команды до и после захвата данных	+	+	+	+	+	+	+
Консолидация резервных копий	—	—	—	—	—	—	—
Многотомные моментальные снимки	+	+	+	+	+	+	+
Создание моментальных снимков LVM	+	+	+	+	+	+	+
Моментальные снимки оборудования SAN	+	+	+	+	+	+	+

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Параметр резервного копирования	Физические и виртуальные машины						
	VMware, Hyper-V	oVirt	Open-Stack	Open-Nebula	ECP VeiL, Space-VM	VM-manager	Basis DynamiX Enter-prise
Многопоточность	—	—	—	—	—	—	—
Обработка ошибок	+	+	+	+	+	+	+
Оповещения	+	+	+	+	+	+	+
Планирование	+	+	+	+	+	+	+
Посекторное резервное копирование	+	+	+	+	+	+	+
Проверка резервных копий	+	+	+	+	+	+	+
Производительность и окно резервного копирования	+	+	+	+	+	+	+
Служба теневого копирования томов (VSS)	+	+	+	+	+	—	+
Служба теневого копирования томов (VSS) для виртуальных машин	+	+	+	+	+	—	+
Уведомления по электронной почте	+	+	+	+	+	+	+
Уведомления в MAX	+	+	+	+	+	+	+
Уровень сжатия	+	+	+	+	+	+	+
Условия запуска задания	+	+	+	+	+	+	+
Фильтры файлов	+	+	+	+	+	+	+
Управление лентами	+	+	+	+	+	+	+
Способ резервного копирования кластера	—	—	—	—	—	—	—
Резервное копирование приложений	—	—	—	—	—	—	—
Кластер почтовых агентов	—	—	—	—	—	—	—
Преобразование в виртуальную машину	+	+	+	+	+	+	+

Параметр резервного копирования	Резервное копирование на уровне файлов и дисков		
	Windows	Linux	ESXi
Функция Changed Block Tracking (CBT)	—	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Параметр резервного копирования	Резервное копирование на уровне файлов и дисков		
	Windows	Linux	ESXi
Быстрое инкрементное и дифференциальное резервное копирование	—	—	—
Действия при сбое задания	+	+	—
Деление	+	+	—
Еженедельное резервное копирование	+	+	+
Журнал событий Windows	+	+	—
Имя файла резервной копии	+	+	+
Команды до и после процедуры резервного копирования	+	+	—
Команды до и после захвата данных	—	—	—
Консолидация резервных копий	+	+	+
Многотомные моментальные снимки	—	—	—
Создание моментальных снимков LVM	—	—	—
Моментальные снимки оборудования SAN	—	—	—
Многопоточность	—	—	—
Обработка ошибок	+	+	+
Оповещения	+	+	+
Планирование	—	—	—
Посекторное резервное копирование	—	—	—
Проверка резервных копий	+	+	+
Производительность и окно резервного копирования	+	+	—
Служба теневого копирования томов (VSS)	—	—	—
Служба теневого копирования томов (VSS) для виртуальных машин	—	—	—
Уведомления по электронной почте	+	+	+
Уведомления в MAX	+	+	+
Уровень сжатия	+	+	+
Условия запуска задания	+	+	+
Фильтры файлов	—	—	—
Управление лентами	+	+	+
Способ резервного копирования кластера	—	—	—
Резервное копирование приложений	—	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Параметр резервного копирования	Резервное копирование на уровне файлов и дисков		
	Windows	Linux	ESXi
Кластер почтовых агентов	—	—	—
Преобразование в виртуальную машину	+[2]	+[2]	+[2]

Параметр резервного копирования	Приложения				
	VK WorkMail	CommuniGate Pro	Почтовые ящики Microsoft Exchange Server	RuPost	Kubernetes
Функция Changed Block Tracking (CBT)	—	—	—	—	—
Быстрое инкрементное и дифференциальное резервное копирование	—	—	—	—	—
Действия при сбое задания	—	—	+	—	—
Деление	+	—	+	+	+
Еженедельное резервное копирование	+	+	+	+	+
Журнал событий Windows	—	—	+	—	—
Имя файла резервной копии	+	+	+	+	+
Команды до и после процедуры резервного копирования	—	—	+	—	—
Команды до и после захвата данных	—	—	—	—	—

(продолжается на следующей странице)

[2] Только для резервного копирования на уровне дисков.

(продолжение с предыдущей страницы)

Параметр резервного копирования	Приложения				
	VK WorkMail	CommuniGate Pro	Почтовые ящики Microsoft Exchange Server	RuPost	Kubernetes
Консолидация резервных копий	—	—	—	—	—
Многотомные моментальные снимки	—	—	—	—	—
Создание моментальных снимков LVM	—	—	—	—	—
Моментальные снимки оборудования SAN	—	—	—	—	—
Многопоточность	—	—	—	—	—
Обработка ошибок	—	+	+	+	+
Оповещения	—	—	+	—	—
Планирование	—	—	—	—	—
Посекторное резервное копирование	—	—	—	—	—
Проверка резервных копий	—	—	+	—	—
Производительность и окно резервного копирования	—	—	+	—	—
Служба теневого копирования томов (VSS)	—	—	—	—	—
Служба теневого копирования томов (VSS) для виртуальных машин	—	—	—	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Параметр резервного копирования	Приложения				
	VK WorkMail	CommuniGate Pro	Почтовые ящики Microsoft Exchange Server	RuPost	Kubernetes
Уведомления по электронной почте	+	+	+	+	+
Уведомления в MAX	+	+	+	+	+
Уровень сжатия	+	+	+	+	+
Условия запуска задания	—	—	+	—	—
Фильтры файлов	—	—	—	—	—
Управление лентами	+	—	+	+	+
Способ резервного копирования кластера	—	—	—	—	—
Резервное копирование приложений	—	—	—	—	—
Кластер почтовых агентов	+	+	—	—	—
Преобразование в виртуальную машину	—	—	—	—	—

Оповещения

За указанное количество дней подряд не создано успешно ни одной резервной копии.

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли создаваться оповещение, если за указанный период времени планом защиты не будет успешно создано ни одной резервной копии. Помимо процессов резервного копирования, которые завершились сбоем, программа считает резервные копии, которые не выполняются по расписанию (отсутствующие резервные копии).

Оповещения создаются для конкретной машины и отображаются на вкладке **Оповещения**.

Можно задать количество дней подряд без созданных резервных копий. По истечении указанного периода будет сформировано уведомление.

Консолидация резервных копий

Этот параметр определяет, нужно ли консолидировать резервные копии при очистке или при полном удалении цепочек резервных копий.

Значение по умолчанию: **Отключено**.

Консолидация — это процесс объединения двух и более последовательных резервных копий в одну резервную копию.

Если этот параметр включен, то резервная копия, которая должна быть удалена при очистке, консолидируется со следующей зависимой резервной копией (инкрементная или дифференциальная).

В противном случае данная резервная копия сохраняется до тех пор, пока все зависимые резервные копии не станут предметом для удаления. Это поможет избежать потенциально долгой консолидации, но требует дополнительного пространства для хранения резервных копий, удаление которых откладывается. Возраст или количество резервных копий могут превысить значения, заданные в правилах хранения.

> **Важно**
>
> Необходимо учитывать, что консолидация — это просто один из методов удаления, но не альтернатива удалению. Итоговая резервная копия не будет содержать данные, которые присутствовали в удаленной резервной копии и отсутствовали в оставшейся инкрементной или дифференциальной резервной копии.

Этот параметр *не действует* в любом из следующих случаев:

- Местом сохранения резервной копии является ленточное устройство.
- Используется схема резервного копирования **Всегда инкрементное**.
- Используется *формат резервной копии* версии 12.

Резервные копии, хранимые на лентах, невозможно консолидировать. Резервные копии, сохраненные в виде одного файла (форматы версий 11 и 12) всегда консолидированы, поскольку их внутренняя структура позволяет ускорить и упростить консолидацию.

Однако если используется формат версии 12 и при этом есть несколько цепочек резервных копий (каждая цепочка хранится в отдельном файле), консолидация работает только для последней цепочки. Все цепочки, за исключением первой, удаляются. Первая цепочка сжимается до минимально

необходимого размера для хранения метаданных (~12 КБ). Эти метаданные требуются, чтобы обеспечить согласованность данных при одновременном выполнении операций чтения и записи. Сразу же после применения правила хранения резервные копии, входящие в эти цепочки, исчезают из графического интерфейса пользователя, хотя физически они существуют до удаления всей цепочки.

Во всех остальных случаях резервные копии, удаление которых отложено, помечаются значком корзины () в графическом пользовательском интерфейсе. Если удалить такую резервную копию, щёлкнув значок X, будет выполнена консолидация. Резервные копии, которые хранятся на ленточном накопителе, удаляются из графического интерфейса пользователя только при перезаписи или удалении данных на ленте.

Имя файла резервной копии

Этот параметр определяет имена файлов резервных копий, создаваемые планом защиты.

Эти имена можно увидеть в диспетчере файлов при обзоре хранилища резервной копии.

Что такое файл резервной копии?

В зависимости от схемы резервного копирования и используемого *формата резервной копии* каждый план защиты создает один или несколько файлов в хранилище резервной копии. В следующей таблице перечислены файлы, которые могут быть созданы на каждой машине или почтовом ящике.

	Всегда инкрементное	**Другие схемы резервного копирования**
Формат резервной копии **Версии 11**	Один файл TIB и один файл метаданных XML	Несколько файлов TIB и один файл метаданных XML (традиционный формат)
Формат резервной копии **Версии 12**	Один файл TIBX на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии).	

Все файлы имеют одинаковое имя с добавлением метки времени или порядкового номера, или без них. При создании или редактировании плана защиты можно задать такое имя (называемое именем файла резервной копии).

Примечание

Метка времени добавляется в имя файла резервной копии в одном из следующих случаев:

- при использовании формата резервного копирования ”Версия 11”;

- если резервное копирование или репликация выполняются в сетевую папку InfoDiode.

После изменения имени файла резервной копии следующей будет полная резервная копия, если не указано имя файла существующей резервной копии той же машины. В последнем случае будет создана полная, инкрементная или дифференциальная резервная копия в соответствии с расписанием плана защиты.

Обратите внимание, что можно задать имена файлов резервных копий для хранилищ, обзор которых невозможно выполнить с помощью диспетчера файлов (например, ленточного устройства). Это целесообразно в том случае, если требуется просмотр пользовательских имен на вкладке **Хранилища резервных копий**.

Где можно просмотреть имена файлов резервных копий?

Выберите вкладку **Хранилища резервных копий**, а затем выберите группу резервных копий.

- Имя файла по умолчанию отображаются на панели **Подробности**.
- Если имена файлов заданы не по умолчанию, они отобразятся непосредственно на вкладке **Хранилища резервных копий** в столбце **Имя**.

Примечание

Если резервное копирование выполняется в сетевую папку InfoDiode, то файлы резервных копий не отображаются в веб-консоли Кибер Бэкап.

Ограничения для имени файла резервной копии

- Имя файла резервной копии не должно заканчиваться цифрой.

  Чтобы имя не заканчивалось цифрой, в конце имени резервной копии по умолчанию добавляется буква ”A”. При создании пользовательского имени убедитесь, что оно не заканчивается цифрой. При использовании переменных имя не должно заканчиваться на переменную, поскольку она может заканчиваться цифрой.

- Имя файла резервной копии не должно содержать следующие символы: **()&?*$<>”:\|/#%**, символы окончания строки (**\n**) и знаки табуляции (**\t**).

Имя файла резервной копии по умолчанию

Имя файла резервной копии по умолчанию имеет вид:

- `[Имя машины]-[Идентификатор плана]-[Уникальный идентификатор]A`.
- `[Идентификатор почтового ящика]_почтовый ящик_[Идентификатор плана]A` — для резервной копии почтового ящика.

При сохранении резервной копии в сетевой папке InfoDiode (после выполнения *предварительной настройки*) в имени файла автоматически указывается метка времени.

На рисунке далее приведены примеры имён файлов резервных копий.



Имя файла резервной копии состоит из следующих элементов:

- `[Имя машины]` Эта переменная заменяется именем машины (такое же имя отображается в веб-консоли Кибер Бэкап) для всех типов резервных копий данных.
- `[Идентификатор плана]` Эта переменная заменяется уникальным идентификатором плана защиты. При переименовании плана это значение не изменяется.
- `[Уникальный идентификатор]` Эта переменная заменяется уникальным идентификатором выбранной машины или почтового ящика. При изменении имени машины или UPN почтового ящика это значение не изменяется.
- `[Идентификатор почтового ящика]` Эта переменная заменяется UPN почтового ящика.
- Защитная буква ”A” добавляется для того, чтобы имя файла не заканчивалось цифрой.
- Метка времени автоматически добавляется, если выполнена *предварительная настройка* для сохранения файла в сетевой папке InfoDiode.

Имена без переменных

Если вы измените имя файла резервной копии на `MyBackup`, файлы резервной копии будут выглядеть как в следующих примерах. Оба примера предполагают, что ежедневные инкрементальные резервные копирования запланированы в 14:40, начиная с 13 сентября 2016 года.

Для формата ”Версия 12” со схемой резервного копирования **Всегда инкрементное**:

```
MyBackup.tibx
```

Для формата ”Версии 12” с другими схемами резервного копирования:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

Для формата ”Версия 11” со схемой резервного копирования **Всегда инкрементное**:

```
MyBackup.xml
MyBackup.tib
```

Для формата ”Версии 11” с другими схемами резервного копирования:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Использование переменных

Кроме переменных, используемых по умолчанию, можно использовать переменную `[Имя плана]`, которая заменяется именем плана защиты.

Если выбрано резервное копирование нескольких машин или почтовых ящиков, имя файла резервной копии должно содержать переменную `[Имя машины]`, `[Идентификатор почтового ящика]` или `[Уникальный идентификатор]`.

Сравнение имени файла резервной копии и упрощенного именования файлов

Используя обычный текст и/или переменные можно создать такие же имена файлов, как и в более ранних версиях Кибер Бэкап. Однако упрощённые имена файлов не могут быть созданы заново — в версии 11 имя файла содержит отметку времени, если не используется формат одного файла.

Примеры использования

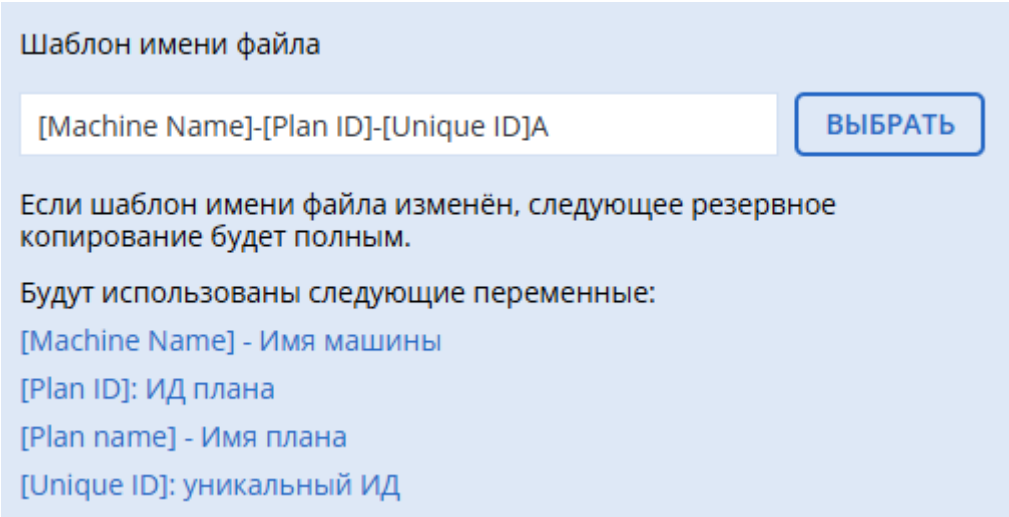
- **Просмотр дружественных к пользователю имен файлов**

  При обзоре хранилища с помощью диспетчера файлов легко отличить резервные копии.

- **Продолжение существующей последовательности резервных копий**

  Предположим, что план защиты применен к одной машине и необходимо удалить эту машину из веб-консоли Кибер Бэкап или удалить агент вместе с его настройками конфигурации. После повторного добавления машины или переустановки агента можно применить план защиты для продолжения выполнения резервного копирования в ту же резервную копию или последовательность резервных копий. Просто перейдите к этому параметру, щёлкните **Выбрать** и выберите требуемую резервную копию.

  Кнопка **Обзор** позволяет показать резервные копии в хранилище, выбранном в разделе **Место сохранения резервной копии** на панели плана защиты. Обзор невозможно выполнить за пределами этого хранилища.

- **Переход с предыдущих версий продукта**

  Если при обновлении плана защиты до новой версии он не был автоматически перенесен, создайте план заново и примените его к старому файлу резервной копии. Если для резервного копирования выбрана только одна машина, щёлкните **Обзор** и выберите требуемую резервную

копию. Если для резервного копирования выбраны несколько машин, заново создайте старое имя файла резервной копии с использованием переменных.

Примечание

Кнопка **Выбрать** доступна только для планов защиты, которые созданы и применены для одного устройства.

Формат резервной копии

Этот параметр показывает формат резервных копий, созданных планом защиты. Он доступен только для уже созданных планов защиты, в которых для сохранения резервных копий используются управляемые хранилища с защитой паролем (см. *Защита хранилища паролем*) или с включенной дедупликацией (см. *Дедупликация*).</p>

Существуют следующие форматы:

- **Версия 12**

  Формат, который используется по умолчанию во всех сценариях резервного копирования и восстановления, кроме сценария с сохранением резервных копий в управляемые хранилища с защитой паролем или с включенной дедупликацией.

- **Версия 11**

  Этот формат выбирается автоматически, если местом сохранения резервной копии (или репликации) является управляемое хранилище с защитой паролем или с включенной дедупликацией. Для изменения формата на ”Версия 12” обратитесь к статье ниже.

  Создание резервных копий почтовых ящиков и групп обеспечения доступности баз данных (DAG) в этом формате не поддерживается.

  Формат архива ”Версия 11” не поддерживается в хранилищах Кибер Инфраструктура и Кибер Хранилище.

  Примечание

  Вариант **Автоматический выбор** в данный момент не поддерживается.

Формат резервной копии и файлы резервных копий

Для хранилищ резервных копий, обзор которых можно выполнить с помощью диспетчера файлов (например, локальные или сетевые папки), формат резервных копий определяет количество файлов и их расширение. Можно назначить имена файлов используя параметр *имя файла резервной копии*. В следующей таблице перечислены файлы, которые создаются на каждой машине или почтовом ящике, и доступные данные для резервного копирования.

	Всегда инкрементное	**Другие схемы резервного копирования**	**Источник данных**
Формат резервной копии **Версии 11**	Один файл TIB и один файл метаданных XML	Несколько файлов TIB и один файл метаданных XML (традиционный формат)	Файлы и папки, физическая машина, виртуальная машина, Microsoft SQL Server и Microsoft Exchange Server
Формат резервной копии **Версии 12**	Один файл TIBX на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии).		Все поддерживаемые источники данных

Изменение формата резервной копии на формат ”Версия 12”

Для корректного перехода резервных копий с формата ”Версия 11” на формат ”Версия 12” укажите местом сохранения резервной копии хранилище, которое не защищено паролем и для которого выключена дедупликация. При этом происходит следующее:

- Следующая резервная копия будет полной.
- В хранилищах резервных копий, которые доступны для обзора в диспетчере файлов (например, локальные или сетевые папки), создается новый файл с расширением TIBX. Новый файл имеет имя исходного файла с добавлением суффикса ”_v12A”.
- Правила хранения и репликации применяются только к новым резервным копиям.
- Старые резервные копии не удаляются и остаются доступными на вкладке **Хранилища резервных копий**. Их можно удалить вручную.

Дедупликация в архиве

Формат ”Версия 12” поддерживает дедупликацию в архиве, которая обеспечивает указанные ниже преимущества.

- Существенно меньший размер резервной копии со встроенной дедупликацией на уровне блоков для любого типа данных.
- Эффективная обработка жестких ссылок обеспечивает отсутствие дублированных элементов в хранилище данных.
- Фрагментирование на основе хэша.

Примечание

Дедупликация в архиве включена по умолчанию для всех резервных копий в формате ”Версия 12”. Для отключения дедупликации обратитесь к статье в базе знаний Отключение внутренней дедупликации архива на стороне агента.

Не рекомендуется отключать дедупликацию, кроме случаев использования системы хранения данных со встроенной поддержкой дедупликации.

Проверка резервных копий

Проверка — это операция по определению возможности восстановления данных из резервной копии. Если этот параметр включен, то каждая резервная копия, созданная в соответствии с планом защиты, проверяется непосредственно после создания. Эта операция выполняется агентом защиты.

Значение по умолчанию: **Отключено**.

При проверке вычисляется контрольная сумма для каждого блока данных, который можно восстановить из данной резервной копии.

Проверка — это длительный процесс даже при инкрементном или дифференциальном резервном копировании небольших объемов данных. Причина заключается в том, что во время операции проверяются не только данные, физически присутствующие в резервной копии, но и все данные, которые восстанавливаются при выборе этой резервной копии. Это требует доступа к созданным ранее резервным копиям.

Хотя успешная проверка означает высокую вероятность восстановления данных, проверяются не все факторы, влияющие на процесс восстановления. При резервном копировании операционной системы рекомендуем выполнить тестовое восстановление с загрузочного носителя на запасной жесткий диск или *запустить виртуальную машину из резервной копии* в среде ESXi или Hyper-V.

Функция Changed Block Tracking (CBT)

Этот параметр применим к следующим ресурсам:

- резервным копиям на уровне дисков для:
  - физических машин с ОС Windows,
  - виртуальных машин;
- резервным копиям баз данных:
  - Microsoft SQL Server,
  - Microsoft Exchange Server.

Этот параметр применим к следующим платформам виртуализации:

- VMware ESXi версии 6.5 и новее,
- Hyper-V Server 2012 R2 и новее,
- oVirt версии 4.5 и новее,
- zVirt версии 4.1 и новее,
- ROSA Virtualization 3.0, 3.1, 4.0,
- РЕД Виртуализация 8.0 и новее.

Примечание

Для успешного применения параметра в средах виртуализации oVirt (zVirt, ROSA Virtualization) в настройках диска виртуальной машины активируйте флаг **Включить инкрементное резервное копирование**. Использовать технологию CBT можно только для виртуальных дисков формата QCOW.

Значение по умолчанию: **Включено**.

Этот параметр определяет, будет ли использоваться технология Changed Block Tracking (CBT) при выполнении инкрементного или дифференциального резервного копирования.

Технология CBT ускоряет процесс резервного копирования. Изменения содержимого диска или базы данных постоянно отслеживаются на уровне блоков. При запуске резервного копирования изменения могут быть незамедлительно сохранены в резервную копию.

Способ резервного копирования кластера

Этот параметр относится к резервному копированию групп доступности Always On (AAG) в Microsoft SQL Server, групп обеспечения доступности баз данных (DAG) в Microsoft Exchange Server, кластера СУБД Jatoba (JaDog) и баз данных PostgreSQL на основе Patroni.

Параметр действует только в случае, если для резервного копирования выбрана сама группа доступности или кластер, а не отдельные содержащиеся в них узлы или базы данных. Если вы выберете отдельные элементы, содержащиеся в группе или кластере, то будут созданы резервные копии только выбранных копий элементов.

Настройка параметра для групп доступности Always On (AAG)

Чтобы параметр действовал для групп доступности Always On (AAG), агент для SQL должен быть установлен на всех узлах AAG. Дополнительные сведения о резервном копировании групп доступности Always On см. в разделе *Защита группы доступности Always On (AAG)*.

Можно выбрать один из следующих вариантов:

- **Дополнительная реплика, если возможно**

  Если все дополнительные реплики отключены от сети, создается резервная копия основной реплики. Резервное копирование основной реплики может замедлить работу SQL Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

- **Дополнительная реплика**

  Если все дополнительные реплики отключены, резервное копирование не будет выполнено. Создание резервной копии дополнительной реплики не влияет на производительность сервера SQL и позволяет расширить окно резервного копирования. Однако пассивные реплики могут содержать не самые последние данные, так как часто настроены на асинхронное обновление (с отставанием).

- **Основная реплика**

  Если основная реплика отключена, резервное копирование не будет выполнено. Резервное копирование основной реплики может замедлить работу SQL Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

Значение по умолчанию: **Дополнительная реплика, если возможно**.

Независимо от значения данного параметра, для обеспечения целостности базы данных, программа пропускает базы данных, которые до начала резервного копирования не находятся в состоянии **СИНХРОНИЗИРОВАНО** или **СИНХРОНИЗАЦИЯ**. Если пропущены все базы данных, резервное копирование не будет выполнено.

Настройка параметра для групп обеспечения доступности баз данных (DAG) в Microsoft Exchange Server

Чтобы параметр действовал, агент для Exchange должен быть установлен на всех узлах DAG. Дополнительные сведения о резервном копировании групп обеспечения доступности баз данных см. в разделе *Защита групп обеспечения доступности базы данных (DAG)*.

Можно выбрать один из следующих вариантов:

- **Пассивная копия, если возможно**

  Если все пассивные копии выключены, создается резервная копия активной копии. Резервное копирование активной копии может замедлить работу Exchange Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

- **Пассивная копия**

  Если все пассивные копии выключены, резервное копирование завершится сбоем. Создание резервной копии пассивных копий не влияет на производительность Exchange Server и позволяет расширить окно резервного копирования. Однако пассивные копии могут содержать не самые последние данные, так как часто настроены на асинхронное обновление (с отставанием).

- **Активная копия**

  Если активная копия выключена, резервное копирование завершится сбоем. Резервное копирование активной копии может замедлить работу Exchange Server, но будет обеспечено самое актуальное состояние данных в резервной копии.

Значение по умолчанию: **Пассивная копия, если возможно**.

Независимо от значения данного параметра, для обеспечения целостности базы данных, программа пропускает базы данных, которые до начала резервного копирования не находятся в состоянии **ИСПРАВНА** или **АКТИВНА**. Если пропущены все базы данных, резервное копирование не будет выполнено.

Настройка параметра для кластеров СУБД Jatoba (JaDog) и баз данных PostgreSQL на основе Patroni

Выберите метод резервного копирования, укажите источник данных и тип реплики.

Метод резервного копирования

- **Удаленное**. Требуется установка агента на одном узле кластера.
- **Локальное**. Требуется установка агентов на каждом узле кластера. Поддерживается многопоточность.

Значение по умолчанию: **Удаленное**.

Для использования многопоточности при резервном копировании кластера в блоке **Метод резервного копирования** необходимо выбрать **Локальное**.

Источник данных

- **Дополнительная реплика или ведомый узел, если возможно**. Если все дополнительные реплики отключены, будет создана резервная копия основной реплики.
- **Дополнительная реплика или ведомый узел**. Если все дополнительные реплики отключены, резервное копирование не будет выполнено.
- **Основная реплика или основной узел**. Если основная реплика отключена, резервное копирование не будет выполнено.

Значение по умолчанию: **Дополнительная реплика или ведомый узел, если возможно**.

Выбор реплики

- **Любая**. Будет выбрана любая дополнительная реплика.
- **Синхронная**. Будет выбрана синхронная реплика, если возможно.
- **Асинхронная**. Будет выбрана асинхронная реплика, если возможно.

Значение по умолчанию: **Любая**.

> **Примечание**
>
> Резервное копирование основной реплики может замедлить работу PostgreSQL, но обеспечит актуальность данных в резервной копии.

Уровень сжатия

Этот параметр определяет уровень сжатия данных при резервном копировании. Доступные уровни: **Отсутствует**, **Обычное**, **Высокое**, **Максимальное**.

Значение по умолчанию: **Обычное**.

Чем выше уровень сжатия, тем больше времени занимает процесс резервного копирования, но созданная резервная копия занимает меньше места. В данный момент уровни ”Высокое” и ”Максимальное” работают аналогичным образом.

Оптимальный уровень сжатия данных зависит от типа копируемых данных. Даже максимальное сжатие не уменьшит значительно размер резервной копии, состоящей из уже сжатых файлов, например JPG, PDF или MP3. Но такие форматы, как DOC или XLS, сжимаются хорошо.

Многопоточность

Этот параметр позволяет указать способ использования многопоточности при резервном копировании PostgreSQL.

Режим многопоточности доступен для отдельных экземпляров PostgreSQL, кластеров Jatoba (JaDog) и Patroni.

Примечание

Для использования режима многопоточности в кластерах необходимо настроить метод резервного копирования (подробнее см. в разделе *Способ резервного копирования кластера*).

Предварительные требования

- Агент для PostgreSQL должен быть установлен на тот же сервер, где находится экземпляр PostgreSQL.
- Резервное копирование кластеров в многопоточном режиме поддерживается начиная с версии Кибер Бэкап 19.0.

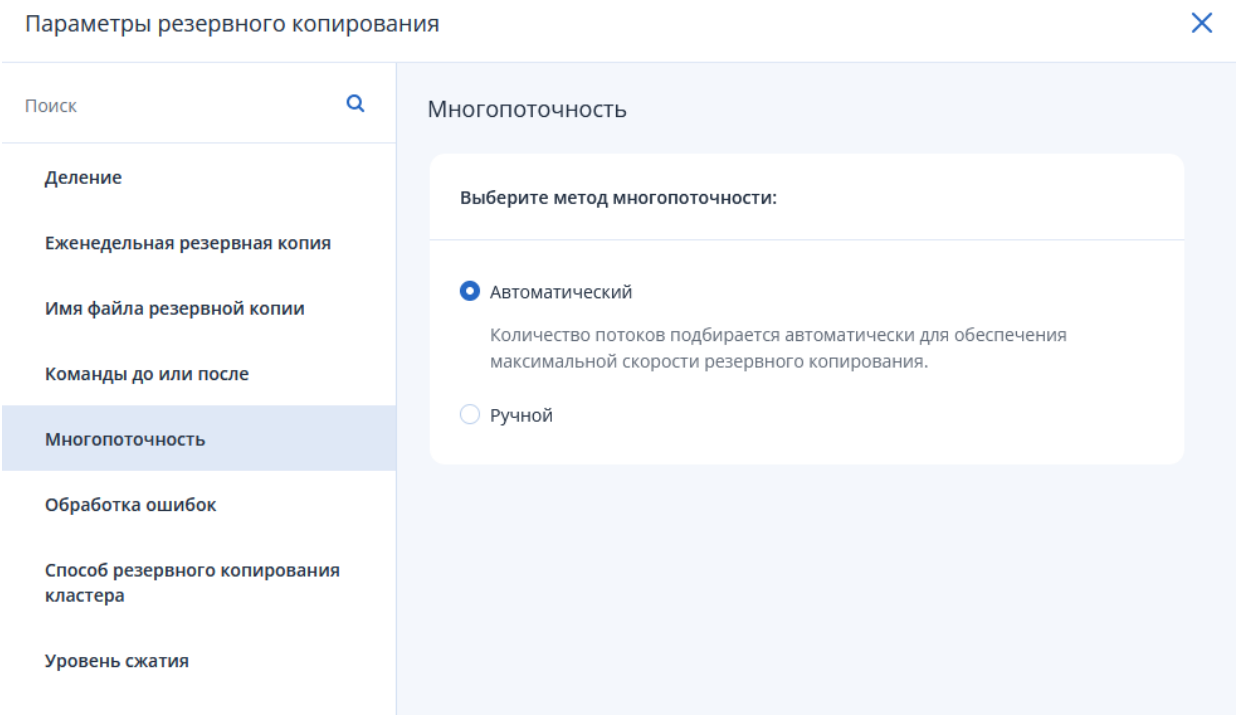
Настройка

1. В меню **Параметры резервного копирования** щёлкните **Многопоточность**.
2. Выберите один из двух следующих вариантов:
    1. **Автоматический**. Значение в автоматическом режиме: 16.
    2. **Ручной**. Установите с помощью кнопок управления необходимое число потоков в диапазоне от 1 до 32.

       При установке количества потоков вручную примите во внимание следующие обстоятельства:

       - увеличение числа потоков создает дополнительную нагрузку на дисковую подсистему;
       - во избежание создания узких мест в системе, увеличивайте число потоков только в том

случае, если в результате общая скорость выполнения плана повышается.



3. Нажмите **Сохранить**.

Уведомления по электронной почте

Этот параметр позволяет задать уведомления по электронной почте о событиях, которые возникают во время резервного копирования.

Значение по умолчанию: **Использовать глобальные настройки для отправки уведомлений по электронной почте.** Глобальные настройки устанавливаются, как описано в разделе *Уведомления по электронной почте*.

Перед настройкой уведомлений необходимо настроить параметры сервера электронной почты (см. раздел *Сервер электронной почты*).

Порядок настройки уведомлений по электронной почте для плана защиты

1. Переведите переключатель **Использовать глобальные настройки для отправки уведомлений по электронной почте** в положение **Выключено**.
2. В поле **Адрес электронной почты получателя** введите адрес электронной почты, на который будут приходить уведомления. Можно указать несколько адресов, разделяя их точкой с запятой.
3. В поле **Шаблон темы** укажите шаблон уведомления.

   Можно использовать следующие переменные:

- `[Оповещение]` — сводка оповещений;
- `[Устройство]` — имя устройства;
- `[План]` — название плана, для которого создано оповещение;
- `[Сервер управления]` — имя хоста машины, на которой установлен сервер управления;
- `[Отдел]` — название отдела, которому принадлежит машина.

Шаблон по умолчанию: [Оповещение] Устройство: [Устройство] План: [План]

4. Установите флажки для событий, о которых необходимо получать уведомления. Их можно выбрать из списка всех оповещений, которые возникают во время резервного копирования, сгруппированных по степени серьезности.
5. В блоке **Группировка уведомлений** выберите один из вариантов:
   - **Включено** (значение по умолчанию) — уведомления группируются по планам защиты (один план может быть применён к нескольким устройствам).

     При выборе этого значения по умолчанию устанавливается флажок **Получать успешные сгруппированные уведомления**. В этом случае отправляются все группы уведомлений, включая полностью успешные. Снимите флажок, если уведомления о полностью успешных операциях не требуются.
   - **Отключено** — уведомления отправляются по каждому устройству отдельно, даже если к ним применён один и тот же план защиты.

> **Примечание**
>
> Группировка уведомлений работает с ресурсами PostgreSQL, CommuniGate Pro, VK WorkMail, VK WorkDisk, Mailion и Kubernetes.

6. Чтобы применить настройки, нажмите кнопку **Готово**.

   Чтобы вернуться к последним сохранённым настройкам, нажмите кнопку **Очистить**.

Уведомления в MAX

Параметр резервного копирования **Уведомления в MAX** определяет возможность автоматической отправки уведомлений о событиях резервного копирования (включая предупреждения и сообщения об ошибках) в созданный пользователем канал на платформе MAX. Уведомления направляются с помощью интеграции через специализированного чат-бота.

Можно использовать:

- Глобальные настройки уведомлений в MAX (подробнее см. в разделе *Настройка уведомлений в MAX*).
- Параметры резервного копирования по умолчанию (см. в раздел *Параметры резервного копирования по умолчанию*). Они дополняют глобальные настройки.
- Индивидуальные настройки уведомлений в MAX для текущего плана защиты. Они дополняют глобальные настройки. О том, как установить индивидуальные параметры для текущего плана защиты, см. далее в этом разделе.

Значение по умолчанию: **Использовать глобальные настройки для отправки MAX уведомлений** (если настроены *параметры по умолчанию*, то применяются они).

> **Примечание**
>
> Изменение *глобальных настроек* автоматически обновляет параметры во всех связанных с ними планах защиты. Изменение *настроек по умолчанию* обновляет параметры только в новых планах защиты и не затрагивает существующие.

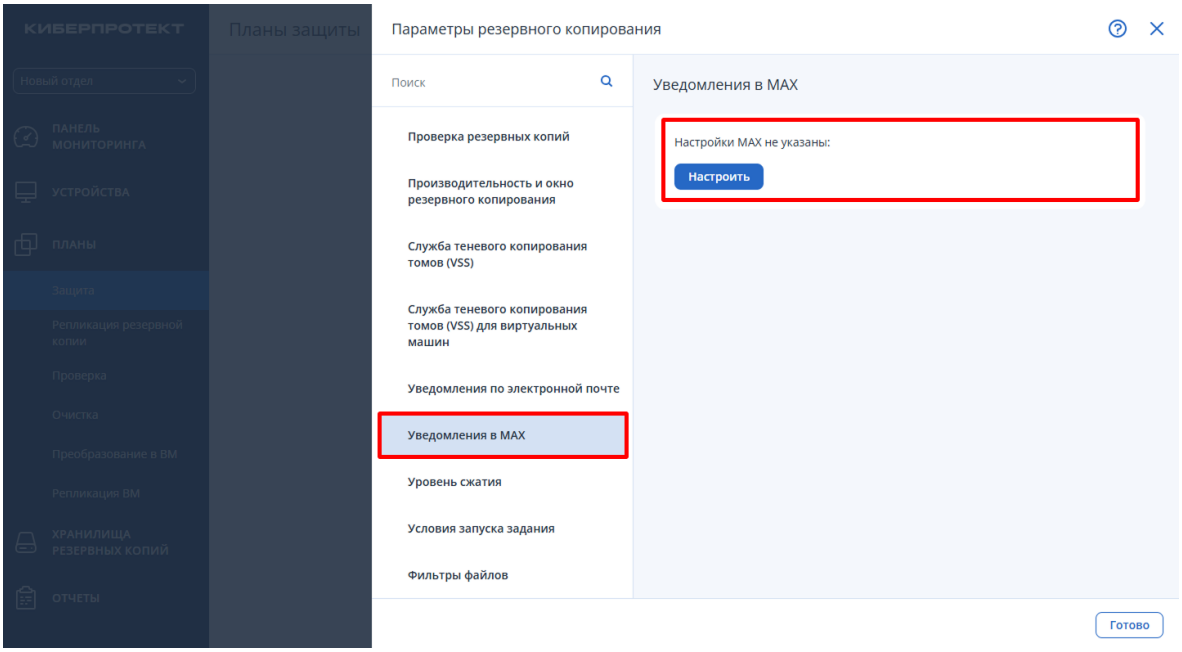
Настройка уведомлений в MAX для плана защиты

Применение глобальных настроек

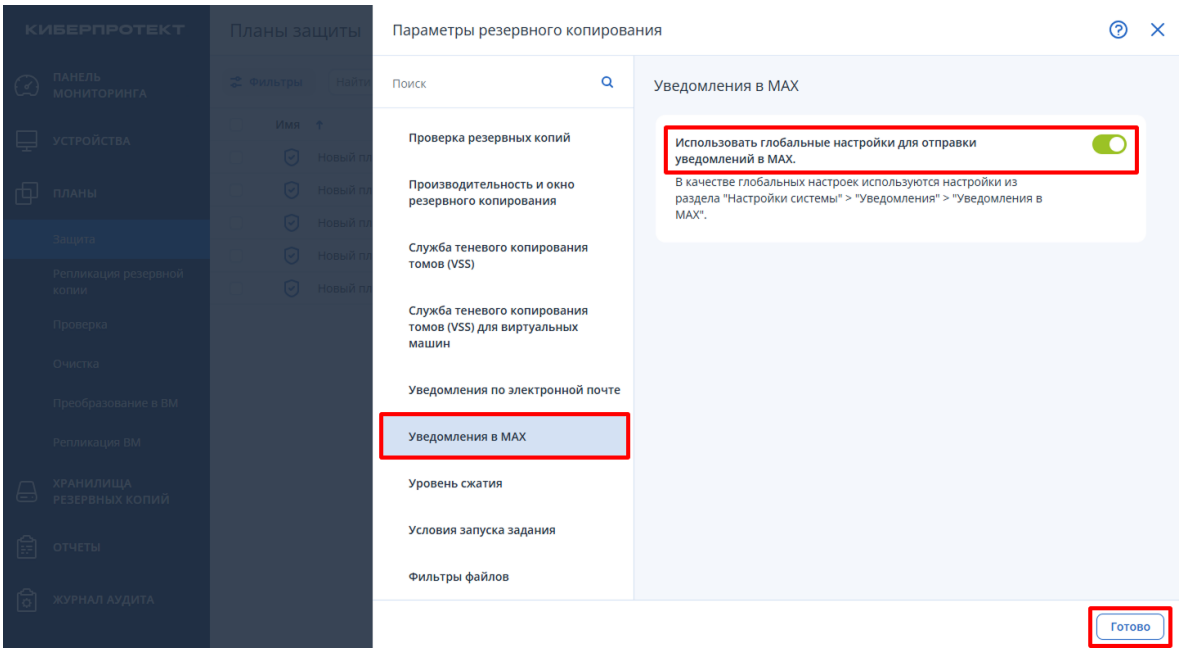
Для применения в плане защиты глобальных настроек отправки уведомлений в MAX выполните следующие действия:

1. В веб-консоли Кибер Бэкап нажмите **Планы** → **Защита**, затем выберите или *создайте* план защиты.
2. Если план защиты существует, в боковой панели **Действия** выберите **Изменить**. Далее в блоке **Параметры резервного копирования** нажмите **Изменить**.

   При создании нового плана защиты в блоке **Параметры резервного копирования** нажмите **Изменить**.
3. В списке параметров резервного копирования выберите **Уведомления в MAX**.
   - Если глобальные настройки не заданы, появится соответствующее сообщение. В таком случае нажмите **Настроить** и укажите требуемые настройки (подробнее см. в разделе *Настройка уведомлений в MAX*).



- Если глобальные настройки заданы, переведите переключатель **Использовать глобальные настройки для отправки уведомлений в MAX** в положение **Включено** и нажмите кнопку **Готово**.



В результате к плану защиты будут применены глобальные настройки уведомлений в MAX.

Настройка индивидуальных уведомлений в MAX для плана защиты

Чтобы настроить индивидуальные параметры уведомлений в MAX для плана защиты, выполните следующие действия:

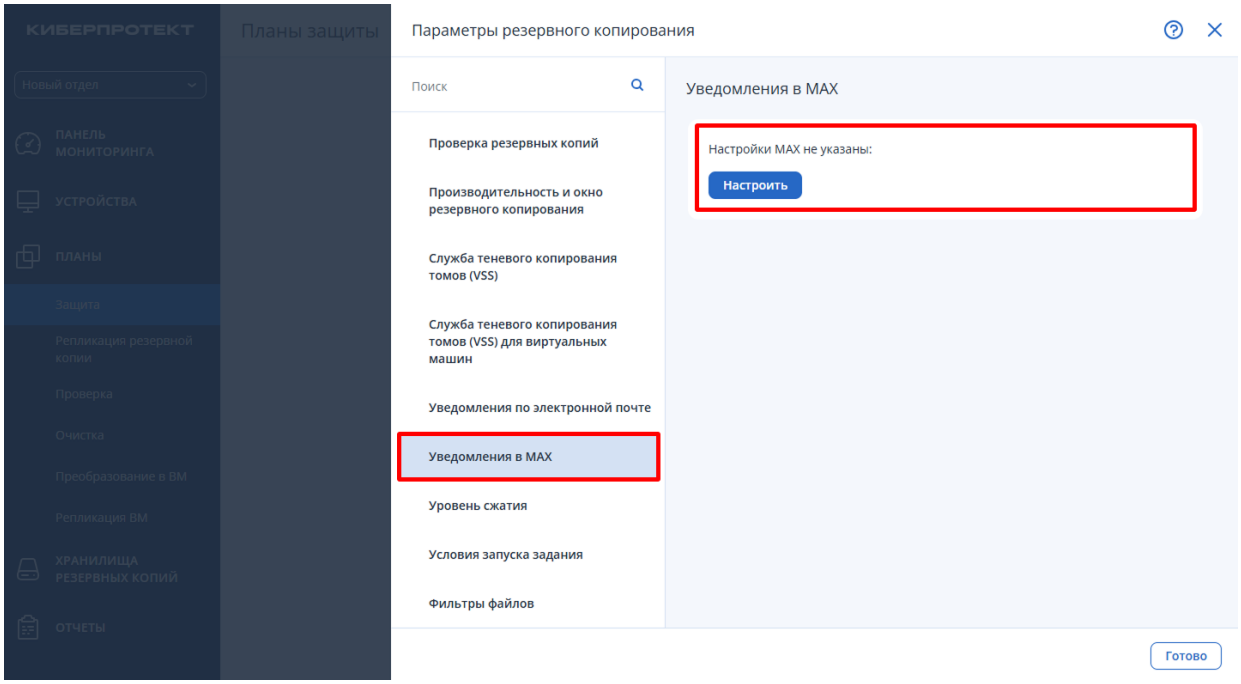
1. В веб-консоли Кибер Бэкап нажмите **Планы** → **Защита**, затем выберите или *создайте* план защиты.

2. Если план защиты существует, в боковой панели **Действия** выберите **Изменить**. Далее в блоке **Параметры резервного копирования** нажмите **Изменить**.

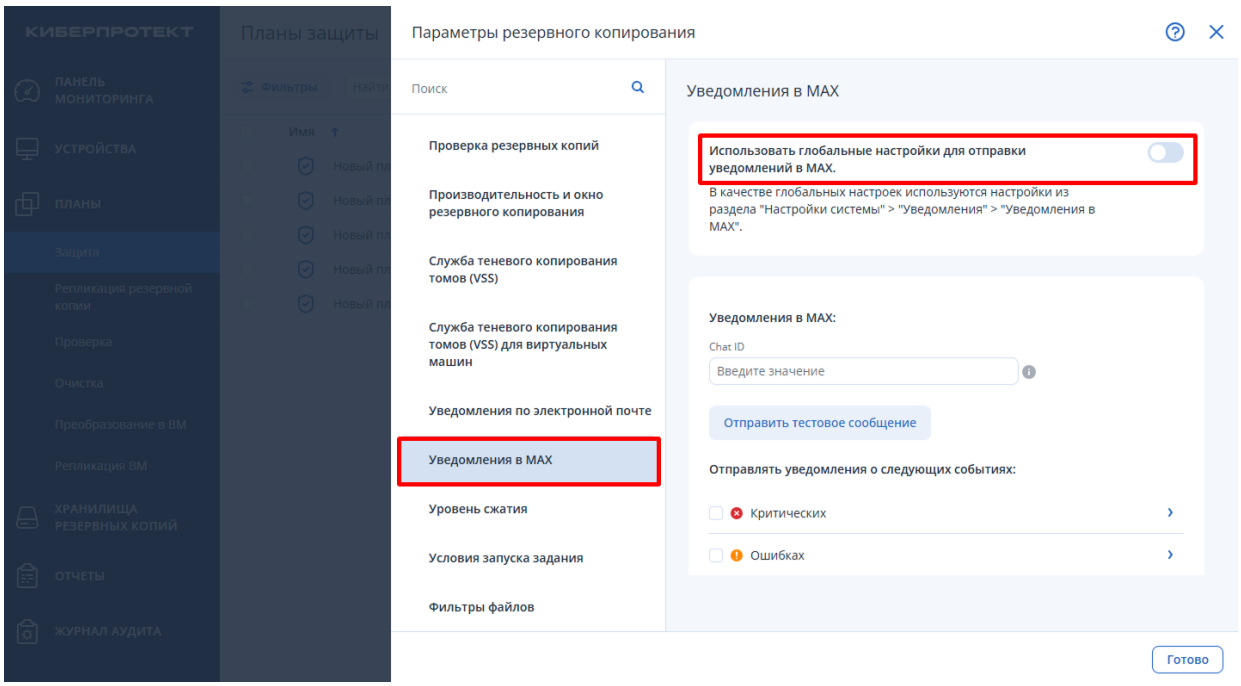
   При создании нового плана защиты в блоке **Параметры резервного копирования** нажмите **Изменить**.

3. В списке параметров резервного копирования выберите **Уведомления в MAX**.

4. Если глобальные настройки не заданы, появится соответствующее сообщение. В таком случае указать индивидуальные настройки для плана защиты будет нельзя. Задайте глобальные настройки в окне **Уведомления в MAX** → **Настроить** (подробнее см. в разделе *Настройка уведомлений в MAX*).



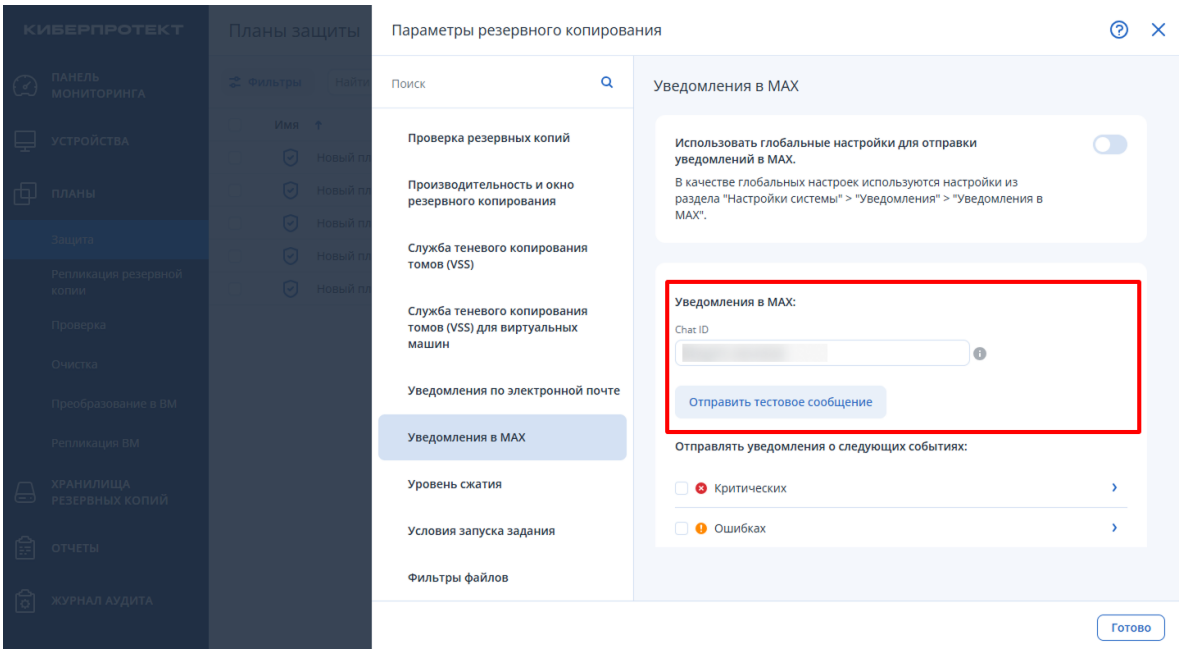
5. Переведите переключатель **Использовать глобальные настройки для отправки уведомлений в MAX** в положение **Выключено**.



6. Укажите требуемые индивидуальные настройки плана защиты:

   1. В поле **Chat ID** через запятую укажите не более 10 идентификаторов чатов, в которые будут отправляться уведомления.

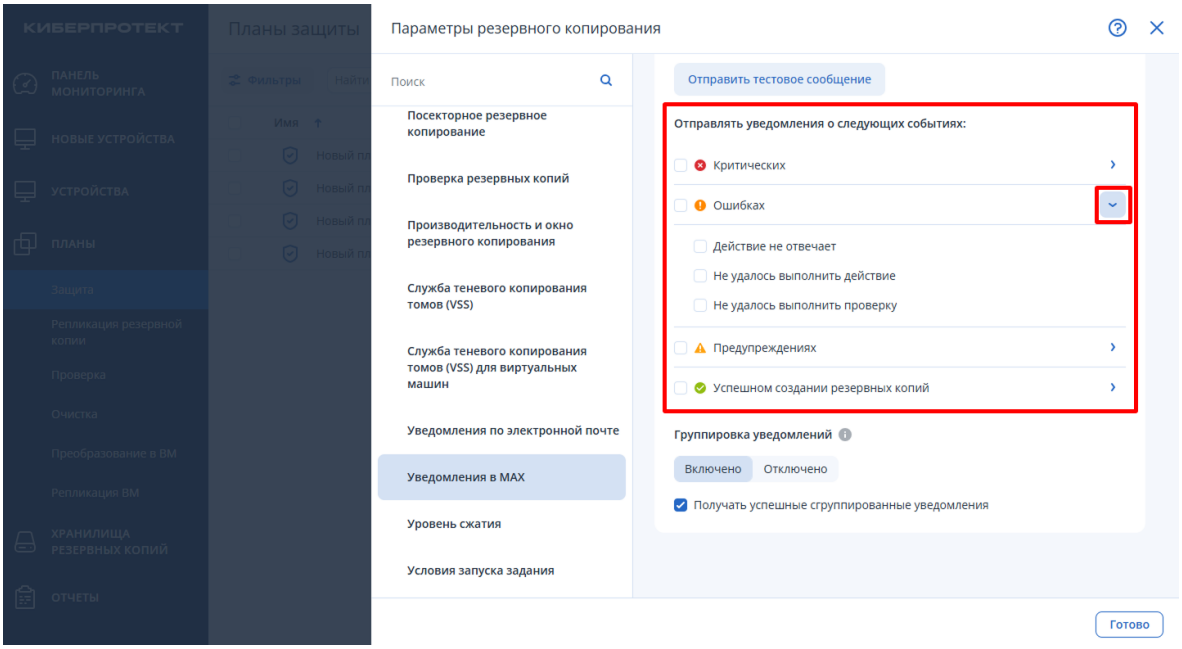
      Для проверки в указанные чаты можно отправить тестовое сообщение соответствующей кнопкой.



Примечание

Если один и тот же чат указан в глобальных и в индивидуальных настройках, уведомление в него придёт дважды: сначала в соответствии с глобальными настройками, а затем — с индивидуальными.

2. В блоке **Отправлять уведомления о следующих событиях:** выберите события, для которых будут направляться уведомления. Для детального просмотра раскройте список, нажав на иконку со стрелкой в строке названия группы событий. По умолчанию события не выбраны.



3. В блоке **Группировка уведомлений** выберите один из вариантов:

   - **Включено** (значение по умолчанию) — уведомления группируются по планам защиты (один план может быть применён к нескольким устройствам).

     При выборе этого значения по умолчанию устанавливается флажок **Получать успешные сгруппированные уведомления**. В этом случае отправляются все группы уведомлений, включая полностью успешные. Снимите флажок, если уведомления о полностью успешных операциях не требуются.

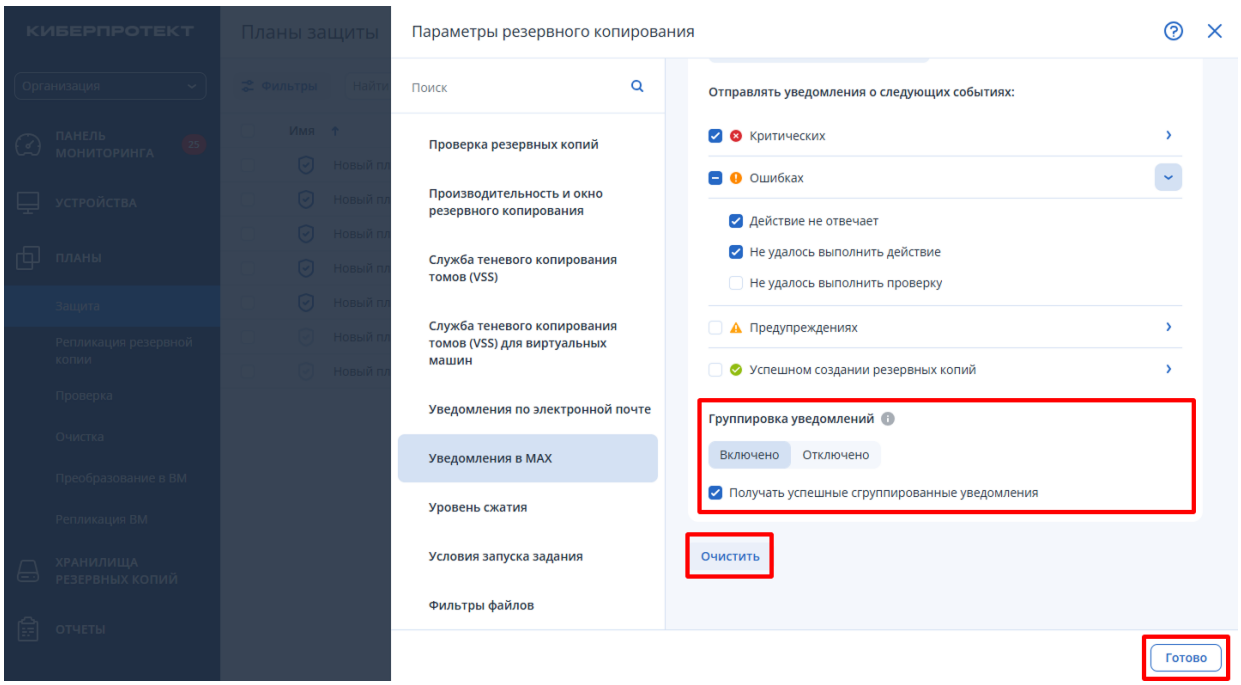
   - **Отключено** — уведомления отправляются по каждому устройству отдельно, даже если к ним применён один и тот же план защиты.

Примечание

Группировка уведомлений работает с ресурсами PostgreSQL, CommuniGate Pro, VK WorkMail, VK WorkDisk, Mailion и Kubernetes.

7. Чтобы применить настройки, нажмите кнопку **Готово**.

   Чтобы вернуться к последним сохранённым настройкам, нажмите кнопку **Очистить**.



Обработка ошибок

Эти параметры позволяют указать, как должны обрабатываться ошибки, возникшие во время резервного копирования.

В случае ошибки повторить операцию

Значение по умолчанию: **Включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. При повторном запуске дозапись в резервную копию продолжается с места прерывания.

Задайте временной интервал и количество попыток. Попытки будут прекращены в случае, если операция будет успешно выполнена, ИЛИ после указанного максимального числа попыток.

Например, если место сохранения резервной копии в сети станет недоступным, программа будет выполнять попытки подключения каждые 30 секунд, но не более 30 раз. Попытки будут прекращены, когда подключение будет восстановлено ИЛИ число попыток достигнет указанного максимума.

В этом случае фактическое количество попыток не ограничено, а время ожидания до возврата ошибки о сбое резервного копирования рассчитывается по следующей формуле: (300 секунд + **Интервал между попытками**) * (**Количество попыток** + 1).

Примеры:

- Со значениями по умолчанию для сбоя резервного копирования должно пройти (300 секунд + 30 секунд) * (300 + 1) = 99330 секунд, или ~27,6 часов.
- Если параметру **Количество попыток** задано значение 1, а параметру **Интервал между попытками** — значение 1, сбой резервного копирования должен произойти через (300 секунд + 1 секунда) * (1 + 1) = 602 секунды или ~10 минут.

Если рассчитанное время ожидания превышает 30 минут, а передача данных еще не началась, для фактического времени ожидания устанавливается время 30 минут.

Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)

Значение по умолчанию: **Включено**.

В режиме без вывода сообщений ситуации, требующие вмешательства пользователя, разрешаются автоматически (за исключением обработки поврежденных секторов, что задается отдельным параметром). Если операция не может быть продолжена без вмешательства пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

Пропуск поврежденных секторов

Значение по умолчанию: **Отключено**.

Если этот параметр отключен, каждый раз, когда встречается поврежденный сектор, действию резервного копирования будет назначено состояние **Требуется вмешательство пользователя**. Чтобы создать резервную копию данных с диска, который быстро выходит из строя, включите параметр пропуска поврежденных секторов. Резервное копирование неповрежденных данных будет выполнено, после чего можно подключить резервную копию диска и извлечь исправные файлы на другой диск.

Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины

Значение по умолчанию: **Включено. Количество попыток: 3. Интервал между попытками: 5 минут.**

Если не удастся создать моментальный снимок виртуальной машины, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены, как только операция будет успешно выполнена ИЛИ по достижении указанного максимального количества попыток (в зависимости от того, что наступит раньше).

Быстрое инкрементное/дифференциальное резервное копирование

Этот параметр работает для инкрементных и дифференциальных резервных копий на уровне дисков.

Этот параметр не работает (всегда отключен) для томов с файловыми системами JFS, ReiserFS3, ReiserFS4, ReFS или XFS.

Значение по умолчанию: **Включено**.

Инкрементная или дифференциальная резервная копия содержит только изменения данных. Чтобы ускорить процесс резервного копирования, программа определяет, есть ли изменения в файле по размеру, дате и времени последнего изменения файла. Если эта функция отключена, то программа будет сравнивать все содержимое файла с тем содержимым, которое сохранено в резервной копии.

Фильтры файлов

Фильтры позволяют включить в резервную копию или исключить из нее только определенные файлы и папки.

Фильтры файлов доступны как для резервных копий на уровне файлов, так и для резервных копий на уровне дисков, если не указано иначе.

Фильтры файлов не работают для динамических дисков (томов LVM или LDM) или виртуальной машины, резервная копия которой создана агентом для VMware или агентом для Hyper-V в режиме без использования агента.

Включение фильтров файлов

1. В плане защиты разверните модуль **Резервное копирование**.
2. В разделе **Параметры резервного копирования** щёлкните **Изменить**.
3. Выберите **Фильтры файлов**.
4. Воспользуйтесь любыми из перечисленных ниже вариантов.

Включение или исключение файлов, соответствующих определенным критериям

Есть два параметра с противоположными принципами действия.

- **Создавать резервные копии файлов, соответствующих следующим критериям**

  Пример: Если выбрать резервное копирование всей машины и указать в качестве условия фильтрации **C:\File.exe**, будет создана резервная копия только этого файла.

- **Не создавать резервные копии файлов, соответствующих следующим критериям**

Пример: Если выбрать резервное копирование всей машины и указать в качестве условия фильтрации **C:\File.exe**, будет пропущен только этот файл.

Оба параметра можно использовать одновременно. При этом второй имеет приоритет над первым (т. е. если указать **C:\File.exe** в обоих полях, этот файл будет пропущен при резервном копировании).

Условия

- **Полный путь**

  Укажите полный путь к файлу или папке, начиная с буквы диска (при резервном копировании ОС Windows) или с корневого каталога (при резервном копировании Linux).

  Как в Windows, так и в Linux, в пути к файлу или папке можно использовать косую черту (например, **C:/Temp/File.tmp**). В Windows также можно использовать традиционную обратную косую черту (например, **C:\Temp\File.tmp**).

  > **Важно**
  >
  > Если операционная система машины, для которой создается резервная копия, определена неправильно при резервном копировании на уровне дисков, фильтры полного пути к файлу не будут работать. Для фильтра исключения будет показано предупреждение. Если есть фильтр включения, резервное копирование завершится сбоем.
  >
  > Фильтр полного пути включает в себя букву диска (в ОС Windows) или корневой каталог (в ОС Linux). Пример полного пути к файлу: **C:\Temp\File.tmp**. Фильтр, который включает в себя букву диска или корневой каталог, например **C:\Temp\File.tmp** или **C:\Temp***, вызовет предупреждение или сбой.
  >
  > Фильтр, в котором не используется буква диска или корневой каталог (например, **Temp*** или **Temp\File.tmp**), или фильтр, который начинается со звездочки (например, ***C:**), не приводит к возврату предупреждения или сбою. Если операционная система машины, для которой создана резервная копия, определена неправильно, фильтры обоих типов не будут работать.

- **Имя**

  Укажите имя файла или папки, например **Document.txt**. Будут выбраны все файлы и папки с этим названием.

В условиях *не* учитывается регистр символов. Например, путь **C:\Temp** включает варианты **C:\TEMP**, **C:\temp** и т. п.

В условии можно использовать любое количество подстановочных символов (*, ** и ?). Эти символы можно использовать как в полном пути, так и в имени файла или папки.

Звездочка (*) замещает 0 или несколько символов имени файла. Например, условие **Doc*.txt** включает в себя файлы `Doc.txt` и **Document.txt**

[Только резервные копии в формате **версия 12**] Две звездочки (*) замещают 0 или несколько символов в имени или пути файла, включая символ косой черты. Например, критерий ****/Docs/**.txt** соответствует всем TXT-файлам во всех подпапках всех папок **Docs**.

Вопросительный знак (?) замещает в имени файла ровно один символ. Например, условие **Doc?.txt** включает в себя файлы `Doc1.txt` и **Docs.txt**, но не включает файлы `Doc.txt` и **Doc11.txt**

Исключить скрытые файлы и папки

Этот параметр действует только в файловых системах, совместимых с Windows. Установите этот флажок, чтобы пропускать файлы и папки с атрибутом **Скрытый**. Если скрыта папка, будет исключено все ее содержимое, включая файлы без атрибута **Скрытый**.

Исключить системные файлы и папки

Этот параметр действует только в файловых системах, совместимых с Windows. Установите этот флажок, чтобы пропустить файлы и папки с атрибутом **Системный**. Если данный атрибут назначен папке, будет исключено все ее содержимое, включая файлы без атрибута **Системный**.

Примечание

Просматривать атрибуты файлов и папок можно в их свойствах или с помощью команды `attrib`. Дополнительные сведения можно получить в центре справки и поддержки Windows.

Моментальные снимки резервных копий на уровне файлов

Этот параметр действует только для резервной копии на уровне файлов.

Этот параметр определяет, выполнять последовательное резервное копирование файлов или делать моментальный снимок данных.

Примечание

Файлы, которые хранятся в сетевых папках, при создании резервной копии всегда копируются по одному.

Значение по умолчанию:

- Если для резервного копирования выбраны только машины с ОС Linux: **Не создавать**

моментальный снимок.

- В противном случае: **По возможности создавать моментальный снимок.**

Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

- **По возможности создавать моментальный снимок**

  Прямое резервное копирование файлов, если создание моментального снимка невозможно.

- **Всегда создавать моментальный снимок**

  Моментальный снимок позволяет выполнять резервное копирование всех файлов, включая те, которые открыты с монопольным доступом. Все файлы в резервной копии будут сохранены в состоянии на данный момент времени. Выберите эту настройку только в случае, если эти факторы имеют важное значение, т. е. резервное копирование файлов без создания моментального снимка лишено смысла. Если моментальный снимок не может быть сделан, резервное копирование завершится ошибкой.

- **Не создавать моментальный снимок**

  Всегда выполнять прямое резервное копирование файлов. Попытка резервного копирования файлов, открытых с монопольным доступом, приведет к ошибке чтения. Файлы в резервной копии могут быть не синхронизированы по времени.

Сокращение журнала Microsoft SQL Server

Этот параметр применим для резервного копирования баз данных Microsoft SQL Server и резервного копирования на уровне дисков с включенным резервным копированием приложения Microsoft SQL Server.

Этот параметр определяет, будут ли сокращаться журналы транзакций SQL Server после успешного резервного копирования.

Значение по умолчанию: **Включено**.

Если этот параметр включен, базу данных можно восстановить только по состоянию на момент создания резервной копии этим программным обеспечением. Отключите этот параметр, если вы создаёте резервные копии журналов транзакции встроенным модулем резервного копирования Microsoft SQL Server. Можно будет применить журналы транзакций после восстановления и таким образом восстановить базу данных в состояние на любой момент времени (Point-in-Time Recovery, PITR).

Убедитесь, что резервные копии журналов транзакций регулярно создаются модулем резервного копирования Microsoft SQL Server и переполнения диска не происходит.

Создание моментальных снимков LVM

Этот параметр действует только для физических машин.

Этот параметр действует только для резервного копирования томов на уровне дисков, управляемых диспетчером логических томов Linux (LVM). Такие тома также называются логическими томами.

Этот параметр определяет способ создания моментального снимка логического тома. Программа резервного копирования может выполнить это самостоятельно или воспользоваться для этого диспетчером логических томов Linux (LVM).

Значение по умолчанию: **С помощью программы для резервного копирования**.

- **С помощью программы для резервного копирования**. Данные моментального снимка хранятся в основном в ОЗУ. Так резервное копирование выполняется быстрее, а в группе томов не требуется нераспределенное пространство. Поэтому рекомендуется изменять заранее заданное значение только при возникновении неполадок с резервным копированием логических томов.
- **С помощью LVM**. Моментальный снимок сохраняется в нераспределеном пространстве группы тома. При отсутствии нераспределенного пространства моментальный снимок будет создан программой резервного копирования.

Моментальный снимок используется только при выполнении операции резервного копирования и автоматически удаляется после её окончания. Временные файлы не сохраняются.

Точки подключения

Этот параметр действует только в Windows для резервной копии на уровне файлов любого источника данных, который включает в себя подключенные тома или общие тома кластера.

Этот параметр работает только в случае, если для резервного копирования выбрана папка, которая в иерархии папок находится выше точки подключения. (Точка подключения — это папка, к которой логически подключен дополнительный том.)

- Если такая папка (родительская папка) выбрана для резервного копирования, и включен параметр **Точки подключения**, все файлы на подключенном томе будут включены в резервную копию. Если параметр **Точки подключения** отключен, точка подключения в резервной копии будет пуста.

  При восстановлении родительской папки содержимое точки подключения восстанавливается, когда для восстановления включен параметр *Точки подключения*.

- Если выбрана сама точка подключения или любая папка в подключенном томе, выбранные папки рассматриваются как обыкновенные. Их резервное копирование будет выполняться независимо от состояния параметра **Точки подключения**, а восстановление — независимо от **Точки подключения для восстановления** (см. *Точки подключения*).

Значение по умолчанию: **Отключено**.

> **Примечание**
>
> Можно создавать резервные копии виртуальных машин Hyper-V, расположенных на общем томе кластера, путем резервного копирования нужных файлов или всего тома на уровне файлов. Просто отключите виртуальные машины, чтобы их резервное копирование выполнялось согласованно.

Пример

Предположим, что папка `C:\Data1\` является точкой подключения для подключенного тома. Этот том содержит папки `Folder1` и `Folder2`. Вы создаете план защиты для резервной копии ваших данных на уровне файлов.

Если установить флажок для тома C и включить параметр **Точки подключения**, в папке `C:\Data1\` в резервной копии будут находиться `Folder1` и `Folder2`. При восстановлении данных с резервной копии помните о правильном использовании параметра **Точки подключения для восстановления** (см. *Точки подключения*).

Если установить флажок для тома C и отключить параметр **Точки подключения**, папка `C:\Data1\` в резервной копии будет пустой.

Если установить флажок для **Data1**, папки `Folder1` или `Folder2`, отмеченные папки будут включены в копию как обыкновенные папки независимо от параметра **Точки подключения**.

Многотомные моментальные снимки

Этот параметр применим для резервных копий физических и виртуальных машин, работающих под управлением Windows или Linux, с установленным в этих ОС агентом.

Этот параметр применяется к резервному копированию дисков. Также этот параметр применим к резервному копированию файлов, если оно выполняется посредством создания моментального снимка. (Параметр *Моментальный снимок файлов* указывает, будет ли создан моментальный снимок при резервном копировании на уровне файлов).

Этот параметр определяет, создаются моментальные снимки нескольких томов одновременно или последовательно.

Значение по умолчанию:

- Если хотя бы одна машина под управлением Windows выбрана для резервного копирования: **Включено**.
- Если не выбрано ни одной машины (например, в начале создания плана защиты на странице

Планы → Резервная копия): **Включено**.

- В противном случае: **Отключено**.

Если этот параметр включен, то моментальные снимки всех томов, для которых выполняется резервное копирование, создаются одновременно. Используйте этот параметр для создания синхронизированных по времени резервных копий данных, расположенных на нескольких томах, например в базе данных Oracle.

Если этот параметр отключен, то моментальные снимки томов будут созданы последовательно. В результате, если данные расположены на нескольких томах, результирующие резервные копии могут быть не синхронизированы по времени.

Производительность и окно резервного копирования

Позволяет задавать один из трех уровней производительности резервного копирования (высокий, низкий, запрещено) для каждого часа недели. Таким образом можно определить окно времени, в течение которого разрешено запускать и выполнять процессы резервного копирования. Высокий и низкий уровни производительности настраиваются в плане приоритета процесса и скорости вывода.

Этот параметр можно настроить отдельно для каждого хранилища, указанного в плане защиты. Чтобы настроить этот параметр для хранилища репликации, щёлкните значок шестерни рядом с именем хранилища и щёлкните **Производительность и окно резервного копирования**.

Этот параметр действует только для резервного копирования и репликации резервной копии. Команды после резервного копирования и другие операции, входящие в план защиты (проверка, преобразование в виртуальную машину), запускаются независимо от значения этого параметра.

Значение по умолчанию: **Отключено**.

Если этот параметр отключен, процессы резервного копирования разрешено запускать в любое время с указанными ниже параметрами (при этом не имеет значения, было ли изменено предустановленное значение параметра):

- Приоритет ЦП: **Низкий** (соответствует значению **Ниже среднего**).
- Скорость вывода: **Без ограничений**.

Если этот параметр включен, запланированные резервные копии разрешаются или блокируются согласно параметрам, указанным для текущего часа. В начале часа блокировки резервного копирования процесс резервного копирования автоматически останавливается; появляется соответствующее оповещение.

Даже если запланированные резервные копии заблокированы, резервное копирование можно запустить вручную. Для него будут использоваться параметры производительности последнего часа, когда

процессы резервного копирования были разрешены.

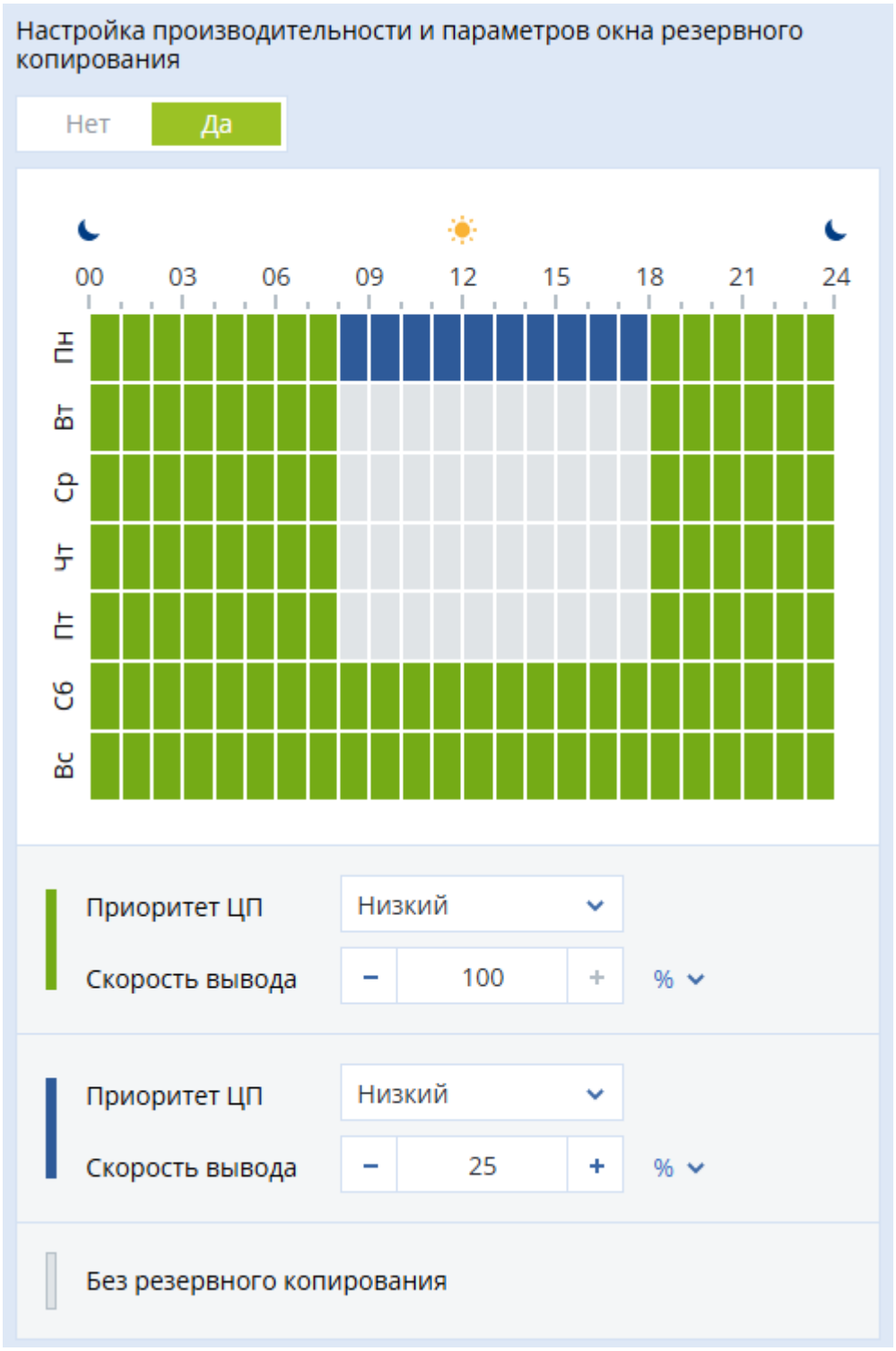
Окно резервного копирования

Каждый прямоугольник представляет один час в пределах дня. По щелчку прямоугольника можно поочередно переходить между указанными состояниями:

- **Зеленый:** резервное копирование разрешено с параметрами, указанными в зеленом разделе ниже.
- **Синий:** резервное копирование разрешено с параметрами, указанными в синем разделе ниже.

  Это состояние недоступно, если для формата резервной копии задано значение **Версия 11**.
- **Серый:** резервное копирование заблокировано.

Чтобы одновременно изменить состояние нескольких прямоугольников, щёлкните один из них и расширьте выделение путем перетаскивания.



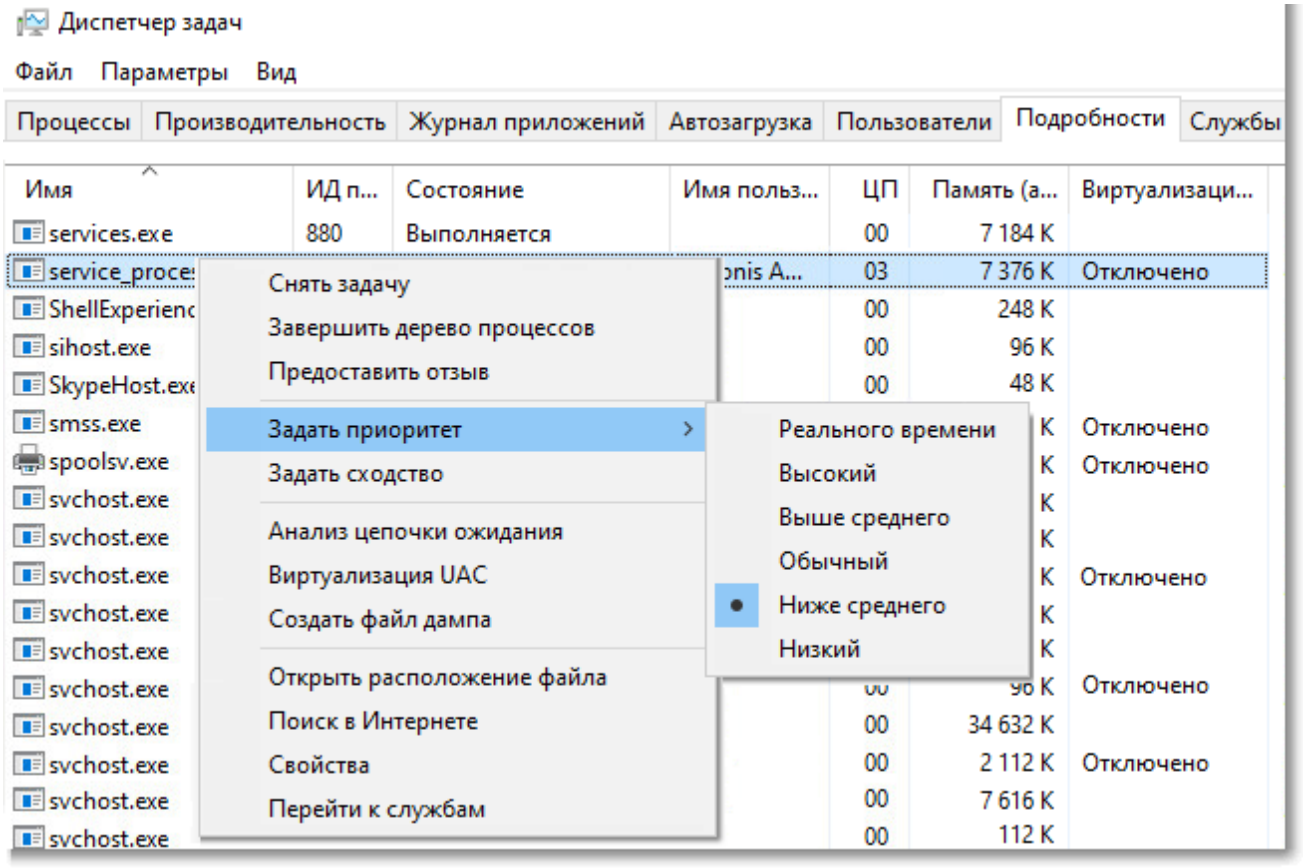
Приоритет ЦП

Этот параметр задает приоритет процесса резервного копирования (`service_process.exe`) в операционной системе Windows.

Доступные значения:

- **Низкий**: соответствует значению **Ниже среднего**.
- **Обычный**: соответствует значению **Обычный**.
- **Высокий**: соответствует значению **Высокий**.

Приоритет процесса, выполняющегося в системе, определяет количество выделенных ему ресурсов ЦП и системы. Понижение приоритета резервного копирования освободит часть ресурсов для других приложений. Повышение приоритета копирования ускорит процесс создания резервных копий за счет того, что операционная система выделит программе резервного копирования больше ресурсов, например ресурсов ЦП. Однако результат будет зависеть от общего использования процессора и других факторов, например от скорости ввода-вывода диска и загруженности сети.



Скорость вывода при резервном копировании

Этот параметр позволяет ограничить скорость записи на жесткий диск (при выполнении резервного копирования в локальную папку) или скорость передачи данных резервной копии по сети (при резервном копировании в сетевую папку).

Если этот параметр включен, можно указать максимально разрешенную скорость вывода:

- В процентах от оценочной скорости записи на целевом жестком диске (при резервном копировании в локальную папку) или оценочной максимальной скорости сетевого подключения

(при резервном копировании сетевой папки).

Эта настройка работает только для Windows-агентов.

- В КБ/секунду (для всех мест сохранения).

  Эта настройка работает для Windows- и Linux-агентов.

Примечание

Если одновременно запущено несколько процессов резервного копирования, итоговая скорость вывода определяется как сумма скоростей вывода этих процессов.

Команды до и после процедуры

Этот параметр позволяет определить команды, которые должны выполняться автоматически перед выполнением процедуры резервного копирования или после нее.

Примеры использования команд до и после процедуры:

- Удаление некоторых временных файлов с диска до начала резервного копирования.
- Настройка антивирусной программы стороннего производителя для запуска до начала резервного копирования.
- Выборочное копирование резервных копий в другое хранилище. Этот параметр может быть полезен, поскольку операция репликации, заданная в плане защиты, копирует каждую резервную копию архива в указанные хранилища.

Агент выполняет репликацию после выполнения команды после резервного копирования.

Кибер Бэкап не поддерживает интерактивные команды, то есть команды, которые требуют пользовательского ввода (например, pause).

Команда до резервного копирования

Чтобы указать команду или пакетный файл, которые будут выполнены перед началом резервного копирования:

1. Включите переключатель **Выполнение команды до резервного копирования**.
2. В поле **Команда…** введите команду или укажите путь к пакетному файлу на машине с агентом. Кибер Бэкап не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).

Примечание

Если в плане указана интерактивная команда, то такой план после запуска может навсегда остаться в состоянии ”Выполняется”, а его выполнение нельзя будет остановить через веб-интефейс Кибер Бэкап. Чтобы остановить выполнение плана в такой ситуации, на каждой целевой машине плана необходимо принудительно завершить процесс этой команды (см. дочерние процессы процесса агента Кибер Бэкап) и перезапустить агент.

3. В поле **Рабочий каталог** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Не запускать план, если не удается выполнить команду[1]	Установить	Снять	Установить	Снять
Выполнить план по окончании выполнения команды	Установить	Установить	Снять	Снять
Результат				
	[По умолчанию] Выполнить резервное копирование только после успешного выполнения команды. Прерывать резервное копирование при сбое команды.	Выполнить резервное копирование после команды независимо от результатов ее выполнения (успешно или ошибка).	—	Выполнить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

[1] Команда считается сбойной, если код завершения не равен нулю. При сбое команды план не перезапускается даже при включенном параметре *Действия при сбое задания*.

Команда после резервного копирования

Чтобы указать команду или исполняемый файл, которые будут выполнены после завершения резервного копирования:

1. Включите переключатель **Выполнение команды после резервного копирования**.
2. В поле **Команда…** введите команду или укажите путь к пакетному файлу на машине с агентом.
3. В поле **Рабочий каталог** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
5. Установите флажок **Прерывать резервное копирование при сбое команды**, если для вас важно успешное выполнение команды. Считается, что команда не выполнена, если код выхода не равен нулю. При сбое выполнения команды состоянию резервной копии будет задано значение **Ошибка**.

   Если флажок не установлен, результат выполнения команды не влияет на успешность выполнения резервного копирования. Можно отследить результат выполнения команды, изучив информацию на вкладке **Действия**.
6. Нажмите кнопку **Готово**.

Команды до и после захвата данных

Этот параметр позволяет задать команды, которые должны выполняться автоматически до и после захвата данных (т. е. создание моментального снимка данных). Захват данных выполняется в начале процедуры резервного копирования.

Следующая схема иллюстрирует порядок выполнения команд до и после захвата данных.

```
           <------------- резервное копирование ------------->
команды до       команды до      захват      команды            команды после
резервного   ->  захвата     ->  данных  ->  после захвата  ->  резервного
копирования      данных                      данных             копирования
```

Если включен параметр *Служба теневого копирования томов (VSS)*, то последовательность выполнения команд и операций Microsoft VSS будет следующей:

```
команды до      приостановка      захват      возобновление      команды после
захвата     ->  VSS           ->  данных  ->  VSS            ->  захвата
данных                                                           данных
```

Использование команд до и после захвата данных предоставляет возможность приостановки и

возобновления базы данных или приложения, которые несовместимы с VSS. Поскольку захват данных выполняется за считанные секунды, время простоя базы данных или приложения сводится к минимуму.

Команды после захвата данных работают только в случае, если включен параметр ”Многотомные моментальные снимки” (см. раздел *Многотомные моментальные снимки*).

Команда до захвата данных

Чтобы указать команду или пакетный файл, которые будут выполнены до захвата данных:

1. Включите переключатель **Выполнение команды до захвата данных**.
2. В поле **Команда…** введите команду или найдите пакетный файл. Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).

   > **Примечание**
   >
   > Если в плане указана интерактивная команда, то такой план после запуска может навсегда остаться в состоянии ”Выполняется”, а его выполнение нельзя будет остановить через веб-интефейс Кибер Бэкап. Чтобы остановить выполнение плана в такой ситуации, на каждой целевой машине плана необходимо принудительно завершить процесс этой команды (см. дочерние процессы процесса агента Кибер Бэкап) и перезапустить агент.

3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Прерывать резервное копирование при сбое команды[1]	Установить	Снять	Установить	Снять

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Флажок	Выбор			
Не выполнять захват данных до полного выполнения команды	Установить	Установить	Снять	Снять
Результат				
	[По умолчанию] Выполнить захват данных только после успешного выполнения команды. Прерывать резервное копирование при сбое команды.	Выполнить захват данных после команды независимо от результатов ее выполнения (успешно или ошибка).	—	Выполнить захват данных одновременно с выполнением команды и независимо от результатов выполнения команды.

Команда после захвата данных

Чтобы указать команду или пакетный файл, которые будут выполнены после захвата данных:

1. Включите переключатель **Выполнение команды после захвата данных**.
2. В поле **Команда…** введите команду или найдите пакетный файл. Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).
3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

[1] Команда считается сбойной, если код завершения не равен нулю.

Флажок	Выбор			
Прерывать резервное копирование при сбое команды[1]	Установить	Снять	Установить	Снять
Не продолжать создание резервной копии до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	[По умолчанию] Продолжить резервное копирование только после успешного выполнения команды.	Продолжить резервное копирование после команды независимо от результатов ее выполнения (успешно или ошибка).	—	Продолжить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

Моментальные снимки оборудования SAN

Этот параметр эффективен для резервного копирования виртуальных машин VMware ESXi и oVirt.

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли использоваться технология моментальных снимков SAN при выполнении резервного копирования.

Если параметр отключен, содержимое виртуального диска будет прочитано с моментального снимка VMware/oVirt. Моментальный снимок хранится все время резервного копирования.

Если этот параметр включен, содержимое виртуального диска будет прочитано с моментального снимка SAN. Моментальный снимок будет создан и сохранен на небольшое время, чтобы привести виртуальные диски в согласованное состояние. Если чтение с моментального снимка SAN невозможно, резервное копирование завершится с ошибкой.

Перед включением параметра проверьте и выполните все требования, указанные в разделе *Использование моментальных снимков оборудования SAN*.

[1] Команда считается сбойной, если код завершения не равен нулю.

Планирование

Этот параметр определяет, запускаются ли процессы резервного копирования по расписанию или с задержкой, а также количество виртуальных машин, для которых резервное копирование выполняется одновременно.

Можно выбрать один из следующих вариантов:

- **Начинать все операции резервного копирования строго по расписанию**

  Резервное копирование физических машин запустится точно в соответствии с расписанием. Резервные копии виртуальных машин будут создаваться поочередно.

- **Распределять время запуска по доступному времени**

  Резервные копии физических машин будут запущены с задержкой от запланированного времени. Значение задержки для каждой машины выбирается случайно и находится в диапазоне от нуля до максимального значения, которое вы укажете. Параметр может быть полезен для резервного копирования нескольких машин в сетевое хранилище, чтобы избежать чрезмерной загрузки сети. Продолжительность задержки для каждой машины определяется при применении плана защиты к машине и остается неизменной до тех пор, пока в плане защиты не будет изменено максимальное значение задержки.

  Резервные копии виртуальных машин будут создаваться поочередно.

- **Ограничить число одновременно выполняющихся операций резервного копирования на уровне**

  Этот параметр доступен только в том случае, если план защиты применен к нескольким виртуальным машинам. Этот параметр определяет количество виртуальных машин, для которых агент может одновременно создавать резервные копии при выполнении данного плана защиты.

  Если в соответствии с планом защиты агенту необходимо начать резервное копирование нескольких машин сразу, он выберет две машины. (Чтобы оптимизировать производительность резервного копирования, агент пытается подобрать машины, хранящиеся в различных хранилищах.) После завершения создания любой из первых двух резервных копий агент выберет третью машину и т. д.

  Количество виртуальных машин, для которых агент будет создавать резервные копии одновременно, можно изменить. Максимальное значение равно 10. Однако если агент выполняет несколько планов защиты, которые пересекаются по времени, указанные в их параметрах числа суммируются. Вы можете *ограничить общее количество виртуальных машин*, для которых агент может одновременно создавать резервные копии, вне зависимости от количества выполняемых планов резервного копирования.

Посекторное резервное копирование

Этот параметр действует только при резервном копировании на уровне дисков.

Этот параметр определяет, создавать ли точную копию диска или тома на физическом уровне.

Значение по умолчанию: **Отключено**.

Если этот параметр включен, создается резервная копия всех секторов диска или тома, включая нераспределенное пространство и те сектора, в которых нет данных. Размер полученной в результате резервной копии будет равен размеру диска, для которого создается резервная копия (если параметру *Уровень сжатия* задано значение **Отсутствует**). Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами.

Примечание

Невозможно будет восстановить данные приложения из резервных копий, созданных в посекторном режиме.

Деление

Этот параметр применим для следующих схем резервного копирования:

- Всегда инкрементное;
- Всегда полное;
- Еженедельно полное, ежедневно инкрементное;
- Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS);
- Другое.

Этот параметр позволяет выбрать метод разделения резервных копий на фрагменты.

Примечание

Параметр не используется для Кибер Инфраструктуры и Кибер Хранилища.

Значение по умолчанию: **Автоматически**.

Доступны следующие настройки:

- **Автоматически**

Резервная копия будет разделена на части, если:

- размер копии превышает максимальный размер файла, который поддерживается в выбранном хранилище;
- копия не помещается на остаток текущей ленты.

> **Примечание**
>
> В том случае, когда в хранилище используется файловая система NTFS и агент для Windows, резервная копия будет разделена на части, если её размер превышает 200 ГБ.

- **Постоянный размер**

  Введите или выберите из предлагаемых вариантов нужный размер файла.

При применении плана репликации к резервной копии (см. раздел *Репликация резервной копии*), разделённой на фиксированные фрагменты, реплицированная копия объединяется в общий архив.

> **Примечание**
>
> При редактировании плана новое значение параметра применяется только после удаления всех резервных копий, сделанных со старым значением.

Известные проблемы и ограничения

Автоматическое разделение резервной копии на файлы при копировании в *сетевую папку InfoDiode* имеет ограничение: не более 1000 файлов в рамках одного плана. Если в процессе работы количество файлов превысит этот лимит, выполнение плана будет прервано с ошибкой (это является штатным ограничением).

Чтобы избежать сбоя, при настройке резервного копирования больших объёмов данных выбирайте больший размер для каждого отдельного файла.

Управление лентами

Эти параметры применимы только при резервном копировании на ленточное устройство.

Включить восстановление файлов из образов дисков на лентах

Значение по умолчанию: **Отключено**.

Если этот флажок установлен, при каждом резервном копировании программа создает дополнительные файлы на жестком диске машины, к которой подсоединено ленточное устройство. Восстановление файлов из резервных копий дисков возможно до тех пор, пока эти дополнительные файлы будут в порядке. Файлы автоматически удаляются при *стирании*, *удалении* или перезаписи ленты с соответствующими резервными копиями.

Дополнительные файлы располагаются в следующих местах:

- В ОС Windows: `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`.
- В ОС Linux: `/var/lib/Acronis/BackupAndRecovery/TapeLocation`.

Пространство, занимаемое этими дополнительными файлами, зависит от количества файлов в соответствующей резервной копии. Для полной резервной копии диска, содержащей примерно 20 000 файлов (обычная резервная копия диска рабочей станции), дополнительные файлы занимают около 150 МБ. Полная резервная копия сервера, содержащая 250 000 файлов, может создать около 700 МБ дополнительных файлов. Поэтому, если вы уверены, что восстановление отдельных файлов не потребуется, можно не устанавливать этот флажок для экономии дискового пространства.

Если дополнительные файлы не были созданы в процессе резервного копирования или были удалены, их все равно можно создать, *повторно просканировав* ленты, на которых хранится резервная копия.

> **Примечание**
>
> Восстановление дополнительных файлов недоступно, если размер архива резервной копии менее 500 КБ.

Вернуть ленту в слот после каждого успешного создания резервной копии каждой машины

Значение по умолчанию: **Включено**.

Если этот параметр отключен, лента будет оставаться в приводе после завершения операции, в которой используется лента. В ином случае программное обеспечение вернет ленту в слот, в котором она находилась до операции. Если, согласно плану защиты, за созданием резервной копии следуют другие операции (например, ее проверка или репликация в другое хранилище), лента будет возвращена в слот после завершения этих операций.

Если включен этот параметр, а также параметр **Извлечь ленты после успешного резервного копирования каждой машины**, лента будет извлечена.

Извлечь ленты после каждого успешного резервного копирования каждой машины

Значение по умолчанию: **Отключено**.

Если установлен этот флажок, программа будет извлекать ленты после любого успешного резервного копирования каждой машины. Если, согласно плану защиты, за созданием резервной копии следуют другие операции (например, ее проверка или репликация в другое хранилище), ленты будут извлечены после завершения этих операций.

Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии

Значение по умолчанию: **Отключено**.

Параметр применяется только к изолированным ленточным устройствам. Если этот параметр включен, лента, вставленная в устройство, будет перезаписываться каждый раз при создании полной резервной копии.

Используйте следующие ленточные устройства и приводы

Этот параметр позволяет указать ленточные устройства и приводы лент, используемые данным планом защиты.

Пул лент включает в себя ленты со всех ленточных устройств, подключенных к машине, будь то узел хранения или машина, на которой установлен агент защиты, или обе эти машины. Если в качестве хранилища резервных копий выбран пул лент, это означает, что косвенно выбрана и машина, к которой подключены ленточные устройства. По умолчанию резервные копии можно записать на ленты в любом приводе лент на любом ленточном устройстве, подключенном к этой машине. Если некоторые устройства или приводы отсутствуют или не работают должным образом, план защиты будет использовать доступные устройства и приводы.

Можно щёлкнуть **Только выбранные устройства и приводы** и выбрать ленточные устройства и приводы в списке. При выборе всего устройства выбираются все его приводы. Это означает, что любой из этих приводов может использоваться планом защиты. Если выбранное устройство или привод отсутствуют или не работают должным образом, а никаких других устройств не выбрано, резервное копирование завершится сбоем.

Этот параметр позволяет управлять процессами резервного копирования, которые выполняются несколькими агентами, в большую библиотеку ленточных носителей с несколькими приводами. Например, резервное копирование большого файлового сервера или большой общей папки может не запуститься, если несколько агентов выполняют резервное копирование машин в одном окне резервного копирования, поскольку агенты могут занимать все приводы. Если разрешить агентам использовать, например, приводы 2 и 3, привод 1 будет зарезервирован для агента, который выполняет резервное копирование общей папки.

С несколькими потоками

Значение по умолчанию: **Отключено**.

Использование нескольких потоков позволяет распределить данные с одного агента на несколько потоков, а затем одновременно записать эти потоки на разные ленточные носители. Это позволяет создавать резервные копии быстрее и особенно полезно в тех случаях, когда производительность агента выше производительности ленточного устройства.

Флажок **С несколькими потоками** доступен только в том случае, если в параметре **Только выбранные устройства и приводы** выбрано несколько ленточных устройств. Количество выбранных ленточных устройств равно количеству одновременных потоков от агента. Если при запуске резервного копирования какое-либо из этих устройств будет недоступно, резервное копирование завершится сбоем.

Для восстановления с многопотоковой резервной копии или с многопотоковой и мультиплексированной резервной копии понадобится как минимум такое же количество приводов, которое было использовано при создании этой резервной копии.

Невозможно изменить настройки многопоточности в существующем плане защиты. Чтобы использовать другие настройки или изменить выбранные ленточные устройства, создайте новый план защиты.

Многопоточность доступна как для локально подключенных ленточных устройств, так и ленточных устройств, подключенных к узлу хранения.

Мультиплексирование

Значение по умолчанию: **Отключено**.

Мультиплексирование позволяет записывать потоки данных с нескольких агентов на один ленточный носитель. Это способствует улучшению использования быстрых ленточных устройств. По умолчанию коэффициент мультиплексирования (количество агентов, которые отправляют данные на один ленточный носитель) равен 2. Его можно увеличить до 10.

Мультиплексирование полезно для больших сред, в которых выполняется множество операций резервного копирования. Оно не повысит производительность единичных процессов резервного копирования.

Чтобы получить максимально возможную быстроту резервного копирования в большой среде, необходимо проанализировать производительность агентов, сети и ленточных устройств. После этого необходимо задать соответствующий коэффициент мультиплексирования. При этом следует избежать чрезмерного мультиплексирования. Например, если агенты передают данные со скоростью 70 Мбит/с, а скорость записи на ленточное устройство составляет 250 Мбит/с, то при отсутствии проблем (задержек) в сети установите для коэффициента мультиплексирования значение 3. Если для коэффициента мультиплексирования задать значение 4, это приведет к излишнему мильтиплексированию и снижению

производительности резервного копирования. Как правило, значение коэффициента мультиплексирования задается в диапазоне от 2 до 5.

Резервные копии, созданные с использованием мультиплексирования, восстанавливаются медленнее. Это обусловлено их структурой. Чем выше коэффициент мультиплексирования, тем медленнее будет восстановление. Одновременное восстановление нескольких резервных копий, записанных на одну мультиплексированную ленту, не поддерживается.

Можно выбрать одно или несколько ленточных устройств для мультиплексирования или использовать мультиплексирование с любым доступным ленточным устройством. Мультиплексирование недоступно для ленточных устройств, подключенных локально.

Невозможно изменить настройки мультиплексирования в существующем плане защиты. Чтобы использовать другие настройки, создайте новый план защиты.

В плане защиты можно использовать следующие комбинации многопоточности и мультиплексирования:

- **Настройки многопоточности и мультиплексирования отключены.**

  Каждый агент отправляет данные на одно ленточное устройство.

- **Выбрана только многопоточность.**

  Каждый агент одновременно отправляет данные как минимум на два ленточных устройства.

- **Выбрано только мультиплексирование.**

  Каждый агент отправляет данные на ленточное устройство, которое одновременно принимает потоки от нескольких агентов. Максимальное количество потоков, которые может принять ленточное устройство, задается в плане защиты. Его невозможно изменить ”на ходу”.

- **Настройки многопоточности и мультиплексирования выбраны.**

  Каждый агент отправляет данные как минимум на два ленточных устройства, которые одновременно принимают потоки от нескольких агентов.

Ленточное устройство единовременно может записывать только один тип резервной копии (с мультиплексированием или без мультиплексирования) в зависимости от того, какой план защиты запущен первым.

Использовать наборы лент в пуле лент, выбранных для резервного копирования

Значение по умолчанию: **Отключено**.

Ленты внутри одного пула можно объединить в так называемые **наборы лент**.

Если оставить этот параметр отключенным, резервное копирование данных будет выполнено на все ленты, принадлежащие пулу. Если включить этот параметр, можно разделить резервные копии в

соответствии с предварительно определенными или пользовательскими правилами.

- **Используйте отдельный набор лент для каждого** (выберите правило: **Тип резервной копии**, **Тип устройства**, **Имя устройства**, **День месяца**, **День недели**, **Месяц**, **Год**, **Дата**).

  При выборе этого варианта возможна организация наборов лент в соответствии с предопределенным правилом. Например, можно указать отдельные наборы лент для каждого дня недели или хранить резервные копии каждой машины на отдельном наборе лент.

  Правило **Имя устройства** не работает, если используется режим мультиплексирования.

  > **Примечание**
  >
  > Этот параметр рекомендуется включать при выборе схемы **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)** (см. *Расписание*). Рекомендуется выбрать шаблон **День недели**.
  >
  > В таком случае для каждого дня недели будет использоваться отдельная лента. Резервные копии, созданные в понедельник, будут храниться на одной ленте. Резервные копии, созданные во вторник, будут храниться на другой ленте. И так далее.

- **Укажите настраиваемое правило для наборов лент.**

  При выборе этого варианта возможно указание собственного правила для организации наборов лент. Правило может содержать следующие переменные:

Синтаксис переменной	Описание переменной	Доступные значения
`[Имя устройства]`	Резервные копии на каждой машине будут храниться на отдельном наборе лент.	Имена машин, зарегистрированных на сервере управления.
`[Тип резервной копии]`	Полные, инкрементные и дифференциальные резервные копии будут храниться на отдельных наборах лент.	`full`, `inc`, `diff`

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Синтаксис переменной	Описание переменной	Доступные значения
`[Тип устройства]`	Резервные копии каждого типа машин будут храниться на отдельном наборе лент.	`Экземпляры сервера`, `сервер`, `рабочая станция`, `физическая машина`, `виртуальная машина VMware`, `виртуальная машина Virtual-PC`, `виртуальная машина виртуального сервера`, `виртуальная машина Hyper-V`, `виртуальная машина XEN`, `виртуальная машина KVM`, `виртуальная машина RHEV`.
`[День месяца]`	Резервные копии, созданные в каждый день месяца, будут храниться на отдельном наборе лент.	`01`, `02`, `03`, ..., `31`
`[День недели]`	Резервные копии, созданные в каждый день недели, будут храниться на отдельном наборе лент.	`Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`, `Sunday`
`[Месяц]`	Резервные копии, созданные в каждый месяц года, будут храниться на отдельном наборе лент.	`January`, `February`, `March`, `April`, `May`, `June`, `July`, `August`, `September`, `October`, `November`, `December`
`[Год]`	Резервные копии, созданные за год, будут храниться на отдельном наборе лент.	`2017`, `2018`, ...
`[Дата]`	Резервные копии, созданные в определённую дату, будут храниться на отдельном наборе лент.	Дата в формате `[Год].[Месяц].[День месяца]` Где: • `[Год]` — значение, доступное для переменной `[Год]`. • `[Месяц]` — значение, доступное для переменной `[Месяц]`. • `[День месяца]` — значение, доступное для переменной `[День месяца]`. Пример: `2025.December.18`

- Например, при указании правила `[Имя устройства]-[Тип резервной копии]` будет создан отдельный набор лент для каждой полной, инкрементной и дифференциальной резервной копии каждой машины, к которой применим план защиты.

Возможно *указать набор лент* для отдельных лент. В данном случае программное обеспечение сначала запишет резервные копии на ленты, значение набора лент которых совпадает со значением

выражения, указанного в плане защиты. После чего при необходимости будут взяты другие ленты этого пула. Если пул пополняемый, после этого будут использованы ленты из пула **Свободные ленты**.

Например, при указании набора лент `Monday` для ленты 1, `Tuesday` для ленты 2 и т. д. и указании `[День недели]` в параметрах резервного копирования надлежащая лента будет использована в соответствующий день недели.

Действие при сбое плана

Этот параметр определяет поведение программы при сбое запланированного плана защиты. Этот параметр не действует для планов с параметром *Команды до и после процедуры* или если план защиты запущен вручную.

Если этот параметр включен, то программа попытается еще раз выполнить план защиты. Можно задать временной интервал между попытками и количеством попыток. Попытки будут прекращены, когда задание будет выполнено успешно ИЛИ количество попыток достигнет указанного предела.

Значение по умолчанию: **Отключено**.

Условия запуска задания

Этот параметр применим в операционных системах Windows и Linux.

Этот параметр определяет поведение программы в момент, когда должно начаться выполнение задания (наступает запланированное время или событие, указанное в расписании), но не выполнено одно или несколько условий. Дополнительную информацию об условиях см. в разделе *Условия запуска*.

Значение по умолчанию: **Дождитесь, пока будут выполнены все условия в расписании.**

Ожидать выполнения условий расписания

С этой настройкой планировщик начинает отслеживать условия и запускает задание, как только условия выполняются. Если условия не выполняются, задание не запускается.

Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка задания становится рискованной, можно установить интервал времени, после которого задание запустится независимо от условия. Установите флажок **Запустить задание в любом случае через** и укажите интервал времени. Задание запустится, если будут выполнены условия или истечет максимальное время задержки.

Пропустить задание

Задержка выполнения задания может быть недопустима, например, если его необходимо выполнить точно в заданное время. В этом случае имеет смысл пропустить задание, а не ждать выполнения условий, особенно если задания выполняются сравнительно часто.

Служба теневого копирования томов (VSS)

Этот параметр работает только в операционных системах Windows.

Этот параметр указывает, должен ли поставщик службы теневого копирования томов (VSS) уведомлять VSS-совместимые приложения о предстоящем запуске резервного копирования. Это обеспечивает согласованное состояние всех данных, используемых приложениями. В частности, завершение всех транзакций в момент создания моментального снимка данных программным обеспечением резервного копирования. Согласованность данных, в свою очередь, обеспечивает восстановление приложения в корректном состоянии и возможность использования сразу после восстановления.

Значение по умолчанию: **Включено**. **Автоматический выбор поставщика моментальных снимков**.

Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

- **Автоматически выбирать поставщика моментальных снимков**

  Автоматический выбор из следующих вариантов: аппаратный поставщик моментальных снимков, программные поставщики моментальных снимков и программный поставщик теневого копирования (Microsoft).

- **Использовать программного поставщика теневого копирования (Microsoft)**

  Мы рекомендуем выбрать этот параметр при резервном копировании серверов приложений (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint или Active Directory).

Отключите этот параметр, если база данных несовместима с VSS. Процесс создания моментальных снимков ускорится, но согласованность данных приложений, в которых имеются незавершенные транзакции, не гарантируется. Можно использовать *Команды до и после захвата данных*, чтобы обеспечить согласованность данных, для которых выполняется резервное копирование. Например, укажите команды до захвата данных, которые приостановят работу базы данных и перенесут содержимое всех временных хранилищ для обеспечения корректного выполнения транзакций, укажите команды после захвата данных, которые возобновят операции базы данных после выполнения моментального снимка.

Примечание

Если этот параметр включен, резервное копирование файлов и папок, указанных в ключе реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot`, не выполняется. В частности, не выполняется резервное копирование файлов данных Outlook (.ost), поскольку они указаны в значении `OutlookOST` данного ключа.

Включить полное резервное копирование VSS

Если этот параметр включен, журналы Microsoft Exchange Server и других приложений, поддерживающих VSS (кроме Microsoft SQL Server), будут сокращаться каждый раз после полного, инкрементного или дифференциального резервного копирования на уровне дисков.

Значение по умолчанию: **Отключено**.

Оставьте параметр отключенным в следующих случаях:

- Если для резервного копирования данных Exchange Server используется агент для Exchange или ПО сторонних производителей. В этом случае усечение журналов помешает последующему резервному копированию журналов транзакций.
- Если для резервного копирования данных SQL Server используется программное обеспечение сторонних производителей. Программа стороннего производителя будет воспринимать получившуюся резервную копию диска как ”свою собственную” полную резервную копию. В результате следующее дифференциальное резервное копирование данных SQL Server завершится ошибкой. Резервное копирование будет завершаться ошибкой, пока программа стороннего производителя не создаст следующую собственную полную резервную копию.
- Если на машине работают другие VSS-совместимые приложения, журналы которых необходимо хранить по какой-либо причине.

При включении этого параметра не происходит усечения журналов Microsoft SQL Server. Чтобы сократить журнал SQL Server после выполнения резервного копирования, включите параметр резервного копирования *Сокращение журнала Microsoft SQL Server*.

Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр определяет, следует ли создавать замороженные моментальные снимки виртуальных машин. Чтобы создать замороженный моментальный снимок, программное обеспечение резервного копирования применяет VSS в виртуальной машине, используя VMware Tools или Hyper-V Integration Services.

Значение по умолчанию: **Включено**.

Если этот параметр включен, то транзакции всех приложений с поддержкой VSS, которые запущены на виртуальной машине, завершаются перед созданием моментального снимка. Если после нескольких попыток, количество которых определено параметром *Обработка ошибок*, не удается создать замороженный моментальный снимок и резервное копирование приложений отключено, создается обычный моментальный снимок. Если включено резервное копирование приложений, то резервное копирование завершается сбоем.

Если этот параметр отключен, создается обычный моментальный снимок. Будет создана резервная копия виртуальной машины с защитой от сбоев. Рекомендуем не выключать этот параметр даже на время и даже для виртуальных машин, на которых не выполняются приложения с поддержкой VSS. В противном случае невозможно будет гарантировать даже однородность файловой системы в рамках созданной резервной копии.

Примечание

Этот параметр не влияет на виртуальные машины oVirt, SpaceVM, ECP VeiL, а также OpenStack. Для них заморозка зависит от того, установлены ли инструменты масштабирования на виртуальной машине.

Еженедельное резервное копирование

Этот параметр определяет то, какие процессы резервного копирования считаются ”еженедельными” в правилах хранения и схемах резервного копирования. ”Еженедельная” резервная копия — это первая копия, которая создается после начала недели.

Значение по умолчанию: **Понедельник**.

Журнал событий Windows

Этот параметр работает только в ОС Windows.

Этот параметр указывает, должны ли агенты записывать события операций резервного копирования в журнал событий приложений Windows (чтобы просмотреть этот журнал, запустите файл eventvwr.exe или выберите **Панель управления** → **Администрирование** → **Просмотр событий**). События содержат статус и время завершения операции; события можно фильтровать.

Значение по умолчанию: **Отключено**.

Восстановление

Восстановление: памятка

Кибер Бэкап поддерживает множество сценариев восстановления:

- универсальное восстановление *физических* и *виртуальных* машин;
- *восстановление* физической машины в виртуальную;
- *миграцию* при восстановлении виртуальных машин;
- *мгновенное* восстановление виртуальных машин;
- гранулярное восстановление данных (файлов, дисков, баз данных, почтовых ящиков и т. д.).

В таблице ниже описаны данные, доступные для гранулярного восстановления.

Тип агента	Источник данных	Гранулярность
Для операционной системы	Linux, Windows	Диск/том, папка, файл
Для платформы виртуализации (на уровне гипервизора)	VMware, Hyper-V, oVirt, zVirt, ROSA, HOSTVM, Red Hat Virtualization, Basis DynamiX, РЕД Виртуализация, ECP Veil, SpaceVM, Кибер Инфраструктура, OpenStack, VK Cloud, OpenNebula, Брест, VMmanager	Диск/том, папка, файл
Для СУБД	Microsoft SQL Server, Oracle Database, SAP HANA, РЕД База Данных, PostgreSQL и СУБД на ее основе	База данных
	MySQL, MariaDB	База данных, таблица
Для платформы коммуникаций	Microsoft Exchange Server, VK WorkMail, Mailion, RuPost, CommuniGate Pro	Почтовый ящик, сообщение

Кибер Бэкап поддерживает различные методы восстановления. В таблице ниже кратко описаны доступные методы для каждой целевой системы.

Объект восстановления	Метод восстановления
Физическая машина (Windows или Linux)	*Использование веб-интерфейса* *Использование загрузочного носителя*
Виртуальная машина	*Использование веб-интерфейса*
Конфигурация ESXi	*Использование загрузочного носителя*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Объект восстановления	Метод восстановления
Файлы и папки	*Использование веб-интерфейса* *Использование загрузочного носителя* *Извлечение файлов из локальных резервных копий*
Базы данных Microsoft SQL Server	*Использование веб-интерфейса*
Базы данных Microsoft Exchange Server	*Использование веб-интерфейса*
Почтовые ящики Microsoft Exchange Server	*Использование веб-интерфейса*
Базы данных PostgreSQL	*Использование веб-интерфейса*
Базы данных Oracle	*Использование инструмента Oracle Explorer*
Данные CommuniGate Pro	*Использование веб-интерфейса*
Данные VK WorkMail и VK WorkDisk	*Использование веб-интерфейса*
Данные Mailion	*Использование веб-интерфейса*
Данные RuPost	*Использование веб-интерфейса*
Данные Kubernetes	*Использование веб-интерфейса*
Данные MySQL и MariaDB	*Использование веб-интерфейса*
РЕД База Данных	*Использование веб-интерфейса*
Серверы SAP HANA	*Использование веб-интерфейса*

Создание загрузочных носителей

Загрузочный носитель — это компакт-диск, DVD-диск, флэш-накопитель USB или другой съемный носитель, с помощью которого можно запустить агент, не используя операционную систему. Основная задача, для которой применяются такие носители, — восстановление операционной системы, которую не удается загрузить.

Мы настоятельно рекомендуем создать и протестировать загрузочный носитель сразу же после первого создания резервных копий дисков. Кроме того, рекомендуется повторно создавать носитель после каждого основного обновления агента защиты.

С помощью одного носителя можно восстановить как ОС Windows, так и Linux.

Создание загрузочного носителя в Windows и Linux

1. Загрузите ISO-файл загрузочного носителя с веб-сайта компании.
2. Выполните любое из следующих действий:
   - Запишите компакт- или DVD-диск, используя ISO-файл.
   - Создайте загрузочный флэш-накопитель USB, используя ISO-файл и один из бесплатных инструментов, доступных в Интернете.

Для машин с UEFI используйте `ISO to USB` или `RUFUS`, для машин с BIOS — `Win32DiskImager`. В Linux можно воспользоваться утилитой `dd`.

- Подключите ISO-файл в качестве CD/DVD-дисковода к виртуальной машине, которую требуется восстановить.

Кроме того, можно создать загрузочный носитель, используя *Мастер создания загрузочных копий*.

Восстановление машины

Физическая машина

В этом разделе описано восстановление физических машин через веб-интерфейс.

Используйте вместо веб-интерфейса загрузочный носитель, если вам необходимо восстановить:

- Любую операционную систему на ”голое железо” либо на отключенной машине.
- Структуру логических томов (тома созданы диспетчером логических томов в ОС Linux). Носитель позволяет автоматически воссоздать структуру логических томов.

Для восстановления операционной системы потребуется перезагрузка. Вы можете перезапустить машину автоматически или присвоить ей статус **Требуется вмешательство**. Восстановленная операционная система автоматически запускается.

Восстановление физической машины

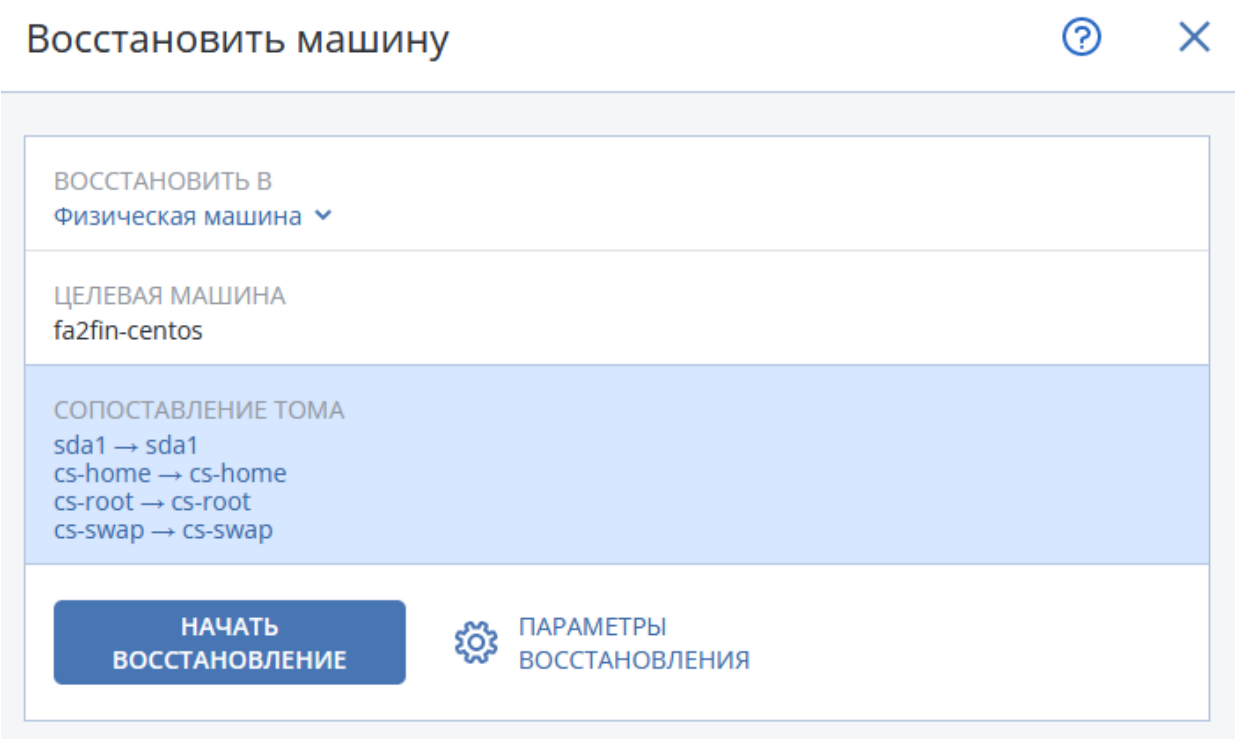
1. Выберите машину, для которой есть резервная копия.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:

   - Если резервная копия расположена в общем хранилище данных (т. е. другие агенты могут получить к ней доступ), щёлкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.
   - Восстановите машину, как описано в теме *Восстановление дисков с помощью загрузочного носителя*.
4. Последовательно выберите пункты **Восстановление** → **Вся машина**.

Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

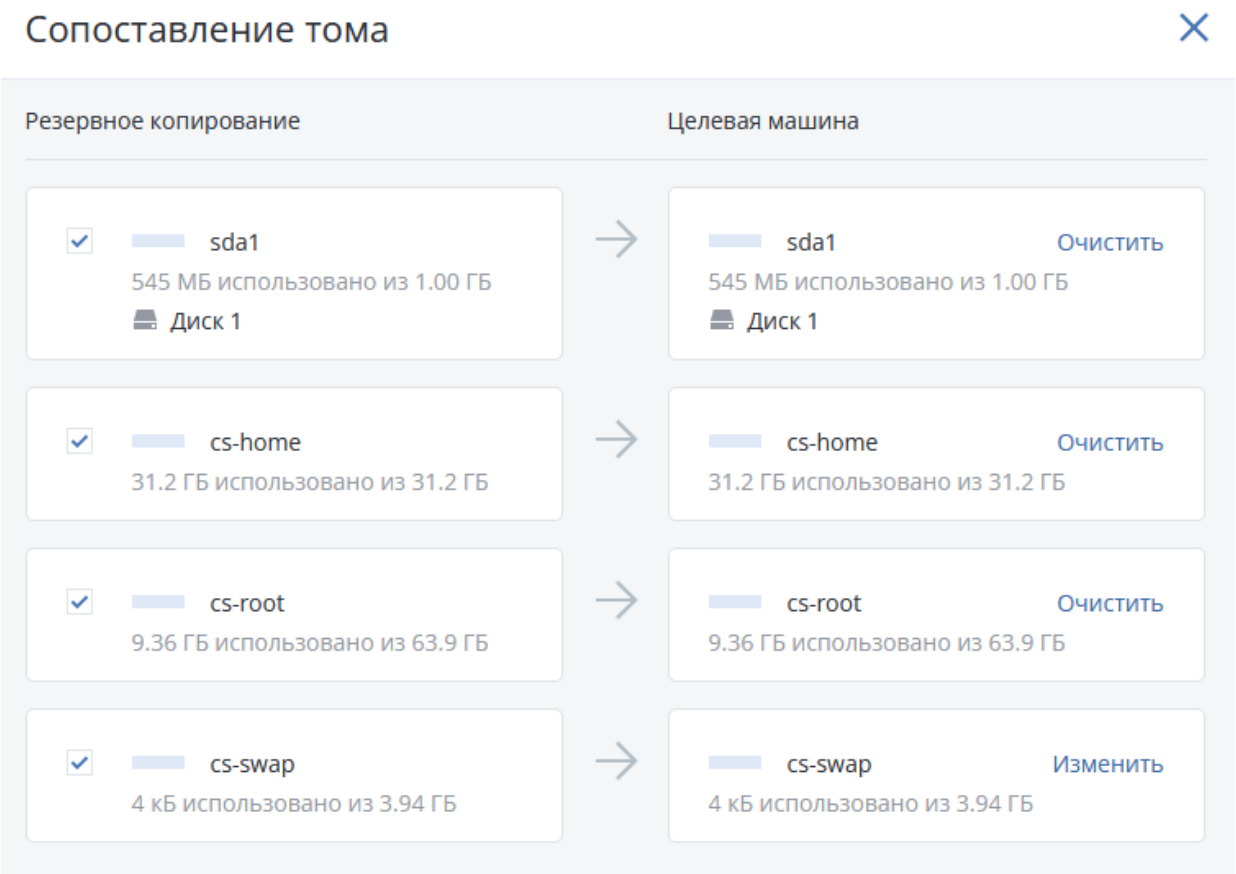
Чтобы выполнить восстановление в другую виртуальную машину, щёлкните **Целевая машина** и выберите включенную целевую машину.



5. Если результат сопоставления вас не удовлетворяет или если выполнить сопоставление не удалось, нажмите **Сопоставление тома**, чтобы сопоставить диски заново вручную.

   Раздел сопоставления также позволяет вам выбирать отдельные диски или тома для восстановления.

> **Примечание**
>
> Автоматическое сопоставление томов возможно только в последовательном порядке при условии, что конфигурации целевой машины и машины-источника одинаковы. Если конфигурации машин различаются, сопоставить тома можно только в ручном режиме.



6. Щёлкните **Начать восстановление**.
7. Подтвердите перезапись дисков версиями из резервной копии. Укажите, следует ли автоматически перезапустить машину.

Ход выполнения восстановления показан на вкладке **Действия**.

Восстановление физической машины в виртуальную

В этом разделе описано восстановление физической машины в качестве виртуальной (P2V) с использованием веб-интерфейса. Эту операцию можно выполнить, если установлен и зарегистрирован хотя бы один агент для целевой платформы виртуализации.

Доступные места восстановления и ограничения восстановления P2V см. в разделе *Миграция машины*.

Для восстановления физической Linux-машины с логическими томами (LVM) в виртуальную см. раздел *Миграция Linux-машины с логическими томами (LVM)*.

Дополнительную информацию о миграции P2V см. в разделе *Миграция машины*.

Восстановление физической машины как виртуальной

1. Выберите машину, для которой есть резервная копия.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

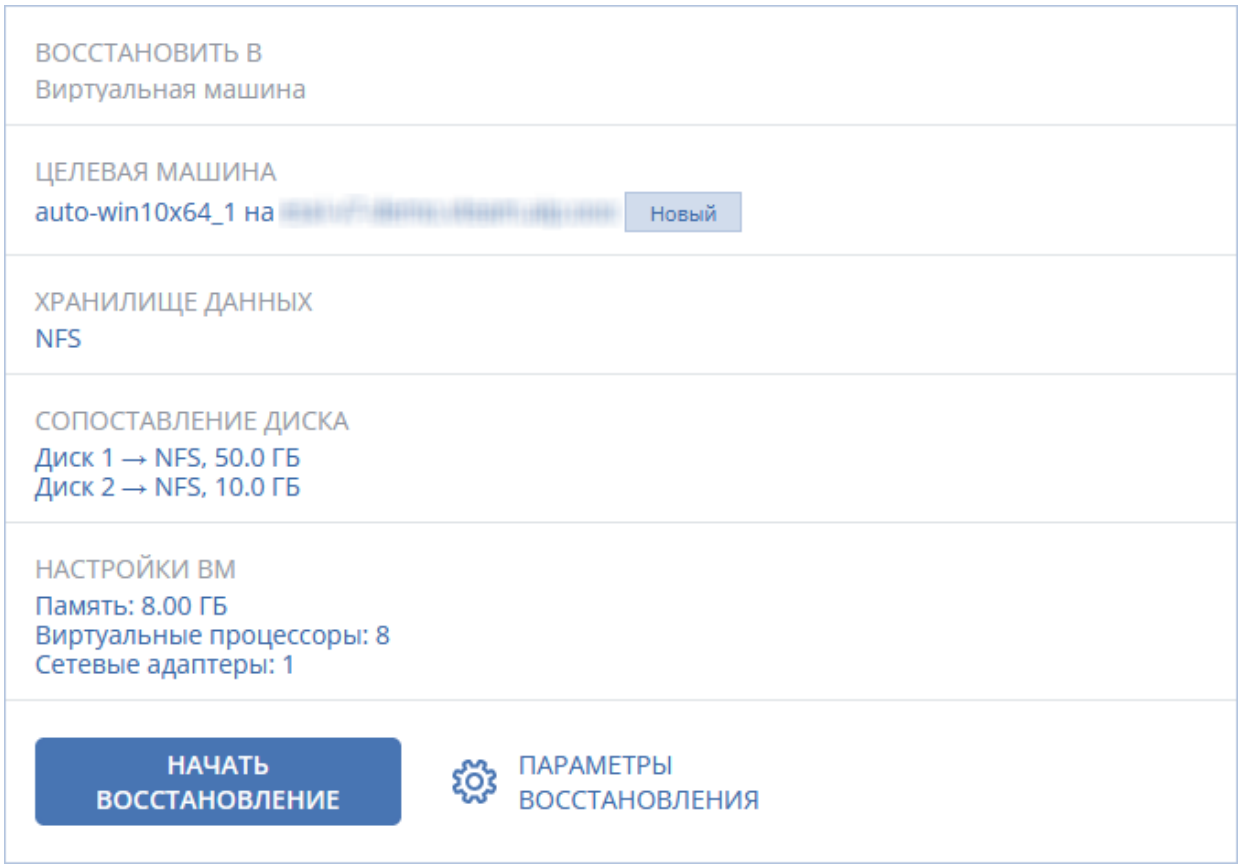
   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих действий:

   - Если резервная копия расположена в общем хранилище данных (другие агенты могут получить к ней доступ), щёлкните **Выбрать машину**, выберите машину, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.
   - Восстановите машину, как описано в разделе *Восстановление дисков с помощью загрузочного носителя*.
4. Последовательно выберите пункты **Восстановление** → **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щёлкните **Целевая машина**.
   1. В выпадающем списке выберите тип целевой виртуальной машины.

      Должен быть установлен хотя бы один агент для выбранного типа виртуальной машины.
   2. Выберите машину, в которую будут выполняться восстановление: новая или существующая. Выбор новой машины предпочтительнее, поскольку для нее не требуется, чтобы конфигурация диска целевой машины в точности соответствовала конфигурации диска в резервной копии.
   3. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.
   4. Нажмите кнопку **ОК**.
7. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:

   - Щёлкните **Хранилище данных** (или **Путь** для Hyper-V) и выберите хранилище данных для данной виртуальной машины.
   - Щёлкните **Сопоставление дисков**, чтобы выбрать хранилище данных, интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.

- Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щёлкните **Настройки ВМ**.



8. Щёлкните **Начать восстановление**.
9. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход выполнения восстановления показан на вкладке **Действия**.

Виртуальная машина

Восстановление на виртуальную машину выполняется, только когда машина остановлена. Программа останавливает машину без запроса. После завершения восстановления машину потребуется запустить вручную.

Это поведение можно изменить, используя параметр восстановления ”Управление питанием ВМ” (выберите **Параметры восстановления** → **Управление питанием ВМ**).

Восстановление виртуальной машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.
2. Последовательно выберите пункты **Восстановление** → **Вся машина**.
3. Чтобы выполнить восстановление на физическую машину, в списке **Восстановить в** выберите пункт **Физическая машина**. В противном случае пропустите этот шаг.

   Восстановление в физическую машину возможно только в том случае, если конфигурация целевой машины в точности соответствует конфигурации диска в данной резервной копии.

   В этом случае продолжите с шага 4 в разделе *Физическая машина*. В противном случае рекомендуется выполнить миграцию виртуальной машины в физическую (V2P), *используя загрузочный носитель*.
4. По умолчанию исходная машина выбирается в качестве целевой.

   Чтобы выполнить восстановление на другую виртуальную машину, выберите **Целевая машина** и выполните следующие действия:

   1. Выберите гипервизор.
   2. Выберите машину, в которую будет выполняться восстановление: новая или существующая.

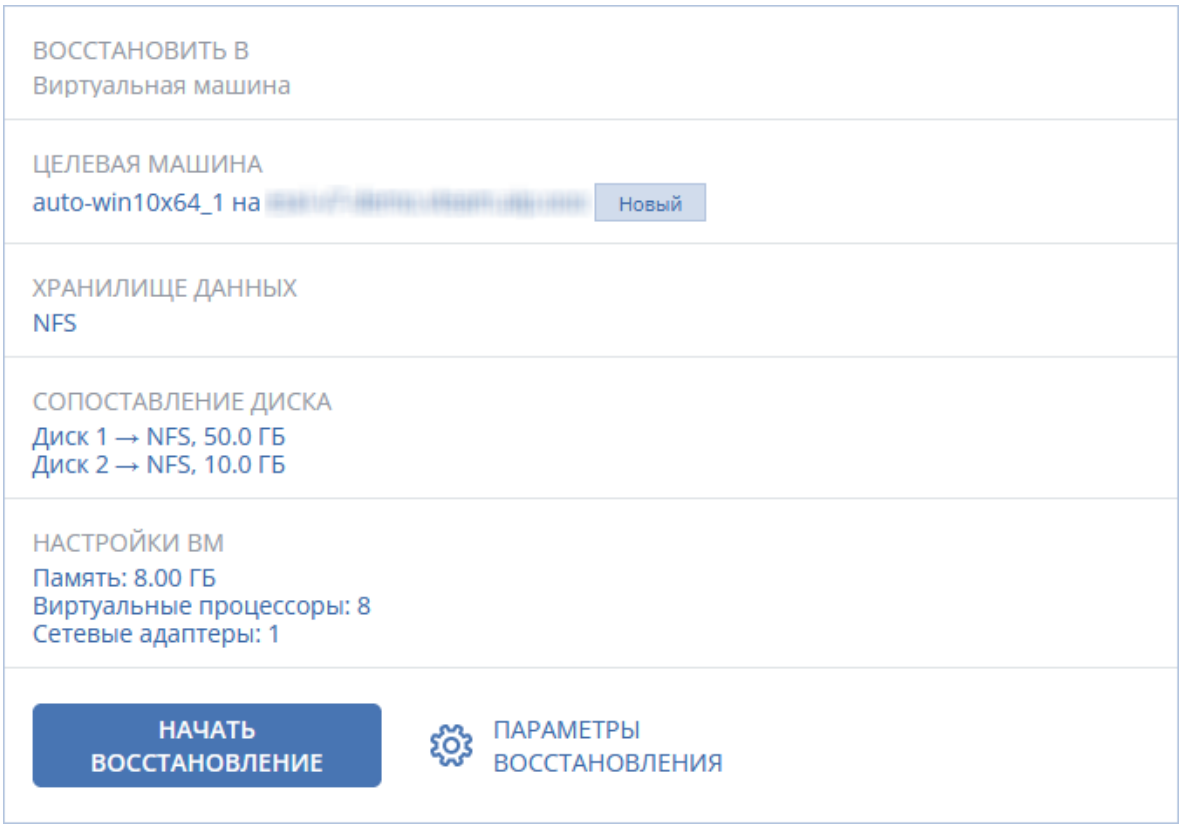
      Примечание

      Виртуальные машины OpenStack можно восстанавливать только в новые ВМ.

   3. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.
   4. Нажмите кнопку **ОК**.
5. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:
   - Щёлкните **Хранилище данных** (или **Путь** для Hyper-V) и выберите хранилище данных для виртуальной машины.
   - Щёлкните **Сопоставление диска**, чтобы выбрать интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.

- Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щёлкните **Настройки ВМ**.

> **Примечание**
>
> При необходимости ВМ можно восстановить без сетевых адаптеров. Исключение составляет система OpenStack и продукты на её основе (Кибер Инфраструктура, VK Cloud), ВМ в которых всегда должны иметь хотя бы один сетевой адаптер.



6. Щёлкните **Начать восстановление**.
7. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход выполнения восстановления показан на вкладке **Действия**.

При восстановлении виртуальной машины OpenStack из резервной копии будут созданы только диски и сетевой порт виртуальной машины, если:

- в конфигурации OpenStack используется единственная внешняя сеть без подсетей и внешний DHCP-сервер (автоматическое восстановление виртуальной машины невозможно из-за ограничений OpenStack);
- виртуальную машину OpenStack не удается восстановить из-за ошибок ПО OpenStack (например, нет доступных хостов для запуска виртуальной машины).

В таком случае используйте восстановленные диски, чтобы создать новую ВМ вручную из командной строки OpenStack (подробнее см. в официальной документации OpenStack).

Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе *Создание загрузочного носителя*.

Порядок восстановления дисков с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щёлкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, щёлкните **Инструменты** → **Прокси-сервер** и укажите имя хоста/IP-адрес и порт прокси-сервера. В противном случае пропустите этот шаг.
4. На экране приветствия нажмите **Восстановить**.
5. Щёлкните **Выбрать данные** и нажмите **Обзор**.
6. Укажите хранилище резервных копий.

   Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **ОК**, чтобы подтвердить выбор.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. В разделе **Содержимое резервной копии** выберите диски, которые нужно восстановить. Нажмите **ОК**, чтобы подтвердить выбор.
9. В разделе **Место восстановления** программное обеспечение автоматически сопоставит выбранные диски с целевыми.

   Если выполнить сопоставление не удалось или его результат вас не устраивает, сопоставьте диски заново вручную.

   > **Примечание**
   >
   > Изменение структуры дисков может повлиять на загружаемость операционной системы. Если вы не уверены в полном успехе, используйте исходную структуру дисков машины.

10. [Только для ОС Linux] Если на машине, резервная копия которой создавалась, имелись логические

тома (LVM), а вам необходимо воспроизвести исходную структуру LVM, выполните перечисленные ниже действия:

1. Убедитесь, что количество дисков на целевой машине и емкость каждого диска равны аналогичным значениям исходной машины, а затем щёлкните **Применить RAID/LVM**.
2. Просмотрите структуру томов, а затем нажмите **Применить RAID/LVM**, чтобы создать ее.

11. [Необязательно] Щёлкните **Параметры восстановления**, чтобы указать дополнительные настройки.
12. Нажмите **ОК**, чтобы начать восстановление.

Использование компонента Универсальное восстановление (Universal Restore)

Новейшие версии операционных систем сохраняют загружаемость при восстановлении на отличающееся оборудование или платформы виртуализации. Если восстановленная операционная система не загружается, используйте компонент Универсальное восстановление (Universal Restore), чтобы обновить драйверы и модули, необходимые для загрузки системы.

Компонент можно применить к операционным системам Windows и Linux.

Порядок использования компонента Универсальное восстановление (Universal Restore)

1. Загрузите машину с загрузочного носителя.
2. Щёлкните **Использовать Universal Restore**.
3. Если на машине несколько операционных систем, выберите, к какой из них следует применить данный компонент.
4. [Только для Windows] *Дополнительные настройки*.
5. Нажмите кнопку **ОК**.

Компонент Универсальное восстановление (Universal Restore) в Windows

Подготовка

Подготовьте драйверы

Прежде чем применять компонент Универсальное восстановление (Universal Restore) к операционной системе Windows, удостоверьтесь в наличии драйверов для нового контроллера жестких дисков и набора микросхем. Эти драйверы являются критическими для запуска операционной системы. Используйте компакт-диски или DVD-диски, предоставленные поставщиками аппаратных средств, или

загрузите драйверы с веб-сайта поставщика. Файлы драйверов должны иметь расширение .inf. В случае загрузки драйверов в форматах EXE, CAB или ZIP получите их с помощью стороннего приложения.

Наилучшим решением является хранение драйверов для всех аппаратных средств, используемых в организации, в едином репозитории с сортировкой по типу устройств или аппаратным конфигурациям. Копию репозитория можно хранить на DVD-диске или флэш-накопителе, поместить нужные драйверы на загрузочный носитель или создать пользовательский загрузочный носитель с требуемыми драйверами (а также файлами конфигурации сети) для каждого сервера. Или можно просто указывать путь к репозиторию каждый раз, когда используется данный компонент.

Проверьте наличие доступа к драйверам в загрузочной среде

Убедитесь в наличии доступа к устройству с драйверами при работе с загрузочного носителя. Используйте носитель на основе WinPE, если устройство доступно в Windows, но носитель на основе Linux не обнаружил его.

Настройки компонента Универсальное восстановление (Universal Restore)

Автоматический поиск драйверов

Укажите, где программа должна искать драйверы слоя абстрагирования оборудования (HAL), контроллера жестких дисков и сетевых адаптеров.

- Если драйверы находятся на диске от производителя или другом съемном носителе, установите флажок **Поиск на съемных носителях**.
- Если драйверы находятся в сетевой папке или на загрузочном носителе, укажите путь к этой папке, нажав кнопку **Добавить папку**.

Кроме того, компонент выполнит поиск драйверов в папке, используемой по умолчанию для хранения драйверов Windows. Ее расположение определяется значением реестра `DevicePath` в разделе `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion`. Обычно это папка `WINDOWS/inf`.

Компонент выполнит рекурсивный поиск во всех папках, вложенных в указанную папку, обнаружит наиболее подходящие драйверы HAL и контроллера жестких дисков из всех имеющихся и установит их в операционную систему. Компонент выполняет также поиск драйвера сетевого адаптера. После его обнаружения компонент передает путь к найденному драйверу операционной системе. Если на машине установлено несколько сетевых интерфейсных плат, компонент попытается настроить драйверы всех плат.

Драйверы запоминающих устройств для обязательной установки

Этот параметр необходим в следующих случаях.

- На компьютере установлен особый контроллер запоминающего устройства, например RAID (особенно NVIDIA RAID) или адаптер Fibre Channel.
- Система перенесена на виртуальную машину, которая использует контроллер жесткого диска SCSI. Используйте драйверы SCSI, предоставленные в пакете программного обеспечения виртуализации, или загрузите последние версии драйверов с веб-сайта разработчика программного обеспечения.
- Если не удалось загрузить систему с помощью автоматического поиска драйверов.

Укажите нужные драйвер, нажав кнопку **Добавить драйвер**. Указанные драйверы будут установлены, даже если программа найдет лучший драйвер, с выдачей соответствующего предупреждения.

Применение компонента Универсальное восстановление (Universal Restore)

Указав требуемые настройки, нажмите кнопку **ОК**.

Если компоненту не удается найти совместимый драйвер в указанных расположениях, будет выведено сообщение о проблемном устройстве. Выполните одно из следующих действий:

- Добавьте драйвер в любое из ранее указанных расположений и нажмите кнопку **Повторить**.
- Если вы не помните расположения, нажмите кнопку **Пропустить**, чтобы продолжить процесс. При неудовлетворительном результате заново примените компонент. При настройке операции укажите необходимый драйвер.

После загрузки Windows начнется стандартная процедура установки новых устройств. Драйвер сетевого адаптера будет установлен без уведомлений при наличии у него подписи Microsoft Windows. В противном случае Windows попросит подтвердить установку неподписанного драйвера.

После этого пользователь сможет настроить сетевое подключение и указать драйверы для видеоадаптера, USB и других устройств.

Компонент Универсальное восстановление (Universal Restore) в Linux

Компонент Универсальное восстановление (Universal Restore) может применяться к операционным системам Linux с версией ядра 3.0 или более поздней.

Если компонент применяется к операционной системе Linux, обновляется временная файловая система, известная как начальный электронный диск (initrd). Это обеспечивает загрузку операционной системы на новом оборудовании.

Компонент добавляет к начальному электронному диску модули для нового оборудования (включая драйверы устройств). Обычно все необходимые модули обнаруживаются в папке `/lib/modules`. Если компонент не может найти нужный модуль, имя файла модуля записывается в журнал.

Компонент может изменить конфигурацию загрузчика GRUB. Возможно, для этого потребуется обеспечить загружаемость системы, если структура томов новой машины отличается от исходной машины.

Компонент никогда не изменяет ядро Linux.

Возврат к исходному начальному RAM-диску

При необходимости можно вернуться к исходному начальному RAM-диску.

Начальный RAM-диск хранится в файле на машине. Перед первым обновлением начального RAM-диска компонент сохраняет его копию в той же папке. Имя копии — это имя файла с прибавлением суффикса **_acronis_backup.img**. При запуске компонента более одного раза (например, после добавления недостающих драйверов) эта копия не перезаписывается.

Чтобы вернуться к исходному начальному RAM-диску, выполните любое из следующих действий.

- Измените имя копии соответствующим образом. Например, выполните команду, подобную следующей:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
```

- Укажите копию в строке `initrd` конфигурации загрузчика GRUB.

Восстановление файлов

Восстановление файлов с помощью веб-интерфейса

С помощью веб-консоли Кибер Бэкап можно восстановить файлы, которые ранее были расположены на физической или виртуальной машине с установленным агентом, или на машине, защищённой с помощью виртуального устройства (virtual appliance).

Восстановить файлы можно:

- на физическую или виртуальную машину с агентом (как на исходную, так и на другую);
- путём сохранения их в сетевое хранилище, из которого впоследствии их можно будет извлечь;
- загрузив их с помощью веб-консоли на машину, в которой открыта веб-консоль.

Порядок восстановления файлов

1. В веб-консоли Кибер Бэкап перейдите во вкладку **Устройства**.
2. Выберите машину, файлы которой необходимо восстановить.
3. Щёлкните **Восстановление**.
4. Выберите точку восстановления, нажав на соответствующие дату и время точки восстановления.

   > **Примечание**
   >
   > Если резервные копии хранятся в нескольких хранилищах, то точки восстановления будут отфильтрованы по хранилищу. Для выбора хранилища установите флажок напротив имени хранилища в списке **Хранилище резервных копий**.

   Если физическая или виртуальная машина с установленным агентом отключена, то значок машины будет серого цвета, а точки восстановления не будут отображены. В этом случае выполните одно из предлагаемых в веб-консоли действий:

   - [Рекомендуется] Если резервная копия расположена в общем хранилище данных (т. е. другие агенты могут получить к ней доступ), щёлкните **Выбор машины**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке **Хранилища резервных копий**.
   - Используйте загрузочный носитель (подробнее см. в разделе *Использовать загрузочный носитель*).
5. Нажмите кнопку **Восстановление** и выберите **Файлы/папки**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

   Можно использовать один или несколько подстановочных символов (* и ?), подробнее см. в разделе *Фильтры файлов*.
7. Отметьте флажками папки и файлы, которые необходимо восстановить.
8. Если требуется сохранить выбранные папки и файлы на машине, с помощью которой открыта веб-консоль Кибер Бэкап, нажмите кнопку **Загрузить** (иначе пропустите этот шаг). В результате выбранные файлы будут загружены в компьютер.

   > **Примечание**
   >
   > Если выбрана папка или несколько файлов, загрузка будет выполнена в виде ZIP-архива.

> **Важно**
>
> Если общий размер выбранных файлов превышает 100 МБ, загрузка будет недоступна.

9. Если требуется восстановить выбранные папки и файлы на машину с установленным агентом, или чтобы сохранить файлы в сетевом хранилище, доступном машине с агентом (который будет выполнять восстановление), нажмите кнопку **Восстановить**.
10. Выберите целевую машину в блоке **Восстановить в**, нажав на отображаемое имя машины, затем в предложенном списке выберите машину с установленным агентом и нажмите **ОК**.
11. В случае отображения окна **Укажите учётные данные** введите имя пользователя и пароль учётной записи для доступа к хранилищу с выбранной резервной копией.
12. В блоке **Путь** установите флажок для выбора целевого места на машине, куда будут сохранены восстанавливаемые файлы. Доступные варианты:
    - Исходное расположение (доступно только при восстановлении на исходную физическую или виртуальную машину с установленным агентом).
    - Пользовательское расположение, нажав **Обзор**, можно выбрать:
        - локальную папку на машине с агентом, с помощью которой осуществляется восстановление;
        - сетевую папку, доступную для машины с агентом, с помощью которой выполняется восстановление.
13. Нажмите кнопку **Начать восстановление**.
14. Выберите один из вариантов восстановления файлов:
    - **Перезаписывать существующие файлы**.
    - **Перезаписывать существующие файлы более новыми**.
    - **Не перезаписывать существующие файлы**.
15. Установите или снимите флажок **При необходимости перезагрузить машину**.
16. Нажмите кнопку **Продолжить**.

Ход выполнения восстановления будет отображаться справа во всплывающей области **Сведения о действии**, а также в разделе **Панель мониторинга** → **Действия**.

Восстановление файлов с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе *Создание загрузочного носителя*.

Чтобы восстановить файлы с помощью загрузочного носителя:

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щёлкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, щёлкните **Инструменты** → **Прокси-сервер** и укажите имя хоста/IP-адрес и порт прокси-сервера. В противном случае пропустите этот шаг.
4. На экране приветствия нажмите кнопку **Восстановить**.
5. Щёлкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. Укажите хранилище резервных копий.

   Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **ОК**, чтобы подтвердить выбор.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. В области **Содержимое резервной копии** выберите **Файлы/папки**.
9. Выберите данные, которые необходимо восстановить. Нажмите кнопку **ОК**, чтобы подтвердить выбор.
10. В разделе **Место восстановления** укажите нужную папку. При желании можно запретить перезапись более новых версий файлов или исключить некоторые файлы из списка восстанавливаемых.
11. [Необязательно] Щёлкните **Параметры восстановления**, чтобы указать дополнительные настройки.
12. Нажмите кнопку **ОК**, чтобы начать восстановление.

Примечание

Хранилище на ленте занимает много места и может не соответствовать ОЗУ при повторном сканировании или восстановлении с использованием загрузочного носителя на основе Linux или WinPE. Для Linux нужно будет подключить другое хранилище для сохранения данных на диске или ресурсе общего доступа. Для Windows PE пока нет решения этой проблемы.

Извлечение файлов из локальных резервных копий

Можно просмотреть содержимое резервных копий и извлечь необходимые файлы.

Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, на которой выполняется поиск резервной копии, должен быть установлен агент защиты.
- Файловая система, для которой создается резервная копия, должна иметь один из следующих типов: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS или HFS+.
- Резервная копия должна хранится в локальной папке или в сетевой папке (SMB/CIFS).

Порядок извлечения файлов из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щёлкните файл резервной копии. Файлы имеют имена на основе следующего шаблона: `<имя машины> - <GUID плана защиты>`
3. Если резервная копия защищена паролем, укажите его. В противном случае пропустите этот шаг.

   В проводнике отображаются точки восстановления.
4. Дважды щёлкните точку восстановления.

   В проводнике отображаются данные, для которых созданы резервные копии.
5. Обзор требуемой папки.
6. Скопируйте требуемые файлы в любую папку в файловой системе.

Восстановление конфигурации ESXi

Чтобы восстановить конфигурацию ESXi, необходим загрузочный носитель на основе Linux. Информацию о том, как создать загрузочный носитель, см. в разделе *Создание загрузочного носителя*.

Если при восстановлении конфигурации ESXi на хост, который не является исходным, исходный хост ESXi все еще подключен к vCenter Server, отключите и удалите этот хост из vCenter Server, чтобы избежать неожиданных проблем при восстановлении. Чтобы сохранить исходный хост вместе с восстановленным, можно снова добавить его по окончании восстановления.

Виртуальные машины, которые выполняются на данном хосте, не включены в резервную копию конфигурации ESXi. Создать для них резервную копию и восстановить их можно отдельно.

Порядок восстановления конфигурации ESXi

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Щёлкните **Локальное управление этой машиной**.
3. На экране приветствия нажмите кнопку **Восстановить**.
4. Щёлкните **Выбрать данные** и нажмите кнопку **Обзор**.
5. Укажите хранилище резервных копий.
   - Укажите папку в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **ОК**, чтобы подтвердить выбор.
6. В поле **Показать** выберите **Конфигурации ESXi**.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. Нажмите кнопку **ОК**.
9. В разделе **Диски для новых хранилищ данных** выполните следующие действия:
   - В поле **Восстановить ESXi в** выберите диск, на который будет восстановлена конфигурация хоста. При восстановлении конфигурации на исходный хост исходный диск выбирается по умолчанию.
   - [Необязательно] В поле **Использовать для новых хранилищ данных** выберите диски, в которых будут созданы новые хранилища данных. Будьте внимательны, поскольку все данные на выбранных дисках могут быть утрачены. Чтобы сохранить виртуальные машины в существующих хранилищах данных, не выбирайте никакие диски.
10. Если для новых хранилищ данных выбраны какие-либо диски, выберите метод создания хранилища данных в поле **Создание новых хранилищ данных**: **Создать одно хранилище данных на диск** или **Создать одно хранилище на всех выбранных жестких дисках**.
11. [Необязательно] В разделе **Сопоставление сети** измените результат автоматического сопоставления виртуальных коммутаторов, присутствующих в резервной копии, с физическими сетевыми картами.
12. [Необязательно] Щёлкните **Параметры восстановления**, чтобы указать дополнительные настройки.
13. Нажмите кнопку **ОК**, чтобы начать восстановление.

Параметры восстановления

Чтобы изменить параметры восстановления, щёлкните **Параметры восстановления** при настройке восстановления.

Доступность параметров восстановления

Набор доступных параметров восстановления зависит от следующих факторов.

- Среда, в которой работает агент, выполняющий восстановление (Windows, Linux или загрузочный носитель).
- Тип данных, для которых выполняется восстановление (диски, файлы, виртуальные машины, данные приложения).

Следующая таблица включает в себя общие сведения о доступности параметров восстановления.

Раздел руководства с описанием параметра	**Диски**			**Файлы**			**Виртуальные машины**	**SQL и Exchange**
	Windows	**Linux**	**Загрузочный носитель**	**Windows**	**Linux**	**Загрузочный носитель**	**ESXi, Hyper-V**	**Windows**
Проверка резервных копий	+	+	+	+	+	+	+	+
Режим загрузки	+	—	—	—	—	—	+	—
Дата и время для файлов	—	—	—	+	+	+	—	—
Обработка ошибок	+	+	+	+	+	+	+	+
Исключения файлов	—	—	—	+	+	+	—	—
Безопасность на уровне файлов	—	—	—	+	—	—	—	—
Flashback	+	+	+	—	—	—	+	—
Восстановление полного пути	—	—	—	+	+	+	—	—
Точки подключения	—	—	—	+	—	—	—	—
Производительность	+	+	—	+	+	—	+	+

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Раздел руководства с описанием параметра	Диски			Файлы			Виртуальные машины	SQL и Exchange
	Windows	Linux	Загрузочный носитель	Windows	Linux	Загрузочный носитель	ESXi, Hyper-V	Windows
Команды до и после процедуры	+	+	—	+	+	—	+	+
Изменение идентификатора безопасности	+	—	—	—	—	—	—	—
Управление питанием ВМ	—	—	—	—	—	—	+	—
Использование кэша диска для ускорения восстановления	—	—	—	+	+	—	—	—
Журнал событий Windows	+	—	—	+	—	—	Только Hyper-V	+
Включить после восстановления	—	—	—	—	—	+	—	—

Проверка резервных копий

Этот параметр определяет, выполнять ли проверку резервной копии на повреждения перед восстановлением из нее данных. Эта операция выполняется агентом защиты.

Значение по умолчанию: **Отключено**.

При проверке резервной копии тома вычисляется контрольная сумма для каждого блока данных, сохраненного в резервной копии.

Проверка — это длительный процесс даже при инкрементном или дифференциальном резервном копировании небольших объемов данных. Причина заключается в том, что во время операции проверяются не только данные, физически присутствующие в резервной копии, но и все данные, которые восстанавливаются при выборе этой резервной копии. Это требует доступа к созданным ранее резервным копиям.

Режим загрузки

Этот параметр работает при восстановлении физической или виртуальной машины с резервной копии на уровне дисков, которая содержит операционную систему Windows.

Этот параметр позволяет выбрать режим загрузки (BIOS или UEFI), который Windows будет использовать после восстановления. Если режим загрузки исходной машины отличается от выбранного режима загрузки, программа:

- Инициализирует диск, на который восстанавливается системный том в соответствии с выбранным режимом загрузки (MBR для BIOS, GPT для UEFI).
- Адаптирует операционную систему Windows для запуска в выбранном режиме загрузки.

Значение по умолчанию: **Как и в целевой машине**.

Можно выбрать один из следующих вариантов:

- **Как и в целевой машине**

  Агент, запущенный на целевой машине, определяет режим загрузки, который в настоящее время используется Windows, и вносит изменения в соответствии с обнаруженным режимом загрузки.

  Это наиболее безопасное значение, которое автоматически приводит к созданию загрузочной системы, если только не применяются указанные ниже ограничения. Поскольку параметр **Режим загрузки** отсутствует на загрузочном носителе, агент на носителе всегда работает таким образом, словно это значение выбрано.

- **Как и в машине, для которой есть резервная копия**

  Агент, запущенный на целевой машине, считывает режим загрузки с резервной копии и вносит изменения в соответствии этим режимом загрузки. Это помогает восстановить систему на другой машине, даже если на этой машине используется другой режим загрузки, а затем заменить диск на машине, для которой создана резервная копия.

- **BIOS**

  Агент, запущенный на целевой машине, вносит изменения для использования BIOS.

- **UEFI**

  Агент, запущенный на целевой машине, вносит изменения для использования UEFI.

После изменения параметра будет повторно выполнена процедура сопоставления диска. Это займет некоторое время.

Рекомендации

Чтобы передать Windows между UEFI и BIOS, выполните указанные ниже действия:

- Восстановите весь диск, на котором расположен системный том. При восстановлении только системного тома поверх существующего тома агент не сможет правильно инициализировать целевой диск.
- Помните, что BIOS не позволяет использовать более 2 ТБ дискового пространства.

Ограничения

- Перенос между UEFI и BIOS поддерживается для 64-разрядных операционных систем Windows и Windows Server.
- Перенос между UEFI и BIOS не поддерживается, если резервная копи хранится на ленточном устройстве.

Если перенос системы между UEFI и BIOS не поддерживается, агент работает так, словно выбрана настройка **Как и в машине, для которой есть резервная копия**. Если целевая машина поддерживает как UEFI, так и BIOS, необходимо вручную включить режим загрузки, соответствующий исходной машине. Иначе система не загрузится.

Дата и время для файлов

Этот параметр применим только при восстановлении файлов.

Этот параметр определяет, получить ли дату и время восстановленных файлов из резервной копии или присвоить файлам текущую дату и время.

Если этот параметр включен, файлам будет назначена текущая дата и время.

Значение по умолчанию: **Отключено**.

Обработка ошибок

Они позволяют указать, как должны обрабатываться ошибки, возникшие при восстановлении.

В случае ошибки повторить операцию

Значение по умолчанию: **Включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены, как только операция

будет успешно выполнена ИЛИ по достижении указанного максимального количества попыток (в зависимости от того, что наступит раньше).

Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)

Значение по умолчанию: **Отключено**.

В режиме без вывода сообщений программа автоматически разрешает ситуации, требующие вмешательства пользователя. Если операция не может быть продолжена без вмешательства пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

Пропускать файлы с ошибками при восстановлении

Значение по умолчанию: **Отключено**.

Режим активируется отдельно для каждого восстановления.

Режим позволяет не прерывать восстановление из файловой резервной копии при возникновении ошибок. Восстановление выполняется в полном размере, с пропуском конфликтных файлов.

Причины, по которым файлы могут быть пропущены:

- имя файла слишком длинное,
- имя файла имеет неподдерживаемые спецсимволы,
- невозможно изменить файл в месте, куда происходит восстановление,
- нет прав на изменение файла в месте, куда происходит восстановление.

Пропущенные при восстановлении файлы можно посмотреть

в ОС Windows

в файле `C:\ProgramData\Acronis\BackupAndRecovery\MMS\pcs.0.log.gz`

в ОС Linux

в файле `/var/lib/Acronis/BackupAndRecovery/MMS/pcs.0.log.gz`

Сохранить сведения о системе при сбое восстановления с перезагрузкой

Этот параметр применим для диска или тома восстановления на физическую машину с Windows или Linux.

Значение по умолчанию: **Отключено**.

Если этот параметр включен, можно указать папку на локальном диске (включая устройства флэш-памяти или жесткие диски (HDD), подсоединенные к целевой машине) или на сетевой папке, в которую будут сохраняться журналы, сведения о системе и файлы аварийных дампов. Этот файл поможет сотрудникам сопровождения ПО определить проблему.

Исключения файлов

Этот параметр применим только при восстановлении файлов.

Этот параметр определяет файлы и папки, которые будут пропущены в процессе восстановления и по причине этого исключены из списка восстановленных элементов.

Каждое условие об исключении файлов (имя файла, путь к файлу или маска) указывается в отдельном поле, при указывании можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе *Условия*.

> **Примечание**
>
> Исключения переопределяют выбор элементов данных для восстановления. Например, если выбрать восстановление файла MyFile.tmp, но при этом исключить все TMP-файлы, файл MyFile.tmp не будет восстановлен.

Безопасность на уровне файлов

Этот параметр действует для файловых систем, поддерживающих атрибуты безопасности (например, NTFS), при восстановлении файлов с диска и резервных копий на уровне файлов.

Этот параметр определяет, должны ли восстанавливаться атрибуты безопасности вместе с файлами.

Значение по умолчанию: **Включено**.

Можно выбрать восстановление атрибутов безопасности или наследование файлами их атрибутов безопасности от папки, в которую они восстанавливаются.

Flashback

Этот параметр действует при восстановлении дисков и томов на физических и виртуальных машинах.

Если этот параметр включен, восстанавливаются только различия между данными в резервной копии и данными на целевом диске. Это ускоряет восстановление данных на диск, для которого создана резервная копия, особенно если структура тома данного диска не изменена. Данные сравниваются на уровне блоков.

Сравнение данных на уровне блоков — это длительная операция для физических машин. При наличии

быстрого подключения к хранилищу резервных копий на восстановление всего диска потребуется меньше времени, чем на вычисления разницы в данных. Поэтому мы рекомендуем включать этот параметр только при медленном подключении к хранилищу резервных копий (например, если резервная копия расположена на удаленной сетевой папке).

При восстановлении физической машины предварительно задана настройка **Отключено**.

При восстановлении виртуальной машины предварительно задана настройка **Включено**.

Восстановление полного пути

Этот параметр действует только при восстановлении из резервной копии на уровне файлов.

Если этот параметр включен, в целевом хранилище воссоздается полный путь к файлу.

Значение по умолчанию: **Отключено**.

Точки подключения

Этот параметр действует только в Windows для восстановления данных с резервной копии на уровне файлов.

Включите этот параметр для восстановления файлов и папок, которые хранятся на подключенных томах и резервные копии которых создавались с включенным параметром *Точки подключения*.

Значение по умолчанию: **Отключено**.

Этот параметр работает только в том случае, если для восстановления выбрана папка, которая в иерархии папок находится выше точки подключения. Если для восстановления выбраны папки в точке подключения или сама точка подключения, выбранные элементы будут восстановлены независимо от значения параметра **Точки подключения**.

> **Примечание**
>
> Помните, что, если том не подключен в момент восстановления, данные будут восстановлены напрямую в папку, которая была точкой подключения во время резервного копирования.

Производительность

Этот параметр определяет приоритет процесса восстановления в операционной системе.

Доступные значения:

- **Низкий**: соответствует значению **Ниже среднего**.
- **Обычный**: соответствует значению **Обычный**.

- **Высокий**: соответствует значению **Высокий**.

Значение по умолчанию: **Обычный**.

Приоритет процесса, выполняющегося в системе, определяет количество выделенных ему ресурсов ЦП и системы. Понизив приоритет восстановления, можно освободить часть ресурсов для других приложений. Повышение приоритета восстановления может ускорить процесс восстановления за счет выделения операционной системой большего объема ресурсов приложению, выполняющему восстановление. Однако результат будет зависеть от общей загрузки процессора и других факторов, например скорости ввода-вывода диска и сетевого трафика.

Команды до и после процедуры

Этот параметр позволяет определить команды, которые должны выполняться автоматически перед выполнением процедуры восстановления данных и после нее.

Пример использования команд до и после процедуры:

- Запустите команду `Checkdisk`, чтобы найти и исправить логические ошибки файловой системы, физические ошибки или поврежденные сектора до запуска восстановления или после его окончания.

Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).

Команда после восстановления не будет выполнена, если восстановление заканчивается перезагрузкой.

Команда, выполняемая перед восстановлением

Чтобы указать команду или пакетный файл, выполняемый перед началом восстановления:

1. Включите переключатель **Выполнение команды до восстановления**.
2. В поле **Команда...** введите команду или найдите пакетный файл. Программа не поддерживает интерактивные команды, то есть те команды, которые требуют пользовательского ввода (например, pause).
3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите аргументы выполнения команды (если необходимо).
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	Выбор			
Прервать восстановление при сбое команды[1]	Установить	Снять	Установить	Снять
Не начинать восстановление до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	[По умолчанию] Выполнить восстановление только после успешного выполнения команды. Прервать восстановление при сбое команды.	Выполнить восстановление после выполнения команды независимо от результатов ее выполнения (успешно или ошибка).	—	Выполнить восстановление параллельно с выполнением команды независимо от результата ее выполнения.

Команда после восстановления

Чтобы указать команду или исполняемый файл, которые будут выполнены после завершения восстановления:

1. Включите переключатель **Выполнение команды после восстановления**.
2. В поле **Команда…** введите команду или найдите пакетный файл.
3. В поле **Рабочая папка** укажите путь к каталогу, в котором будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
5. Установите флажок **Прерывать восстановление при сбое команды**, если для вас важно успешное выполнение программы. Считается, что команда не выполнена, если код выхода не равен нулю. При сбое выполнения команды статусу восстановления будет задано значение **Ошибка**.

   Если флажок не установлен, результат выполнения команды не влияет на успешность выполнения восстановления. Можно отследить результат выполнения команды, изучив информацию на вкладке **Действия**.

[1] Команда считается сбойной, если код завершения не равен нулю.

6. Нажмите кнопку **Готово**.

Примечание

Команда после восстановления не будет выполнена, если восстановление заканчивается перезагрузкой.

Управление лентами

Можно использовать указанные ниже параметры восстановления управления лентами.

Использование кэша диска для ускорения восстановления

Значение по умолчанию: **Отключено**.

Настоятельно рекомендуем использовать параметр **Используйте кэш диска, чтобы ускорить восстановление** при восстановлении файлов из архива изображения. В противном случае операция восстановления может занять много времени. При использовании этого параметра лента читается последовательно без прерываний и перемоток.

Изменение идентификатора безопасности

Этот параметр действует при восстановлении ОС Windows Server 2012 R2 или более ранних версий.

Этот параметр не работает, если восстановление в виртуальную машину выполняется агентом для VMware или агентом для Hyper-V.

Значение по умолчанию: **Отключено**.

Это программное обеспечение может генерировать уникальный идентификатор безопасности (SID компьютера) для восстановленной операционной системы. Этот параметр требуется только для обеспечения работоспособности программного обеспечения сторонних производителей, в котором используется SID компьютера.

Корпорация Майкрософт не поддерживает официально изменение SID в развернутых или восстановленных системах. Это означает, что, используя этот параметр, вы принимаете на себя весь риск.

Управление питанием ВМ

Эти параметры применяются вне зависимости от типа агента при восстановлении на виртуальную машину.

Выключать целевые виртуальные машины при запуске восстановления

Значение по умолчанию: **Включено**.

Невозможно выполнить восстановление в существующую виртуальную машину, если она включена, поэтому машина выключается автоматически при запуске восстановления. Пользователи будут отключены от этой машины, а любые несохраненные данные потеряны.

Снимите флажок, соответствующий этому параметру, если предпочитаете вручную выключать виртуальные машины перед восстановлением.

Включите целевую виртуальную машину по окончании восстановления.

Значение по умолчанию: **Отключено**.

После восстановления машины из резервной копии на другой машине существует вероятность появления копии существующей машины в сети. На всякий случай включите восстановленную виртуальную машину вручную после принятия всех необходимых мер предосторожности.

Журнал событий Windows

Этот параметр работает только в ОС Windows.

Этот параметр указывает, должны ли агенты записывать события операций восстановления в журнал событий приложений Windows (чтобы просмотреть этот журнал, запустите файл eventvwr.exe или выберите **Панель управления** → **Администрирование** → **Просмотр событий**). События содержат статус и время завершения операции; события можно фильтровать.

Значение по умолчанию: **Отключено**.

> **Примечание**
>
> Параметр работает только для операций восстановления файлов (см. раздел *Восстановление файлов*).

Включить после восстановления

Этот параметр применим при работе с загрузочного носителя.

Значение по умолчанию: **Отключено**.

Этот параметр позволяет загрузить машину с восстановленной операционной системой без вмешательства пользователя.

Операции с резервными копиями

Подключение томов из резервной копии

Подключение томов из резервной копии на уровне дисков позволяет получить доступ к томам так же, как и к физическим дискам.

Подключение томов в режиме чтения/записи позволяет менять содержимое резервной копии, то есть сохранять, перемещать, создавать и удалять файлы или папки и запускать исполняемые сценарии, состоящие из одного файла. В этом режиме программное обеспечение создает инкрементную резервную копию, которая содержит изменения, внесенные в содержимое резервной копии. Помните, что ни одного из этих изменений не будет в последующих резервных копиях.

Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, которая выполняет операцию подключения, должен быть установлен агент для Windows.
- Файловая система, для которой создана резервная копия, должна поддерживаться в той версии Windows, которая выполняется на данной машине.
- Резервная копия должна хранится в локальной папке, сетевой папке (SMB/CIFS) или в Зоне безопасности.

Сценарии использования

- **Предоставление общего доступа к данным**

  Можно предоставить общий доступ к подключенным томам по сети.

- **Временное решение по восстановлению базы данных**

  Подключите том, который содержит базу данных SQL, из вышедшей недавно из строя машины. Это предоставит доступ к базе данных до восстановления этой машины. Этот подход можно использовать для фрагментарного восстановления данных Microsoft SharePoint, используя SharePoint Explorer.

- **Обработка ошибок**

  Сбой восстановления с возможностью восстановления размера тома может происходить по причине ошибки в файловой системе, для которой создана резервная копия. Подключите

резервную копию в режиме чтения/записи. После этого проверьте подключенный том на наличие ошибок, используя команду **chkdsk /r**. После исправления ошибок и создания новой инкрементной резервной копии восстановите систему из этой резервной копии.

Порядок подключения тома из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щёлкните файл резервной копии. По умолчанию файлы имеют имена на основе следующего шаблона: `<имя машины> - <GUID плана защиты>`
3. Если резервная копия защищена паролем, укажите его. В противном случае пропустите этот шаг.

   В проводнике отображаются точки восстановления.
4. Дважды щёлкните точку восстановления.

   В проводнике отображаются тома, для которых созданы резервные копии.

   > **Примечание**
   >
   > Дважды щёлкните том для обзора его содержимого. Можно скопировать файлы и папки из резервной копии в любую папку в файловой системе.

5. Правой кнопкой мыши щёлкните том для подключения, затем выберите один из следующих пунктов меню:
   - **Подключить**
   - **Подключить в режиме ”только чтение”**
6. Если резервная копия хранится в сетевой папке, укажите учетные данные для доступа. В противном случае пропустите этот шаг.

   Программа подключит выбранный том. Данному тому назначается первая неиспользованная буква.

Порядок отключения тома

1. В проводнике откройте **Этот компьютер**.
2. Правой кнопкой мыши щёлкните подключенный том.
3. Нажмите **Отключить**.
4. Если том подключен в режиме чтения/записи и его содержимое было изменено, выберите, создавать ли инкрементную резервную копию с этими изменениями. В противном случае

пропустите этот шаг.

Программа отключит выбранный том.

Экспорт резервных копий

При экспорте в указанном хранилище создается самодостаточная копия резервной копии. Исходная резервная копия остается без изменений. Экспорт позволяет выделить определенную резервную копию из цепочки инкрементных и дифференциальных резервных копий для быстрого восстановления и записать ее на съемный носитель для использования в других целях.

Результатом операции экспорта всегда является полная резервная копия. Чтобы выполнить репликацию всей цепочки резервных копий в другое хранилище и сохранить несколько точек восстановления, используйте *план репликации резервных копий*.

Имя файла экспортированной резервной копии зависит от значения параметра *формат резервной копии*:

- Для формата **Версия 12** с любой схемой резервного копирования имя файла резервной копии будет таким же, как и имя файла оригинальной резервной копии, плюс порядковый номер. Если несколько резервных копий одной цепочки экспортируются в одно хранилище, имена файлов (за исключением первого) в конце дополняются порядковым номером из четырех цифр.
- Для формата **Версии 11** со схемой резервного копирования **Всегда инкрементное** имя файла резервной копии в точности соответствует имени файла исходной резервной копии. Если несколько резервных копий одной цепочки экспортируются в одно хранилище, то каждая операция экспорта перезаписывает ранее экспортированную резервную копию.
- Для формата **Версия 11** с другими схемами резервного копирования имя файла резервной копии будет таким же, как и имя файла оригинальной резервной копии, плюс метка времени. Метки времени экспортированных резервных копий соответствуют времени выполнения экспорта.

Экспортированная резервная копия наследует настройки защиты паролем и сам пароль от исходной резервной копии. При экспорте защищенной резервной копии необходимо указать пароль.

Порядок экспорта резервной копии

1. Выберите машину, для которой есть резервная копия.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните любое из следующих

действий:

- Если резервная копия расположена в общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щёлкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
- Выберите точку восстановления на вкладке *Хранилища резервных копий*.

4. Щёлкните значок шестерни, затем щёлкните **Экспорт**.
5. Выберите агент, который будет выполнять экспорт.
6. Если резервная копия защищена паролем, укажите его. В противном случае пропустите этот шаг.
7. Укажите место сохранения экспорта.
8. Нажмите кнопку **Запустить**.

Удаление резервных копий

Предупреждение

При удалении резервной копии все ее данные удаляются окончательно. Удаленные данные невозможно восстановить.

Порядок удаления резервных копий машины, которая включена и присутствует в веб-консоли Кибер Бэкап

1. На вкладке **Физические и виртуальные машины** выберите машину, резервные копии которой необходимо удалить.
2. Щёлкните **Восстановление**.
3. Выберите хранилище, в котором расположены резервные копии для удаления.
4. Выполните одно из следующих действий:
   - Чтобы удалить одну резервную копию, выберите резервную копию для удаления, щёлкните значок шестерни и выберите пункт **Удалить**.
   - Чтобы удалить все резервные копии в выбранном хранилище, щёлкните **Удалить все**.
5. Подтвердите операцию.

Порядок удаления резервных копий любой машины

1. На вкладке **Хранилища резервных копий** выберите хранилище, из которого необходимо удалить резервные копии.

   В программном обеспечении отображаются все резервные копии, которые разрешено просматривать в выбранном хранилище для вашей учетной записи. Резервные копии объединены по группам. Группы имеют имена на основе следующего шаблона: `<имя машины> - <имя плана защиты>`

2. Выберите группу.
3. Выполните одно из следующих действий:
   - Чтобы удалить одну резервную копию, щёлкните **Показать резервные копии**, выберите резервную копию для удаления, щёлкните значок шестерни и выберите пункт **Удалить**.
   - Чтобы удалить выбранную группу, щёлкните **Удалить**.
4. Подтвердите операцию.

Обработка данных вне хоста (off-host)

Большинство действий, предусмотренных в плане резервного копирования, например, репликация, проверка и применение правил хранения, выполняются агентом резервного копирования. Это увеличивает рабочую нагрузку на машину, на которой запущен агент, даже после завершения процесса резервного копирования.

Разграничение планов репликации, проверки, очистки и преобразования резервных копий в виртуальные машины повышает гибкость и предоставляет следующие возможности:

- выбор другого агента/агентов для выполнения таких операций;
- планирование выполнения таких операций на часы наименьшей загрузки для снижения использования полосы пропускания;
- перенесение выполнения таких операций на нерабочие часы, если в ваши планы не входит установка выделенного агента для обработки данных.

Если вы используете узел хранения, то для обработки данных вне хоста можно использовать выделенный агент, поставляемый в комплекте с узлом хранения.

В отличие от планов резервного копирования и репликации ВМ, которые используют настройки времени, заданные на машинах с агентами, планы обработки данных вне хоста запускаются в соответствии с настройками времени на машине сервера управления.

Репликация резервных копий

При применении плана репликации к резервной копии, разделенной на фиксированные фрагменты (см. раздел *Деление*), реплицированная копия объединяется в общий архив.

Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами репликации резервных копий.

Источник репликации	**Целевое хранилище репликации**							
	Локальная папка	**Хранилище под управлением узла хранения**			**Сетевая папка**	**Папка NFS**	**SFTP-сервер**	**Кибер Инфраструктура или Кибер Хранилище**
		с дедупликацией	**без дедупликации**	**с лентами**				
Локальная папка	+	+[1]	+	+	+	—	—	+
Сетевая папка	+	+[с. 488, 1]	+	+	+	—	—	+
Хранилище под управлением узла хранения с дедупликацией	+	+[с. 488, 1]	+	+	+	—	—	—
Хранилище под управлением узла хранения без дедупликации	+	+[с. 488, 1]	+	+	+	—	—	+
Хранилище под управлением узла хранения с лентами	+	+[с. 488, 1]	+	+	+	—	—	+
Зона безопасности	+	+[с. 488, 1]	+	+	+	—	—	+
Папка NFS	—	—	—	—	—	—	—	—
SFTP-сервер	—	—	—	—	—	—	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Источник репликации	Целевое хранилище репликации							
	Локальная папка	Хранилище под управлением узла хранения			Сетевая папка	Папка NFS	SFTP-сервер	Кибер Инфраструктура или Кибер Хранилище
		с дедупликацией	без дедупликации	с лентами				
Кибер Инфраструктура или Кибер Хранилище	+	—	+	+	+	—	—	+

Формат архива ”Версия 11” не поддерживается в хранилищах Кибер Инфраструктура и Кибер Хранилище.

Примечание

Хранилище под управлением узла хранения с включённой дедупликацией не рекомендуется использовать для постоянной репликации. Дедупликация является длительным и ресурсоёмким процессом, который может привести к снижению скорости репликации, если в качестве источника реплицируемых данных используется хранилище под управлением узла хранения с дедупликацией.

Дополнительные условия использования хранилища под управлением узла хранения см. в разделе *Замечания по использованию узла хранения*.

Порядок создания плана репликации резервных копий

Для создания плана репликации резервных копий выполните следующие действия:

1. Щёлкните **Планы** → **Репликация резервной копии**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. Щёлкните **Агент**, а затем выберите агента, который выполнит репликацию.

[1] Только для резервных копий формата ”Версия 11”. Подробнее о форматах резервных копий см. раздел *Формат резервной копии*.

Можно выбрать любого агента, который имеет доступ к источнику и месту сохранения хранилища резервной копии.

5. Щёлкните **Элементы для репликации** и выберите резервные копии для репликации этим планом.

   Используя переключатель **Расположения** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.

6. Щёлкните **Место сохранения** и укажите место сохранения.
7. [Дополнительно] В разделе **Порядок преобразования** выберите резервные копии для репликации. Можно выбрать один из следующих вариантов:
   - **все резервные копии** (по умолчанию),
   - **только полные резервные копии**,
   - **только последняя резервная копия**.
8. [Дополнительно] Щёлкните **Расписание**, а затем измените расписание.
9. [Необязательно] Щёлкните **Правила хранения**, а затем укажите правила хранения для целевого расположения, как описано в разделе *Правила хранения*.
10. Если резервные копии, выбранные в **Элементы для репликации**, защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
11. [Дополнительно] Для изменения параметров плана щёлкните значок шестеренки.
12. Нажмите кнопку **Создать**.

Проверка резервных копий

Проверка — это операция по определению возможности восстановления данных из резервной копии.

Проверка хранилища резервных копий проверяет все резервные копии, расположенные в хранилище.

Методы проверки резервных копий

В планах проверки предусмотрено два метода проверки резервных копий. Если выбрать оба метода, операции будут выполняться последовательно.

- **Вычисление контрольной суммы для каждого блока данных, сохранённого в резервной копии**

Дополнительную информацию о проверке путём определения контрольной суммы см. в разделе *Проверка резервных копий*.

- **Запуск виртуальной машины из резервной копии**

  Этот метод работает только для резервных копий дисков, содержащих операционную систему (Windows или Linux). Резервная копия может быть создана на физическом сервере или на виртуальном сервере поддерживаемой среды виртуализации. Чтобы использовать этот метод, необходимо иметь хост ESXi или Hyper-V и агент защиты (агент для VMware или агент для Hyper-V соответственно), который управляет этим хостом. В этой среде будет запущена виртуальная машина из проверяемой резервной копии.

  Агент запускает виртуальную машину из резервной копии и подключается к VMware Tools или службе Hyper-V Heartbeat для проверки успешности запуска операционной системы. При сбое подключения агент пытается подключиться каждые две минуты. Всего предпринимается пять попыток подключения. Если ни одна из попыток не будет успешной, проверка завершится сбоем, подробные сведения будут доступны во вкладке **Панель мониторинга** → **Действия**.

  Независимо от количества планов проверки и проверенных резервных копий агент, который выполняет планы проверки, одновременно запускает одну виртуальную машину. При этом добавляемые к запускаемой машине диски подключаются напрямую из хранилища резервных копий без переноса в среду виртуализации. Как только результат проверки становится известным, агент удаляет виртуальную машину и запускает следующую.

Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами проверки.

Хранилище резервных копий	**Вычисление контрольной суммы**	**Запуск виртуальной машины**
Локальная папка	+	+
Сетевая папка	+	+
Папка NFS	—	—
Зона безопасности	—	—
Сервер SFTP	—	—
Управляемое хранилище	+	+
Ленточное устройство	+	—
Кибер Инфраструктура или Кибер Хранилище	+	+

Порядок создания нового плана проверки

1. Нажмите **Планы** → **Проверка**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана проверки нажмите на имя по умолчанию, далее в открывшемся окне введите новое имя и нажмите **ОК**.
4. Щёлкните **Агент**, а затем выберите агент, который выполнит проверку, и нажмите **ОК**.

   Для удобства воспользуйтесь поиском по имени агента, введя его имя в соответствующее поле.

   Для настройки отображаемых столбцов с информацией об агентах нажмите на значок шестерёнки и установите флажки для отображаемых столбцов.

   Для выполнения проверки посредством запуска виртуальной машины из резервной копии выберите агент для VMware или агент для Hyper-V. В противном случае выберите любой агент, который зарегистрирован на сервере управления и имеет доступ к хранилищу резервной копии.
5. Щёлкните **Элементы для проверки** и выберите резервные копии для проверки этим планом.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.
6. [Необязательно] В **Объект проверки**, выберите резервные копии для проверки. Можно выбрать один из следующих вариантов:
   - **Все резервные копии**;
   - **Только последняя резервная копия**.
7. [Необязательно] Нажмите **Порядок проверки** и затем выберите метод, переведя соответствующий переключатель в положение **Вкл** (можно выбрать оба метода):
   - **Проверка контрольной суммы**

     Программное обеспечение вычислит контрольную сумму для каждого блока данных резервной копии.
   - **Запустить как виртуальную машину**

     Программное обеспечение запустит виртуальную машину из каждой резервной копии.
8. Если выбран вариант **Запустить как виртуальную машину**, дополнительно выполните

следующие шаги:

1. Щёлкните **Целевая машина** и выберите тип виртуальной машины (ESXi или Hyper-V), хост и шаблон имени машины.

   По умолчанию установлено имя **[Machine Name]_validate**.

2. Нажмите **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.

3. Для получения результата проверки используется параметр **Сигнал пульса ВМ**, который получает состояние пульса виртуальный машины от гостевой операционной системы через инструментарий гипервизора (VMware Tools или Hyper-V Integration Services). Параметр включен по умолчанию и не может быть выключен.

4. [Необязательно] Щёлкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.

   > **Примечание**
   >
   > По умолчанию виртуальная машина *не* подключена к сети, а размер памяти виртуальной машины соответствует размеру памяти оригинальной машины. При необходимости подключения виртуальной машины к сети будьте осторожны во избежание создания помех другим машинам.

9. [Необязательно] Щёлкните **Расписание**, а затем укажите требуемые параметры расписания и нажмите **Готово**.

10. Если резервные копии, выбранные в разделе **Элементы для проверки**, защищены паролем, установите пароль, щёлкнув по переключателю **Пароль резервной копии**. В противном случае пропустите этот шаг.

11. [Необязательно] Для настройки действий при сбое плана щёлкните значок шестерёнки, выберите **Действие при сбое плана** и установите требуемые параметры, после чего нажмите **Готово**.

12. [Необязательно] Для настройки команд, которые должны выполняться до или после плана проверки, щёлкните значок шестерёнки, выберите **Команды до и после** и установите требуемые параметры, после чего нажмите **Готово**.

13. [Необязательно] Для настройки повторного выполнения плана проверки в случае сбоев щёлкните значок шестерёнки, выберите **Обработка ошибок** и установите требуемые параметры, после чего нажмите **Готово**.

14. [Необязательно] Для настройки приоритета резервного копирования щёлкните значок шестерёнки,

выберите **Производительность** и установите требуемые параметры, после чего нажмите **Готово**.

15. Нажмите кнопку **Создать**.

В результате выполненных действий план проверки будет создан, а его имя будет отображено в списке **Планы проверки**.

Порядок проверки резервных копий

Проверка резервных копий с использованием созданного плана проверки может быть выполнена:

- по расписанию;
- по требованию (доступно как для планов с настроенным расписанием, так и без него).

Проверка резервных копий по расписанию

При выполнении проверки по расписанию процесс будет выполняться автоматически в заданнное время.

Для просмотра результатов проверки перейдите в **Планы** → **Проверка**, выберите план проверки и щёлкните **Действия**.

Проверка резервных копий по требованию

Чтобы выполнить проверку резервной копии по требованию, выполните следующие действия:

1. Щёлкните **Планы** → **Проверка**.
2. Выберите в списке план проверки.
3. На панели **Действия** нажмите **Запустить сейчас**.

В результате выполненных действий будет начат процесс проверки резервных копий в соответствии с используемым планом.

Для просмотра статуса выполнения проверки щёлкните **Действия**. В случае возникновения ошибок соответствующие сообщения будут отображены в этом разделе.

Очистка от устаревших резервных копий

Очистка — это операция, которая удаляет устаревшие резервные копии в соответствии с правилами хранения.

Поддерживаемые расположения

Планы очистки поддерживаются всеми хранилищами резервных копий, за исключением папок NFS, SFTP-серверов и Зона безопасности.

Порядок создания нового плана очистки

1. Щёлкните **Планы** → **Очистка**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. Щёлкните **Агент**, а затем выберите агента, который будет выполнять очистку.

   Можно выбрать любой агент, который имеет доступ к расположению резервного копирования.
5. Щёлкните **Элементы для очистки**, затем выберите резервные копии, которые будут очищены этим планом.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.
6. [Дополнительно] Щёлкните **Расписание**, а затем измените расписание.
7. [Дополнительно] Щёлкните **Правило хранения**, а затем укажите правила хранения, как описано в разделе *Правила хранения*.
8. Если резервные копии, выбранные в **Элементы для очистки** защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
9. [Дополнительно] Для изменения параметров плана щёлкните значок шестеренки.
10. Нажмите кнопку **Создать**.

Преобразование резервных копий в виртуальные машины

Можно создать отдельный план для преобразования резервной копии в виртуальную машину и запустить его вручную или по расписанию.

Информацию о предварительных требованиях и ограничениях см. в разделе *Преобразование в виртуальную машину*.

Порядок создания плана для преобразования в виртуальную машину

1. Щёлкните **Планы** → **Преобразование в ВМ**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. В поле **Преобразовать в** выберите тип целевой виртуальной машины. Для этого укажите Учетная запись для входа службы агента. Можно выбрать один из следующих вариантов:

   - VMware ESXi
   - Microsoft Hyper-V
   - VMware Workstation
   - Файлы VHDX

   > **Примечание**
   >
   > Для экономии дискового пространства при каждом преобразовании в файлы VHDX выполняется перезапись файлов VHDX в целевом расположении, созданном при предыдущем преобразовании.

5. Выполните одно из следующих действий:

   - Для VMware ESXi и Hyper-V: щёлкните **Хост**, выберите целевой хост, а затем укажите новый шаблон имени машины.
   - Для виртуальных машин других типов: в поле **Путь** укажите расположение для сохранения файлов виртуальной машины и шаблон имени файла.

   Имя по умолчанию — **[Имя машины]_converted**.
6. Щёлкните **Агент**, а затем выберите агент, который выполнит преобразование.
7. Щёлкните **Элементы для преобразования**, выберите резервные копии, которые данный план преобразует в виртуальные машины.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии защищены паролем, пароль для всех должен быть одинаков. Для резервных копий, для которых используются разные пароли, создайте отдельные планы.

8. [Только для VMware ESXi и Hyper-V] Щёлкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
9. [Необязательно] Для VMware ESXi и Hyper-V можно также выполнить следующие действия:
    - Измените режим распределения ресурса дисков. По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
    - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щёлкните **Настройки ВМ**.
10. [Дополнительно] Щёлкните **Расписание**, а затем измените расписание.
11. Если резервные копии, выбранные в **Элементы для преобразования** защищены паролем, включите переключатель **Пароль резервной копии** и укажите пароль. В противном случае пропустите этот шаг.
12. [Дополнительно] Для изменения параметров плана щёлкните значок шестеренки.
13. Нажмите кнопку **Создать**.

Вкладка ”Планы”

При наличии лицензии Кибер Бэкап расширенная редакция планами защиты и прочими планами можно управлять на вкладке **Планы**.

Каждый раздел вкладки **Планы** содержит все планы конкретного типа. Доступны следующие разделы:

- *Защита*
- *Репликация резервной копии*
- *Проверка*
- *Очистка*
- *Преобразование в ВМ*
- *Репликация ВМ*
- *Загрузочный носитель* — в этом разделе показаны планы защиты, которые созданы для машин, загружаемых с загрузочных носителей, и применяются только к этим машинам.

На вкладке **Планы** также можно выполнять операции с планами. В каждом разделе вкладки можно создавать, редактировать, отключать, включать, удалять, запускать и отслеживать выполнение плана.

Список действий с планами находится в меню справа. По умолчанию из этого меню вы можете:

Создать план - создает план защиты с выбранными параметрами;

Импорт - позволяет импортировать план из файла;

Для просмотра свойств и настройки уже существующего плана отметьте нужный план в списке планов. Справа появится дополнительное меню действий с планами. В меню содержатся следующие пункты:

- **Сведения** — показывает сведения о выбранном плане;
- **Остановить** — позволяет остановить выполнение выбранного плана;
- **Изменить** — позволяет изменить параметры выбранного плана;
- **Действия** — предоставляет сведения о действиях с выбранным планом;
- **Оповещения** — предоставляет список оповещений относительно выбранного плана;
- **Клонировать** — позволяет применить выбранный план вместе с параметрами к другому устройству;
- **Экспорт** — позволяет сохранить план в файл;
- **Отключить** (**Включить**) — отключает (включает) план;

- **Удалить** — удаляет план.

Подробнее об этом см. в разделе *Операции с планами защиты*.

Клонирование и остановка доступны только для планов защиты. В отличие от остановки резервного копирования на вкладке **Устройства**, при остановке плана защиты будут остановлены процессы создания резервных копий на всех устройствах, к которым он применен.

Также возможно экспортировать план в файл и импортировать предварительно экспортированный план.

Вкладка ”Хранилища резервных копий”

На вкладке **Хранилища резервных копий** показаны резервные копии всех машин, которые когда-либо были зарегистрированы на сервере управления. Сюда входят отключенные машины и машины, которые больше не зарегистрированы.

Резервные копии, которые хранятся в общем расположении (например на общем ресурсе SMB или NFS) видимы всем пользователям, которые имеют разрешение на чтение в данном расположении.

В ОС Windows файлы резервных копий наследуют разрешения на доступ от родительской папки. Поэтому мы рекомендуем ограничить разрешения на чтение для этой папки.

Хранилища резервных копий, которые используются в планах защиты, автоматически добавляются на вкладку **Хранилища резервных копий**. Чтобы добавить хранилище, а также локальную или сетевую папку, узел хранения, Кибер Инфраструктуру и прочее, щёлкните **Добавить хранилище** и следуйте инструкции.

⚠ Предупреждение

Не пытайтесь редактировать файлы резервной копии вручную, поскольку это может привести к повреждению файла и сделать резервные копии нестабильными. Кроме того, мы рекомендуем экспортировать резервные копии или реплицировать их, а не перемещать их файлы вручную.

Порядок выбора точки восстановления на вкладке ”Хранилища резервных копий”

1. На вкладке **Хранилища резервных копий** выберите хранилище резервных копий.

   В программном обеспечении отображаются все резервные копии, которые разрешено просматривать в выбранном хранилище для вашей учетной записи. Резервные копии объединены по группам. Группы имеют имена на основе следующего шаблона: `<имя машины> - <имя плана защиты>`

2. Выберите группу, с которой необходимо восстановить данные.

3. [Необязательно] Щёлкните **Изменить** рядом с полем **Машина для обзора** и выберите другую машину. Обзор некоторых резервных копий могут выполнить только определенные агенты. Например, чтобы просмотреть резервные копии баз данных Microsoft SQL Server, необходимо выбрать машину с запущенным агентом для SQL.

Важно

Имейте в виду, что расположение, указанное в поле **Машина для обзора**, является расположением по умолчанию для восстановления с резервной копии физической машины. После того как вы выберете точку восстановления и щёлкните **Восстановление**, дважды проверьте настройку **Целевая машина**, чтобы убедиться в правильности указанной машины, в которую будут выполнено восстановление. Чтобы изменить целевое место восстановления, укажите другую машину в поле **Машина для обзора**.

4. Щёлкните **Показать резервные копии**.
5. Выберите точку восстановления.

Примечание

Точку восстановления можно также выбрать, нажав **Устройства** → **<устройство>** → **Восстановление** (см. *Восстановление*).

Загрузочный носитель

Загрузочный носитель представляет собой физический носитель (компакт-диск, DVD-диск, флеш-накопитель USB или другой съемный носитель, распознаваемый BIOS машины в качестве загрузочного устройства), который позволяет запускать агент Кибер Бэкап в среде Linux или среде предустановки Windows (WinPE) без помощи операционной системы.

Загрузочный носитель чаще всего используется в следующих случаях:

- Восстановление операционной системы, которая не может запуститься.
- Доступ к данным, сохранившимся после повреждения системы и их резервного копирования.
- Развертывание операционной системы на ”голое железо”.
- Создание базовых или динамических томов на ”голом железе”.
- Посекторное резервное копирование диска с неподдерживаемой файловой системой.
- Резервное копирование в автономном режиме любых данных, которые не удалось скопировать в онлайн-режиме, например, из-за блокировки запущенным приложением или ограничения доступа.

Кроме того, машину можно загрузить с использованием сетевой загрузки с помощью PXE-сервера Киберпротект, службы развертывания Windows (WDS) или службы удаленной установки (RIS). Эти серверы с загружаемыми загрузочными компонентами также могут рассматриваться как один из видов загрузочных носителей. С помощью одного мастера можно создать загрузочный носитель, настроить PXE-сервер или службы WDS/RIS.

Создание загрузочных носителей

Используя *мастер создания загрузочных носителей*, можно создать собственный загрузочный носитель (*на основе Linux* или *на основе WinPE*) для компьютеров Windows или Linux. Чтобы создать полнофункциональный загрузочный носитель, необходимо указать лицензионный ключ Кибер Бэкап. Если не указать этот ключ, с загрузочного носителя можно будет выполнить только операции восстановления.

Примечание

Загрузочный носитель не поддерживает гибридные диски.

Кроме того, можно скачать готовый загрузочный носитель (только на основе Linux) с веб-сайта Киберпротект. Скачанный загрузочный носитель можно использовать только для операций

восстановления и доступа к инструменту Универсальное восстановление (Universal Restore). Вы не сможете создавать резервные копии данных, проверять или экспортировать резервные копии, выполнять операции управления дисками или использовать сценарии с ними.

Примечание

Готовый загрузочный носитель не поддерживает узел хранения, хранилища на ленте и хранилища SFTP. Если вы намерены использовать эти хранилища, необходимо будет создать собственный загрузочный носитель, используя для этого мастер создания загрузочных носителей.

Можно записать скачанный ISO-файл на CD/DVD-диск или создать загрузочный флэш-накопитель USB, используя один из бесплатных инструментов, доступных в Интернете. Для машин с UEFI используйте `ISO to USB` или `RUFUS`, для машин с BIOS —`Win32DiskImager`. В Linux можно воспользоваться утилитой `dd`.

Выбор среды загрузочного носителя

На основе Linux

Загрузочный носитель на основе Linux содержит загружаемый агент Кибер Бэкап на основе ядра Linux. Этот агент может выполнять загрузку и операции на любом PC-совместимом оборудовании, включая ”голое железо” и машины с поврежденными или неподдерживаемыми файловыми системами. Операции можно настраивать и контролировать в локальном или удаленном режиме в веб-консоли Кибер Бэкап.

На основе WinPE

Загрузочный носитель на основе WinPE содержит минимальную систему Windows, которая называется среда предустановки Windows (WinPE), и подключаемый модуль Киберпротект для WinPE, то есть модификацию агента Кибер Бэкап, запускаемую в среде предустановки.

WinPE — самое удобное загрузочное решение в больших средах с разнообразным оборудованием.

Преимущества:

- Использование Кибер Бэкап в среде предустановки Windows предоставляет больше возможностей, чем применение загрузочного носителя на основе Linux. После загрузки среды WinPE на ПК-совместимом оборудовании можно использовать не только агент Кибер Бэкап, но и команды и сценарии PE и другие подключаемые модули, добавленные в среду PE.
- С помощью загрузочного носителя на основе PE удается решить некоторые проблемы, свойственные загрузочным носителям Linux, например поддержку определенных RAID-контроллеров или только определенных уровней RAID-массивов. Носители на основе WinPE 2.x и последующих версий позволяют динамическую загрузку необходимых драйверов устройств.

Ограничения:

- загрузочные носители на основе версий WinPE ниже 4.0 не позволяют выполнять начальную загрузку компьютеров, на которых используется единый интерфейс EFI (UEFI).
- При загрузке машины с загрузочного носителя для среды PE невозможно выбрать в качестве места сохранения резервной копии оптический носитель, например CD, DVD или диск Blu-ray (BD).

Мастер создания загрузочных носителей

Мастер создания загрузочных носителей — это специальное средство для создания загрузочных носителей.

Мастер создания загрузочных носителей устанавливается по умолчанию при установке сервера управления. Его можно установить отдельно на любой машине с ОС Windows или Linux. Поддерживаются те же операционные системы, что и для соответствующих агентов.

В большинстве случаев для загрузки машины, которая использует интерфейс UEFI, требуется 64-разрядный носитель.

Цели использования мастера создания носителей

Готовый загрузочный носитель, доступный для скачивания на веб-сайте Киберпротект, можно использовать только для восстановления. Этот носитель основан на ядре Linux. В отличие от среды Windows PE, он не позволяет вводить пользовательские драйверы на лету.

- С помощью мастера создания загрузочных носителей можно создавать настраиваемые полнофункциональные загрузочные носители *на основе Linux* или *WinPE* с функциями резервного копирования.
- Помимо создания физического загрузочного носителя, можно передать его компоненты в службах развертывания Windows (WDS) и использовать загрузку по сети.
- Готовый загрузочный носитель не поддерживает узел хранения, хранилища на ленте и хранилища SFTP. Если вы намерены использовать эти хранилища, необходимо будет создать собственный загрузочный носитель, используя для этого мастер создания загрузочных носителей.

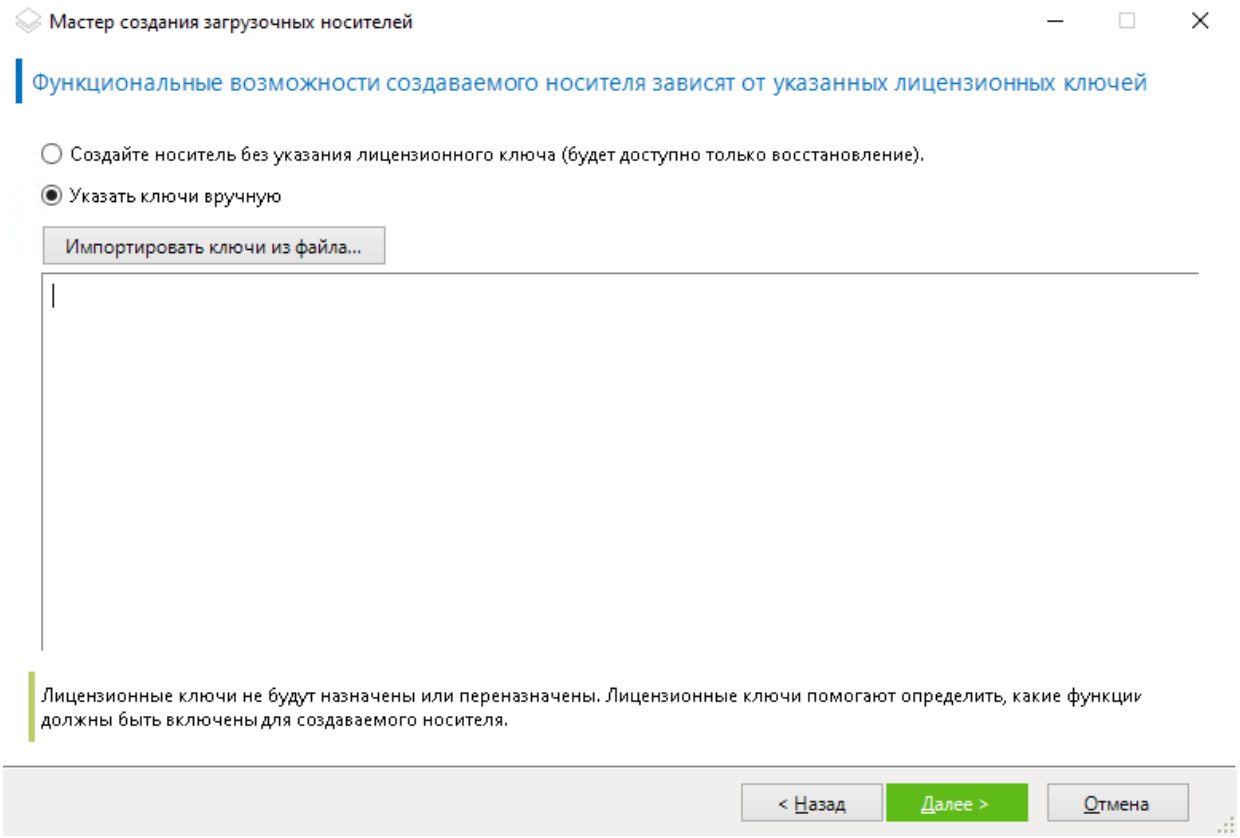
Загрузочные носители на основе Linux

Как создать загрузочный носитель на основе Linux

1. Запустите **Мастер создания загрузочных носителей**.
2. Чтобы создать полнофункциональный загрузочный носитель, укажите лицензионный ключ Кибер Бэкап. Этот ключ используется для определения функций, которые будут представлены на

загрузочном носителе. Лицензии не будут отзываться.

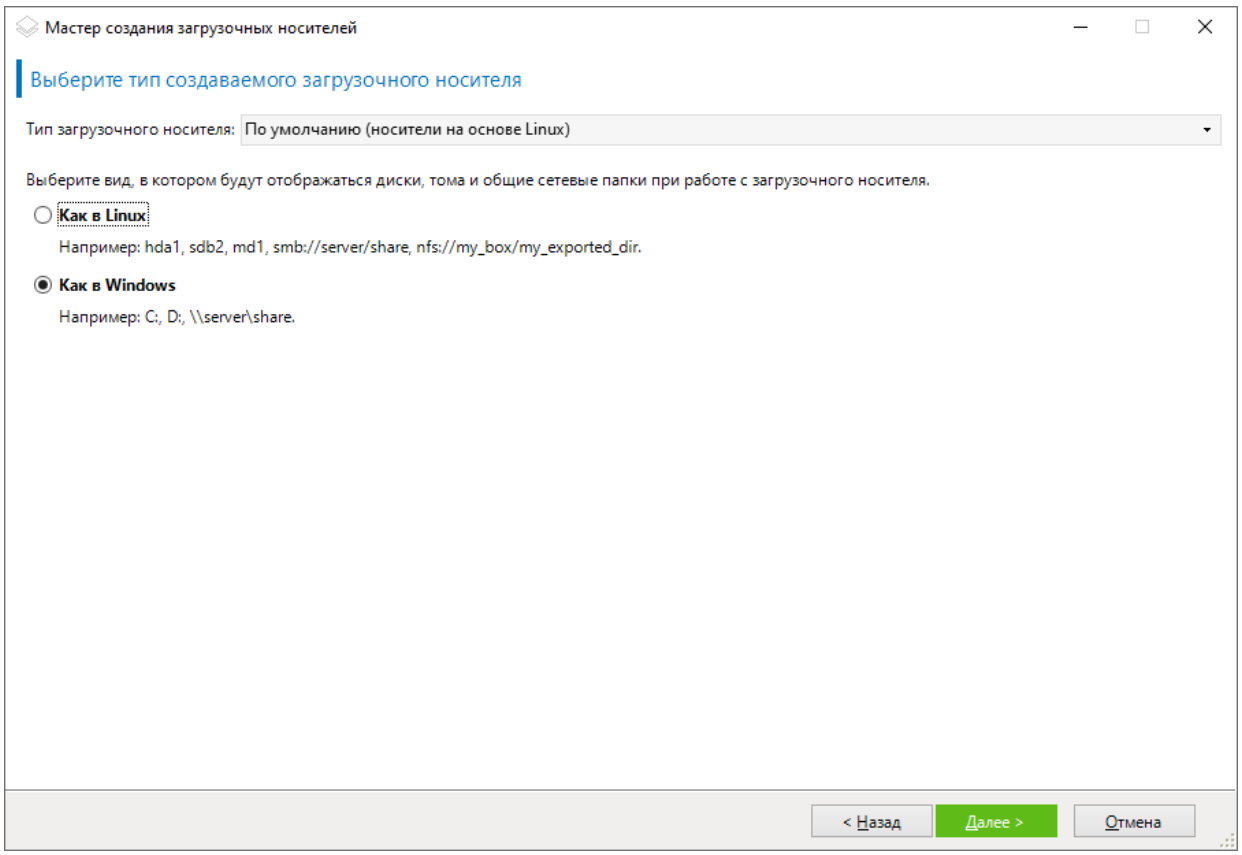
Если не указать лицензионный ключ, полученный загрузочный носитель можно использовать только для операций восстановления и доступа к компоненту Универсальное восстановление (Universal Restore).



3. Выберите **Тип загрузочного носителя: По умолчанию (носители на основе Linux)**.

   Выберите способ представления томов и сетевых ресурсов:

   - На носителе с представлением томов по типу Linux тома отображаются как, например, hda1 и sdb2. Перед началом восстановления предпринимается попытка реконструировать MD-устройства и LVM (диспетчер логических томов).
   - На носителе с представлением томов по типу Windows тома отображаются как, например, C: и D:. Он обеспечивает доступ к динамическим томам (LDM).

4. 

5. [Необязательно] Укажите параметры ядра Linux. Несколько параметров разделяются пробелами.

   Например, чтобы включить выбор режима дисплея для загрузочного агента при каждом запуске носителя, введите: `vga=ask`.

   Дополнительную информацию о доступных параметрах см. в разделе *Параметры ядра*.

6. [Дополнительно] Выберите язык, который будет использоваться в загрузочном носителе.

7. Выберите компоненты, которые будут размещены на носителе: загрузочный агент Кибер Бэкап и (или) Универсальное восстановление (Universal Restore), если вы планируете восстанавливать систему на отличающееся оборудование.

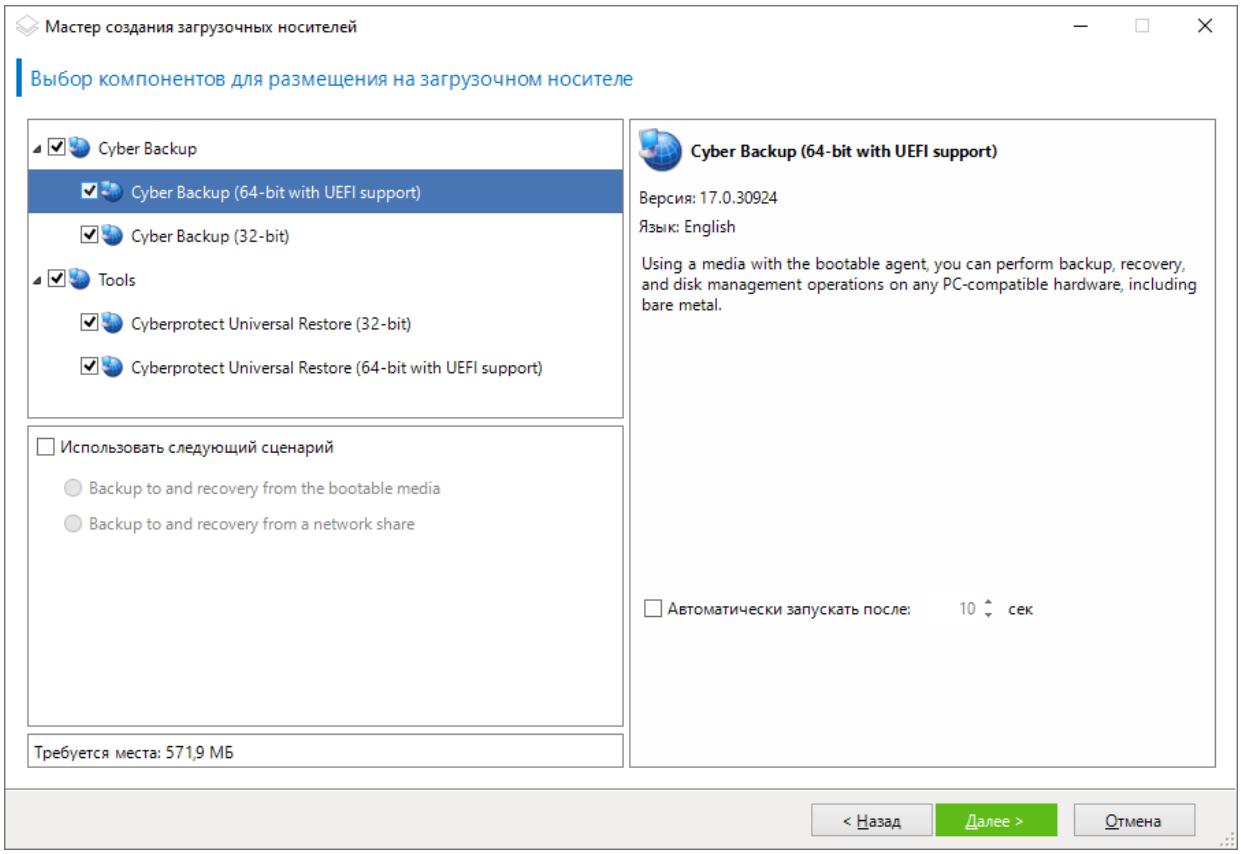
   Загрузочный агент позволяет выполнить операции резервного копирования, восстановления и управления дисками на любом ПК-совместимом оборудовании, включая ”голое железо”.

   Компонент Универсальное восстановление (Universal Restore) позволяет загружать операционную систему, восстановленную на отличающееся оборудование или на виртуальную машину. Этот инструмент находит и устанавливает драйверы для устройств, необходимых для запуска операционной системы, таких как контроллеры памяти, системная плата или набор микросхем.

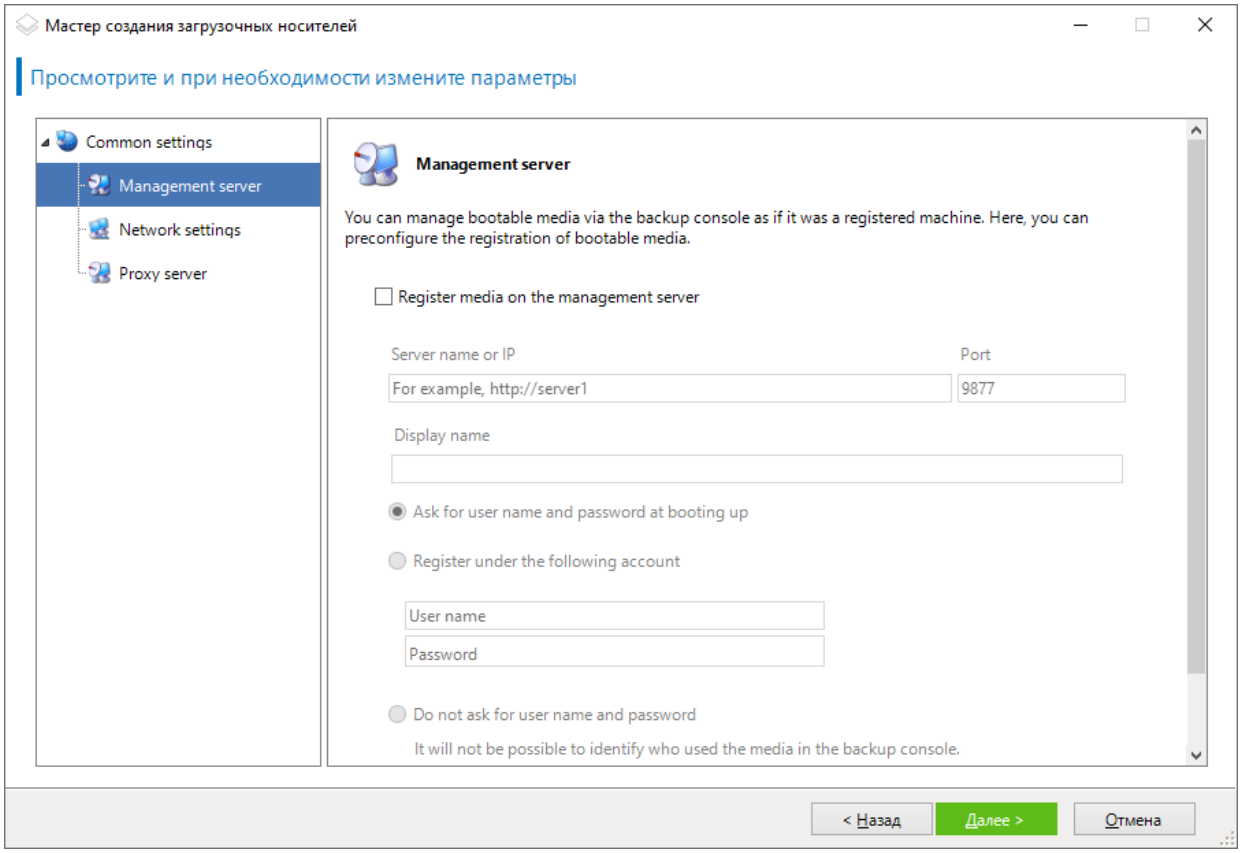
8. [Необязательно] Укажите время ожидания для меню загрузки и компонент, который будет автоматически запускаться по истечении этого времени. Для этого щёлкните нужный компонент в

левой верхней панели и задайте интервал для него. Это позволяет автоматически выполнять операции на рабочем месте при загрузке из WDS или RIS.

Если эта настройка не задана, загрузчик ждет, пока вы выберете, загружать ли операционную систему (если есть) или компонент.



9. [Необязательно] Чтобы автоматизировать операции загрузочного агента, установите флажок **Использовать следующий сценарий**. Затем выберите *один из сценариев* и задайте его параметры.
10. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительную информацию о настройках регистрации см. в разделе *Сервер управления*.



11. [Необязательно] Укажите *сетевые настройки*: настройки TCP/IP для назначения сетевым адаптерам машины.
12. [Необязательно] Укажите *сетевой порт*: TCP-порт, который прослушивается загрузочным агентом для приема входящих подключений.
13. [Необязательно] Если в сети включен прокси-сервер, укажите его имя хоста или IP-адрес и порт.
14. Выберите тип носителя. Можно сделать следующее:
    - Создайте ISO-образ. Затем можно записать его на CD/DVD-диск, использовать для создания загрузочного флэш-накопителя USB или подключить его к виртуальной машине.
    - Создайте ZIP-файл.
    - Передать выбранные компоненты на PXE-сервер Киберпротект.
    - Загрузить выбранные компоненты на WDS/RIS.
15. [Необязательно] Добавьте системные *драйверы Windows для использования компонентом Универсальное восстановление (Universal Restore)*. Это окно отображается в том случае, если компонент добавлен на носитель и выбран носитель, отличный от WDS и RIS.
16. При необходимости укажите имя хоста или IP-адрес и учетные данные для WDS или RIS либо путь к ISO-файлу носителя.

17. Проверьте настройки в итоговом окне и щёлкните **Приступить**.

Параметры ядра

Это окно позволяет указывать параметры для ядра Linux. Они будут применены автоматически при запуске загрузочного носителя.

Обычно эти параметры используются при наличии проблем с работой загрузочных носителей. Как правило, это поле оставляется пустым.

Кроме того, можно указать любой из этих параметров, нажав клавишу `F11` в меню загрузки.

Если задается несколько параметров, они должны быть разделены пробелами.

Список параметров:

`acpi=off`

Отключает интерфейс ACPI. Этот параметр может использоваться при наличии проблем с определенной конфигурацией оборудования.

`noapic`

Отключает расширенный программируемый контроллер прерываний Advanced Programmable Interrupt Controller (APIC). Этот параметр может использоваться при наличии проблем с определенной конфигурацией оборудования.

`vga=ask`

Предлагает указать видеорежим для графического пользовательского интерфейса загрузочного носителя. Если параметр `vga` не задан, то видеорежим определяется автоматически.

`vga=mode_number`

Задает видеорежим для графического пользовательского интерфейса загрузочного носителя. Номер режима задается параметром `<mode_number>` в шестнадцатеричном формате, например `vga=0x318`

Разрешение экрана и количество цветов, соответствующее номеру режима, может различаться на разных машинах. Рекомендуется в качестве значения `номер_режима` сначала использовать параметр `vga=ask`.

`quiet`

Отключает отображение загрузочных сообщений при загрузке ядра Linux и запускает консоль управления после загрузки ядра.

Этот параметр указан неявно при создании загрузочного носителя, однако его можно удалить из меню загрузки.

Без этого параметра будут отображаться все сообщения загрузки, потом появится командная

строка. Чтобы запустить консоль управления из командной строки, запустите следующую команду: `/bin/product`

`nousb`

Отключает загрузку подсистемы USB.

`nousb2`

Отключает поддержку USB 2.0. Устройства USB 1.1 при наличии этого параметра продолжают работать. Этот параметр позволяет использовать некоторые USB-устройства в режиме USB 1.1, если они не работают в режиме USB 2.0.

`nodma`

Отключает прямой доступ к памяти access (DMA) для всех жестких дисков IDE. Предотвращает зависание ядра с некоторым оборудованием.

`nofw`

Отключает поддержку интерфейса FireWire (IEEE1394).

`nopcmcia`

Отключает распознавание оборудования PCMCIA.

`nomouse`

Отключает поддержку мыши.

`<module_name>=off`

Отключает модуль, имя которого задано параметром `<module_name>`. Например, чтобы отключить использование модуля SATA, задайте параметр `sata_sis=off`.

`pci=bios`

Включает принудительное использование BIOS PCI вместо непосредственного доступа к устройству. Этот параметр может потребоваться, если машина имеет нестандартный мост хоста PCI.

`pci=nobios`

Отключает использование BIOS PCI. Будут разрешены только прямые методы доступа к оборудованию. Этот параметр может понадобиться, если загрузочный носитель не загружается. Это может вызывать BIOS.

`pci=biosirq`

Использует вызовы BIOS PCI для получения таблицы маршрутизации прерываний. Этот параметр может понадобиться, если ядру не удается выделять запросы на прерывания (IRQ) или не удается обнаружить вторичные шины PCI на материнской плате.

Эти вызовы могут работать на некоторых машинах неправильно. Однако это может быть единственный способ получения таблицы маршрутизации прерываний.

LAYOUTS=ru-RU, en-US, ...

Задает раскладки клавиатуры, которые можно использовать в графическом интерфейсе пользователя загрузочного носителя.

Если данный параметр не указан, могут использоваться только две раскладки: ”Английский (США)” и раскладка, которая соответствует языку, выбранному в меню загрузки носителя.

Укажите один из следующих параметров:

- `ru-RU` — русский
- `be-BE` — бельгийский
- `cz-CZ` — чешский
- `de-CH` — немецкий (Швейцария)
- `de-DE` — немецкий
- `en-GB` — английский
- `en-US` — английский (США)
- `es-ES` — испанский
- `fr-CH` — французский (Швейцария)
- `fr-FR` — французский
- `it-IT` — итальянский
- `pl-PL` — польский
- `pt-BR` — португальский (Бразилия)
- `pt-PT` — португальский
- `sr-CR` — сербский (кириллица)
- `sr-LT` — сербский (латиница)

При работе на загрузочном носителе, используйте CTRL + SHIFT для перехода по доступным раскладкам.

Сценарии на загрузочных носителях

Для того, чтобы на загрузочном носителе выполнялся определенный набор операций, укажите сценарий при создании носителя в Bootable Media Builder. При каждой загрузке носителя вместо отображения пользовательского интерфейса начнется выполнение сценария.

Выберите один из предопределенных сценариев или создайте пользовательский сценарий в соответствии со стандартами создания сценариев.

Предопределенный сценарий

Bootable Media Builder предоставляет следующие предопределенные сценарии:

- резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя (**entire_pc_local**);
- резервное копирование данных в сетевую папку и восстановление данных из сетевой папки (**entire_pc_share**);

Сценарии находятся на машине, на которой установлено приложение Bootable Media Builder, в следующих папках:

- В ОС Windows: `%\ProgramData%\Acronis\MediaBuilder\scripts\`

- В ОС Linux: `/var/lib/Acronis/MediaBuilder/scripts/`

Резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя

Сценарий создаст резервную копию машины на загрузочном носителе или восстановит машину из последней резервной копии, созданной этим сценарием на том же носителе. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder вы можете указать пароль, который сценарий будет использовать для защиты резервных копий или доступа к ним.

Резервное копирование данных в сетевую папку и восстановление данных из сетевой папки

Сценарий создаст резервную копию машины в сетевой папке или восстановит машину из последней резервной копии, расположенной в сетевой папке. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder укажите следующие параметры сценария:

1. путь к сетевой папке;
2. имя пользователя и пароль для доступа в сетевую папку;
3. [Необязательно] имя файла резервной копии. Значением по умолчанию является **AutoBackup** (Автоматическое резервное копирование). Если вы хотите, чтобы сценарий добавлял резервные копии к уже существующим резервным копиям, или провести восстановление из резервной копии с заданным пользователем именем, измените значение по умолчанию на имя файла желаемой резервной копии.

   Чтобы узнать имя файла резервной копии:

   1. В веб-консоли Кибер Бэкап последовательно выберите пункты **Хранилища резервных копий** → **Хранилища**.
   2. Выберите сетевую папку (нажмите **Добавить хранилище**, если нужной папки нет в списке).
   3. Выберите резервную копию.
   4. Нажмите **Сведения**. Имя файла отобразиться в поле **Имя файла резервной копии**.
4. [Необязательно] пароль, который сценарий будет использовать для защиты резервных копий или доступа к ним.

Пользовательские сценарии

Важно

Создание пользовательских сценариев требует знания команд оболочки Bash и формата JavaScript Object Notation (JSON). Если вы не знакомы с командной оболочкой Bash, хороший учебник можно найти по ссылке http://www.tldp.org/LDP/abs/html. Спецификация JSON доступна на сайте http://www.json.org.

Файлы сценария

Сценарий должен быть расположен в указанных ниже каталогах на машине, в которой установлен мастер создания загрузочных носителей:

- В ОС Windows: `%\ProgramData%\Acronis\MediaBuilder\scripts\`
- В ОС Linux: `/var/lib/Acronis/MediaBuilder/scripts/`

Сценарий должен состоять из по меньшей мере трех файлов:

- `<файл_сценария>.sh` — файл со сценарием Bash. При создании сценария используйте только ограниченный набор команд оболочки, который вы можете найти по ссылке https://busybox.net/downloads/BusyBox.html. Также могут быть использованы следующие команды:
  - `acrocmd` — утилита командной строки для создания резервной копии и восстановления
  - `product` — команда, запускающая пользовательский интерфейс загрузочного носителя

  Этот файл и все другие включенные в сценарий дополнительные файлы (например, посредством использования команды с точкой) должны быть расположены в подпапке `bin`. В сценарии укажите дополнительные пути к файлам в виде `/ConfigurationFiles/bin/<файл>`.
- `autostart` — файл для запуска `<файл_сценария>.sh`. Содержимое файла должно быть следующим:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- `autostart.json` — файл формата JSON, содержащий следующее:
  - Имя сценария и описания будут отображаться в мастере создания загрузочных носителей.
  - Имена переменных сценария должны быть настроены через мастер создания загрузочных носителей.

- Параметры элементов управления, которые будут отображены в Bootable Media Builder для каждой переменной.

Структура autostart.json

Объект высшего уровня

Пара		Требуется	Описание
Имя	**Тип значения**		
`displayName`	строка	Да	Имя сценария, которое будет отображаться в Bootable Media Builder.
`description`	строка	Нет	Описание сценария, которое будет отображаться в Bootable Media Builder.
`timeout`	число	Нет	Время ожидания (в секундах) для меню загрузки перед запуском сценария. Если пара не указана, время ожидания составит десять секунд.
`variables`	объект	Нет	Любые переменные для **<файл_сценария>.sh**, которые вы хотите сконфигурировать посредством Bootable Media Builder. Значение должно быть указано в виде набора следующих пар: идентификатор строки переменной и объект переменной (см. в таблице ниже).

Объект переменной

Пара		Требуется	Описание
Имя	**Тип значения**		
`displayName`	строка	Да	Имя переменной, использованное в **<файл_сценария>.sh**.
`type`	строка	Да	Тип элемента управления, отображенный в Bootable Media Builder. Этот элемент управления используется для конфигурирования значения переменной. Список всех поддерживаемых типов см. в таблице ниже.
`description`	строка	Да	Метка элемента управления, отображаемая над элементом управления в Bootable Media Builder.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Пара		Требуется	Описание
Имя	**Тип значения**		
`default`	строка, если `type` является `string`, `multiString`, `password` или `enum` число, если `type` является `number`, `spinner` или `checkbox`	Нет	Значение по умолчанию элемента управления. Если пара не указана, значением по умолчанию будет являться пустая строка или ноль, в зависимости от типа элемента управления. Значением по умолчанию для флажка может быть `0` (флажок не установлен) или `1` (флажок установлен).
`order`	число (не отрицательное)	Да	Порядок элементов управления в Bootable Media Builder. Чем выше значение, тем ниже расположен элемент управления относительно других элементов управления, указанных в **autostart.json**. Изначальным значение должен быть `0`.
`min` (только для `spinner`)	число	Нет	Минимальное значение элемента управления ”счетчик” в поле счетчика. Если пара не указана, значением будет `0`.
`max` (только для `spinner`)	число	Нет	Максимальное значение элемента управления ”счетчик” в поле счетчика. Если пара не указана, значением будет `100`.
`step` (только для `spinner`)	число	Нет	Значение шага элемента управления ”счетчик” в поле счетчика. Если пара не указана, значением будет `1`.
`items` (только для `enum`)	массив строк	Да	Значения для раскрывающегося списка.
`required` (для `string`, `multiString`, `password` и `enum`)	число	Нет	Указывает, может ли значение элемента управления быть пустым (`0`) или нет (`1`). Если пара не указана, значение элемента управления может быть пустым.

Тип элемента управления

Имя	Описание
`string`	Текстовое поле высотой в одну строку и без ограничений ширины, используемое для введения или редактирования коротких строк.

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Имя	Описание
`multiString`	Текстовое поле высотой в несколько строк и без ограничений ширины, используемое для введения или редактирования коротких строк.
`password`	Текстовое поле высотой в одну строку и без ограничений ширины, используемое для безопасного введения пароля.
`number`	Текстовое поле высотой в одну строку, с допустимым введением только числовых значений, используемое для введения или редактирования чисел.
`spinner`	Текстовое поле высотой в одну строку, с допустимым введением только числовых значений, используемое для введения или редактирования чисел, с элементом управления ”счетчик”. Также называется полем счетчика.
`enum`	Стандартный выпадающий список с фиксированным набором предварительно указанных значений.
`checkbox`	Поле флажка с двумя положениями — флажок установлен и флажок не установлен.

Указанный ниже пример `autostart.json` содержит все возможные типы элементов управления, которые могут быть использованы для конфигурирования переменных для файла `<файл_сценария>.sh`.

```
{
  ”displayName”: ”Имя автоматически запускаемого сценария”,
  ”description”: ”Описание автоматически запускаемого сценария”,
  ”variables”: {
    ”var_string”: {
      ”displayName”: ”VAR_STRING”,
      ”type”: ”string”,
      ”order”: 1,
      ”description”: ”Элемент управления 'string':”,
      ”default”: ”Hello, world!”
    },
    ”var_multistring”: {
      ”displayName”: ”VAR_MULTISTRING”,
      ”type”: ”multiString”,
      ”order”: 2,
      ”description”: ”Элемент управления 'multiString':”,
      ”default”: ”Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit.”
    },
    ”var_number”: {
      ”displayName”: ”VAR_NUMBER”,
      ”type”: ”number”,
      ”order”: 3,
      ”description”: ”Элемент управления 'number':”,
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
      ”default”: 10
    },
    ”var_spinner”: {
      ”displayName”: ”VAR_SPINNER”,
      ”type”: ”spinner”,
      ”order”: 4,
      ”description”: ”Элемент управления 'spinner':”,
      ”min”: 1,
      ”max”: 10,
      ”step”: 1,
      ”default”: 5
    },
    ”var_enum”: {
      ”displayName”: ”VAR_ENUM”,
      ”type”: ”enum”,
      ”order”: 5,
      ”description”: ”Элемент управления 'enum':”,
      ”items”: [
        ”первый”,
        ”второй”,
        ”третий”
      ],
      ”default”: ”второй”
    },
    ”var_password”: {
      ”displayName”: ”VAR_PASSWORD”,
      ”type”: ”password”,
      ”order”: 6,
      ”description”: ”Элемент управления 'password':”,
      ”default”: ”qwe”
    },
    ”var_checkbox”: {
      ”displayName”: ”VAR_CHECKBOX”,
      ”type”: ”checkbox”,
      ”order”: 7,
      ”description”: ”Элемент управления 'checkbox'”,
      ”default”: 1
    }
  }
}
```

Сервер управления

При создании загрузочного носителя есть возможность предварительно сконфигурировать регистрацию носителя на сервере управления.

Регистрация носителя позволит выполнять операции управления с загрузочным носителем посредством веб-консоли Кибер Бэкап, как с зарегистрированной машиной. Кроме удобства удаленного доступа это дает системному администратору возможность отслеживать все операции, выполняемые на загрузочном носителе. Операции находятся на вкладке **Действия**, где можно увидеть, кто и когда начал выполнение операции.

Если регистрация не была предварительно сконфигурирована, остается возможность зарегистрировать носитель *после загрузки с него машины*.

Как выполнить предварительную конфигурацию регистрации на сервере управления.

1. Установите флажок **Зарегистрировать носитель на сервере управления**.
2. В строке **Имя или IP-адрес сервера** укажите имя хоста или IP-адрес машины, на которой установлен сервер управления. Используйте один из следующих форматов.
   - `http://<сервер>`. Например, `http://10.250.10.10` или `http://server1`.
   - `<IP-адрес>`. Например, `10.250.10.10`.
   - `<имя хоста>`. Например, `server1` или `server1.example.com`.
3. В строке **Порт** укажите порт, который будет использоваться для доступа к серверу управления. Значение по умолчанию составляет 9877.
4. В строке **Отображаемое имя** укажите имя, которое будет отображаться для этой машины в веб-консоли Кибер Бэкап. Если это поле будет оставлено пустым, в качестве отображаемого имени будет указано одно из следующих.
   - Если машина ранее была зарегистрирована на сервере управления, у нее будет то же имя.
   - В ином случае будет использовано полное доменное имя (FQDN) или IP-адрес машины.
5. Выберите учетную запись, которая будет использована для регистрации носителя на сервере управления. Доступны следующие параметры:
   - **Спрашивать имя пользователя и пароль при загрузке**

     Учетные данные необходимо вводить при каждой загрузке машины с носителя.

     Для выполнения регистрации учетная запись должна находится в списке администраторов

сервера управления (**Настройки** → **Учетные записи**). В веб-консоли Кибер Бэкап носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которые предоставлены данной учетной записи.

В интерфейсе загрузочного носителя будет возможно изменить имя пользователя и пароль, перейдя по пути **Инструменты** → **Зарегистрировать носитель на сервере управления**.

- **Зарегистрироваться под следующей учетной записью**

  Машина будет регистрироваться автоматически при каждой загрузке с носителя.

  Указанная учетная запись должна находится в списке администраторов сервера управления (**Настройки** → **Учетные записи**). В веб-консоли Кибер Бэкап носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которые предоставлены данной учетной записи.

  В интерфейсе загрузочного носителя будет *невозможно* сменить параметры регистрации.

Сетевые настройки

При создании загрузочного носителя можно предварительно настроить сетевые подключения, которые будут использоваться загрузочным агентом. Предварительно настроить можно следующие параметры:

- IP-адрес,
- маску подсети,
- шлюз,
- DNS-сервер,
- WINS-сервер.

После запуска загрузочного агента на машине конфигурация применяется к сетевому адаптеру машины. Если параметры не были предварительно настроены, агент использует автонастройку DHCP. Также вы можете задать сетевые параметры вручную при запуске загрузочного агента на машине.

Предварительная настройка нескольких сетевых подключений

Можно предварительно настроить параметры TCP/IP вплоть до десяти сетевых адаптеров. Чтобы убедиться, что каждому сетевому адаптеру будут назначены соответствующие параметры, создайте носитель на сервере, для которого настраивается носитель. При выборе существующего сетевого адаптера в окне мастера ее настройки выбираются для сохранения на носителе. MAC-адрес каждого существующего сетевого адаптера также сохраняется на носителе.

Параметры, кроме MAC-адреса, можно изменить или при необходимости настроить для несуществующего сетевого адаптера.

После запуска загрузочного агента на сервере он получает список доступных сетевых адаптеров. Этот список сортируется по слотам, которые занимают сетевые адаптеры: чем ближе к процессору, тем выше в списке.

Загрузочный агент назначает каждому известному сетевому адаптеру соответствующие настройки, идентифицируя адаптеры по MAC-адресам. После настройки сетевых адаптеров с известными MAC-адресами оставшимся сетевым адаптерам назначаются настройки, созданные для несуществующих сетевых адаптеров, начиная с верхнего неназначенного адаптера.

Загрузочный носитель можно настроить для любой машины, а не только для той, на которой он был создан. Для этого настройте сетевые адаптеры в соответствии с порядком их слотов на нужной машине: NIC1 занимает ближайший к процессору слот, NIC2 — следующий слот и т. д. При запуске загрузочного агента на этой машине он не найдет сетевых адаптеров с известными MAC-адресами и настроит адаптеры в том порядке, который вы указали.

Пример

Загрузочный агент может использовать один из сетевых адаптеров для связи с консолью управления через производственную сеть. Для этого подключения можно выполнить автоматическую настройку. Объемные данные для восстановления можно передавать через второй сетевой адаптер, включенный в выделенную резервную сеть посредством статических настроек TCP/IP.

Сетевой порт

Во время создания загрузочного носителя можно предварительно настроить сетевой порт, который будет прослушиваться загрузочным агентом на наличие входящего подключения от утилиты `acrocmd`. Можно выбрать один из указанных ниже вариантов.

- Порт по умолчанию
- Текущий используемый порт
- Новый порт (введите номер порта)

Если порт не был предварительно настроен, агент использует порт 9876.

Драйверы для компонента Универсальное восстановление (Universal Restore)

При создании загрузочного носителя есть возможность добавить на него драйверы Windows. Эти драйверы будут использоваться компонентом Универсальное восстановление (Universal Restore) для загрузки системы Windows, перенесенной на отличающееся оборудование.

Компонент Универсальное восстановление (Universal Restore) можно будет настроить для следующих целей:

- для поиска на носителе драйверов, наилучшим образом подходящих для целевого оборудования;
- для получения драйверов устройств хранения данных, явно заданных с носителя. Это необходимо, если целевое оборудование оснащено специфическим контроллером запоминающего устройства (таким как SCSI, RAID или адаптер Fiber Channel) для жесткого диска.

Драйверы будут размещены в видимой папке Drivers на загрузочном носителе. Драйверы не загружаются в ОЗУ целевой машины, поэтому носитель должен оставаться вставленным или подключенным в течение всей работы компонента Универсальное восстановление (Universal Restore).

Добавить драйверы на загрузочный носитель можно при создании съемного носителя, его ISO-образа или подключаемого носителя, такого как флэш-накопитель. Драйверы невозможно загрузить в WDS или RIS.

Драйверы можно добавить в список только в группах путем добавления INF-файлов или папок, содержащих такие файлы. Выбор отдельных драйверов из INF-файлов невозможен, однако мастер создания загрузочных носителей отображает содержимое файла для сведений.

Добавление драйверов

1. Щёлкните **Добавить** и перейдите к INF-файлу или папке, содержащей INF-файлы.
2. Выберите INF-файл или папку.
3. Нажмите кнопку **ОК**.

Драйверы можно удалить из списка только в группах путем удаления INF-файлов.

Удаление драйверов

1. Выберите INF-файл.
2. Нажмите кнопку **Удалить**.

Загрузочный носитель на основе WinPE

Мастер создания загрузочных носителей предоставляет два способа интеграции Кибер Бэкап с WinPE:

- Создание ISO-образа PE с подключаемым модулем с нуля.
- Добавление подключаемого модуля Киберпротект к WIM-файлу для использования в будущем (ручное создание ISO-образа, добавление других средств к образу и т. д.).

Можно создать PE-образы на основе WinRE без какой-либо дополнительной подготовки или создать PE-образы после установки комплекта средств для развёртывания и оценки Windows (ADK).

PE-образы на основе WinRE

Создание образов на основе WinRE поддерживается для следующих операционных систем:

- Windows 10—11 (64-разрядные версии);
- Windows Server 2016—2025 (64-разрядные версии).

PE-образы

После установки пакета Windows AIK или комплекта средств для развёртывания и оценки Windows (ADK) мастер создания загрузочных носителей поддерживает дистрибутивы WinPE, основанные на любой из следующих ОС:

- Windows 10 (PE для Windows 10);
- Windows 11 (PE для Windows 11).

Мастер создания загрузочных носителей поддерживает 64-разрядные дистрибутивы WinPE для загрузки машин, которые используют интерфейс UEFI.

Для работы образов среды предустановки на основе WinPE 4 (и более поздних версий) требуется около 1 ГБ ОЗУ.

> **Примечание**
>
> Для выполнения операций управления дисками в ОС Windows 10 и более поздних версий необходимо установить Управление Дисками.

Подготовка WinPE 4.0 и более поздние версии

Для создания или изменения образов PE 4 или более поздних версий установите мастер создания загрузочных носителей на машину с установленным комплектом средств для развёртывания и оценки Windows (ADK). Если у вас нет машины с ADK, подготовьте её следующим образом.

Подготовка машины с ADK:

1. Загрузите программу установки комплекта средств для развёртывания и оценки (ADK).

   Скачайте комплект средств для развёртывания и оценки Windows (ADK) для Windows с официальной страницы.

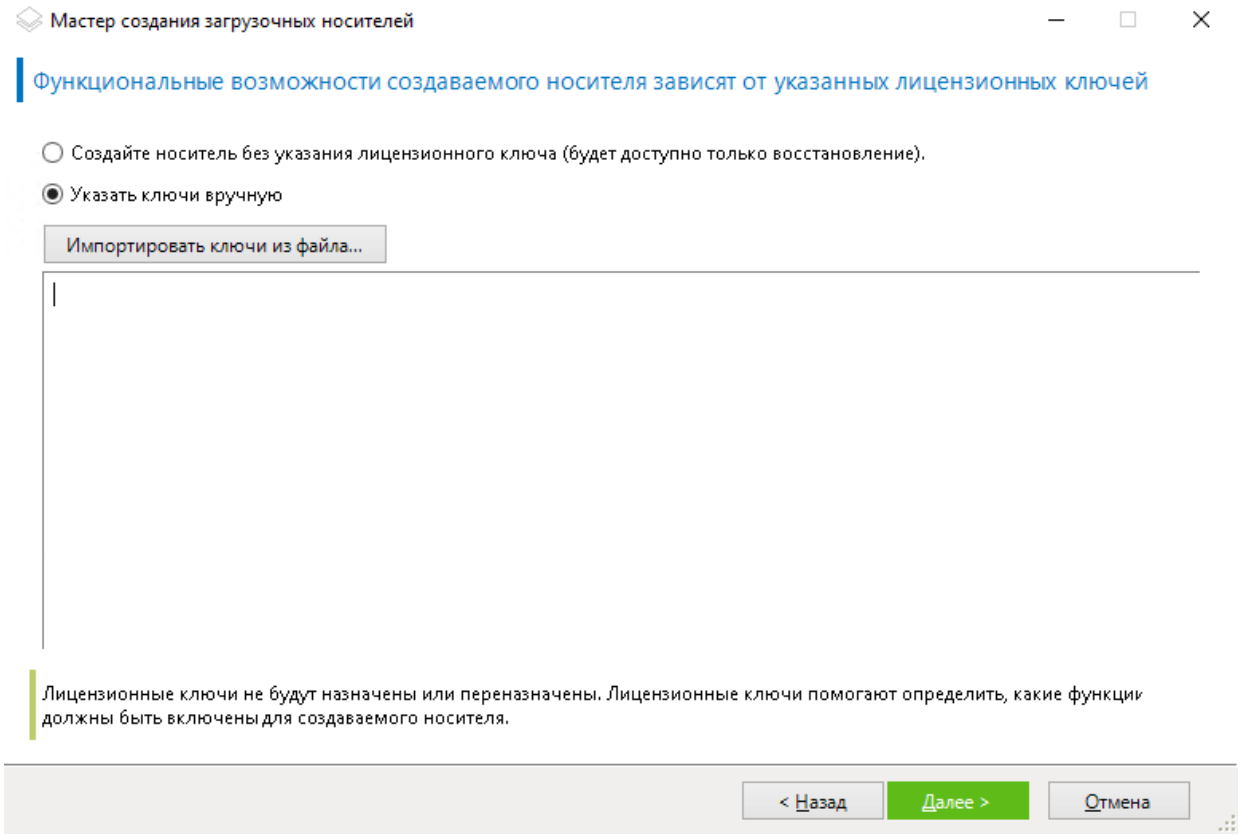
   Системные требования для установки приведены по указанной выше ссылке.

2. Установите комплект ADK на машине.
3. Установите мастер создания загрузочных носителей на этой же машине.

Добавление подключаемого модуля Киберпротект к WinPE

Порядок добавления подключаемого модуля Киберпротект к WinPE

1. Запустите мастер создания загрузочных носителей.
2. Чтобы создать полнофункциональный загрузочный носитель, укажите лицензионный ключ Кибер Бэкап. Этот ключ используется для определения функций, которые будут представлены на загрузочном носителе. Лицензии не будут отзываться. Если не указать лицензионный ключ, полученный загрузочный носитель можно использовать только для операций восстановления и доступа к компоненту Универсальное восстановление (Universal Restore).

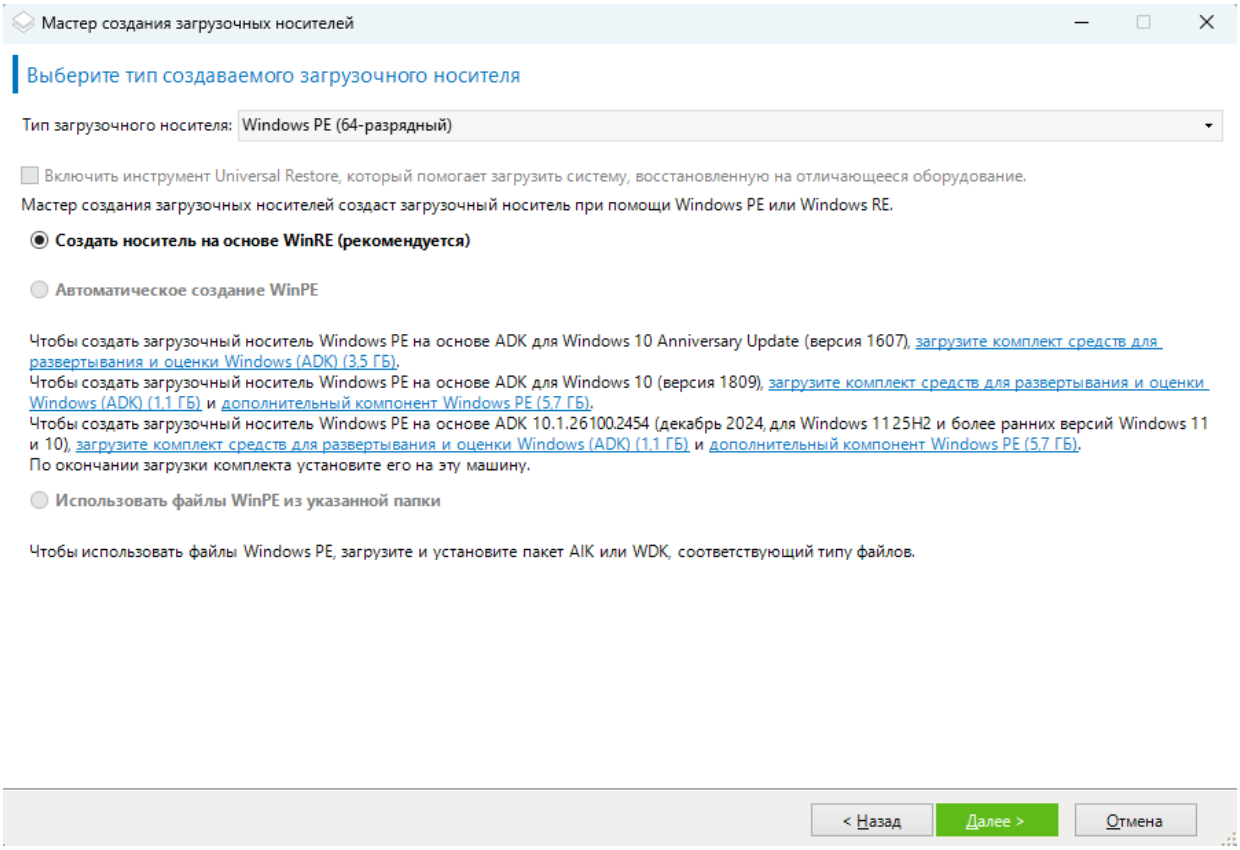


3. Выберите **Тип загрузочного носителя: Windows PE (64-разрядный)**.

   Если планируется восстановить операционную систему на компьютере с другим оборудованием или на виртуальной машине и необходимо обеспечить загружаемость системы, установите флажок **Включить инструмент Universal Restore...**

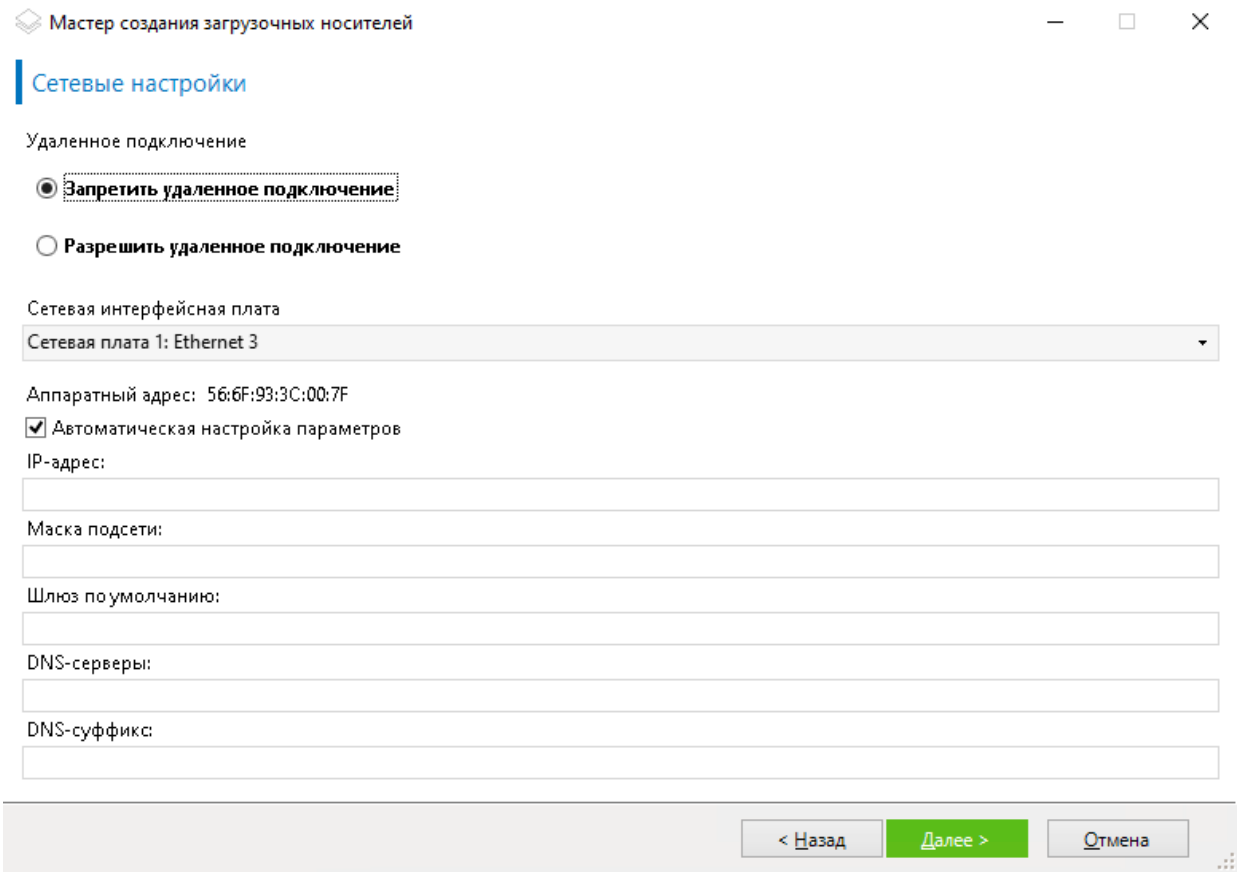
4. Выберите **Создать носитель на основе WinRE (рекомендуется)**.

   Программа запустит соответствующий сценарий и перейдёт к следующему окну.



5. Выберите язык, который будет использоваться в загрузочном носителе.
6. Выберите, разрешить или запретить удалённое подключение к машине, загружаемой с носителя. Если подключение разрешено, введите имя пользователя и пароль, которые должны быть указаны в командной строке в случае, когда утилита `acrocmd` выполняется на другой машине. Можно оставить эти поля пустыми. В этом случае удалённое подключение через интерфейс командной строки можно будет выполнить без ввода учётных данных.

   Эти учётные данные также необходимы при *регистрации носителя на сервере управления в веб-консоли*.



7. Укажите *сетевые настройки* для сетевых адаптеров машины или выберите автоконфигурацию DHCP.
8. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительную информацию о настройках регистрации см. в разделе *Сервер управления*.
9. [Необязательно] Укажите драйверы Windows, которые нужно добавить к Windows PE.

   После загрузки Windows PE на машину эти драйверы помогут получить доступ к устройствам, на которых расположена резервная копия.

   Кроме того, можно будет указать добавленные драйверы при настройке компонента Универсальное восстановление (Universal Restore) для Windows.

   Как добавить драйверы

   - Щёлкните **Добавить** и задайте путь к INF-файлу для соответствующего контроллера SCSI, RAID или SATA, сетевого адаптера, ленточного устройства или другого устройства.
   - Повторите эту процедуру для каждого драйвера, который необходимо записать на носитель WinPE.
10. Выберите, следует ли создать ISO- или WIM-образ либо загрузить носитель на сервер (WDS или RIS).

11. Задайте полный путь к полученному файлу образа, включая его имя, или укажите сервер и задайте имя пользователя и пароль для доступа к нему.
12. Проверьте настройки в итоговом окне и щёлкните **Приступить**.
13. Запишите ISO-образ на CD- или DVD-диск, используя стороннюю программу, или подготовьте загрузочный флэш-накопитель.

После загрузки машины в WinPE агент запустится автоматически.

Создание образа среды предустановки (ISO-файл) из получившегося WIM-файла

- Замените в папке Windows PE файл boot.wim, используемый по умолчанию, созданным WIM-файлом. Например, введите:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Используйте инструмент `Oscdimg`. Например, введите:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

> **Предупреждение**
>
> Не копируйте этот пример. Введите команду вручную.

Подключение к машине, загружаемой с носителя

После загрузки машины с загрузочного носителя терминал машины отображает окно загрузки с IP-адресами, полученными от сервера DHCP или установленными в соответствии с предварительно заданными значениями.

Настройка сети

Чтобы изменить сетевые параметры для текущего сеанса, щёлкните **Настроить параметры сети** в окне запуска. Появится окно **Сетевые параметры**, где можно задать сетевые настройки для каждого сетевого адаптера (NIC) машины.

Изменения, внесенные во время сеанса, будут потеряны после перезагрузки машины.

Добавление VLAN

В окне **Сетевые параметры** можно добавить виртуальные локальные сети (VLAN). Используйте эту функцию, если требуется доступ к хранилищу резервных копий, включенному в определенную сеть VLAN.

В основном сети VLAN используются для разделения локальной сети на сегменты. Сетевой адаптер, подключенный к порту *доступа* коммутатора, всегда имеет доступ к сети VLAN, указанной в настройках порта. Сетевой адаптер, подключенный к *магистральному* порту коммутатора, имеет доступ к сетям VLAN, указанным в настройках порта, только в случае, если сети VLAN заданы в сетевых параметрах.

Включение доступа к сети VLAN через магистральный порт

1. Щёлкните **Добавить VLAN**.
2. Выберите сетевой адаптер, обеспечивающий доступ к локальной сети с нужной сетью VLAN.
3. Укажите идентификатор VLAN.

После щелчка на **OK** появится новая запись в списке сетевых адаптеров.

Если требуется удалить VLAN, щёлкните соответствующую сеть VLAN и нажмите кнопку **Удалить VLAN**.

Локальное подключение

Для непосредственной работы на машине, загружаемой с носителя, щёлкните **Локальное управление этой машиной** в окне загрузки.

Удаленное подключение

Для удаленного подключения к носителю зарегистрируйте его на сервере управления, как описано в разделе *Регистрация носителя на сервере управления*.

Регистрация носителя на сервере управления

Регистрация загрузочного носителя позволит выполнять операции управления с загрузочным носителем посредством веб-консоли Кибер Бэкап, как с зарегистрированной машиной. Это применимо ко всем загрузочным носителям вне зависимости от метода загрузки (физический носитель, диспетчер восстановления при загрузке, Киберпротект PXE Server, WDS или RIS).

Регистрация носителей возможна только при наличии на сервере управления хотя бы одной расширенной лицензии Кибер Бэкап.

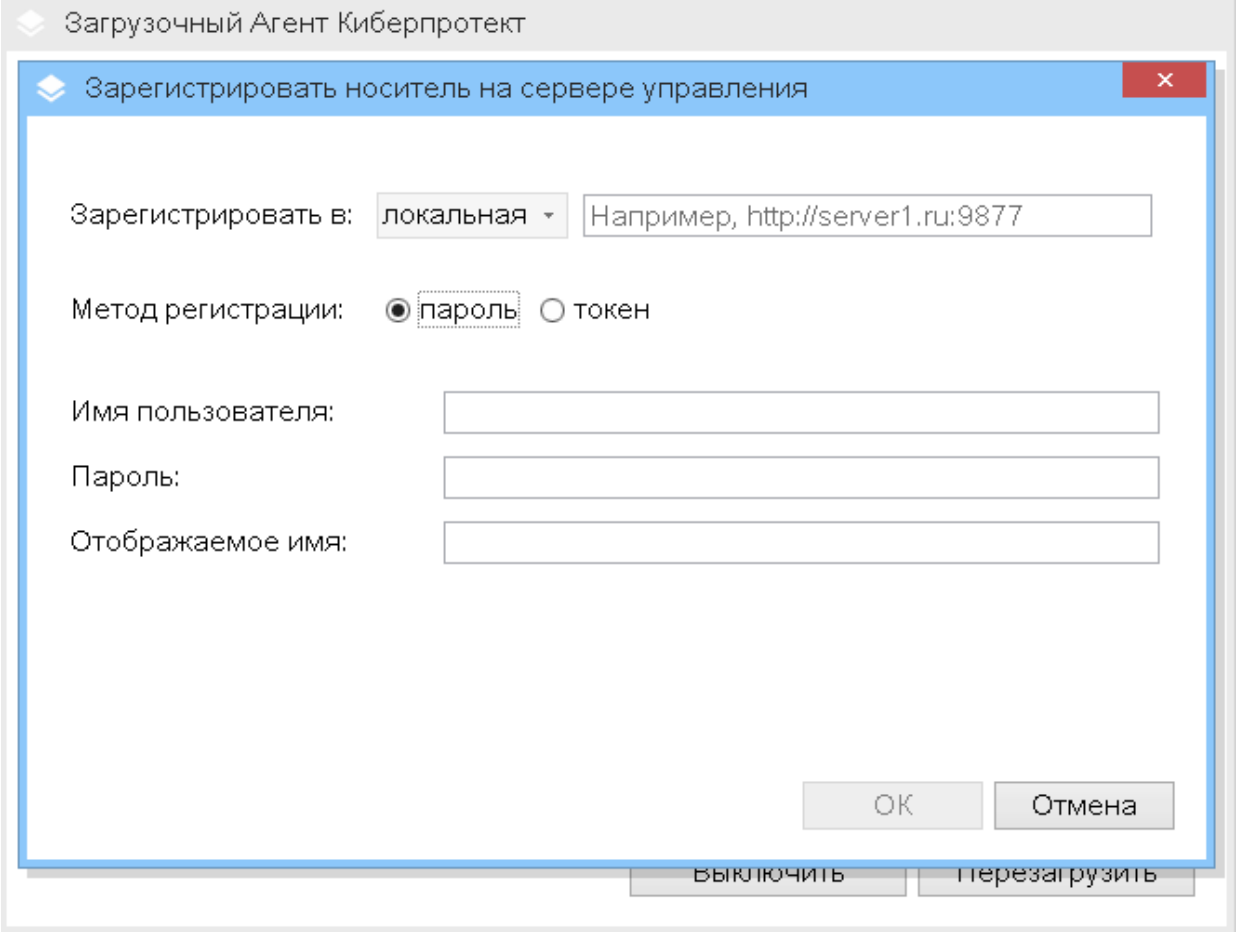
Носитель можно зарегистрировать в пользовательском интерфейсе носителя.

Параметры регистрации могут быть предварительно настроены в параметре *Сервер управления* Bootable Media Builder. Если все параметры регистрации настроены предварительно, носитель автоматически отображается в веб-консоли Кибер Бэкап. Если некоторые параметры настроены предварительно, некоторые шаги описанной далее процедуры могут быть недоступны.

Регистрация носителя в пользовательском интерфейсе носителя

Носитель можно создать или загрузить с использованием *Bootable Media Builder*.

1. Загрузите машину с носителя.
2. Выполните одно из следующих действий:
   - В окне запуска в поле **Сервер управления** нажмите **Редактировать**.
   - В интерфейсе загрузочного носителя нажмите **Инструменты** → **Зарегистрировать носитель на сервере управления**.



3. В поле **Зарегистрировать в** выберите **Локальная** и укажите имя хоста или IP-адрес машины, на которой установлен сервер управления. Используйте один из следующих форматов.
   - `http://<сервер>`. Например, `http://10.250.10.10` или `http://server`.

- `<IP-адрес>`. Например, `10.250.10.10`.
- `<имя хоста>`. Например, `server` или `server.example.com`.

4. Выберите метод регистрации: пароль или токен. Информацию о создании токена см. в разделе *Развертывание агентов с использованием групповой политики*.
5. При регистрации по токену укажите его в поле **Регистрационный токен** и перейдите к шагу 8.
6. При регистрации по паролю в полях **Имя пользователя** и **Пароль** введите учетные данные учетной записи, которая находится в списке администраторов сервера управления (**Настройки** → **Учетные записи**). В веб-консоли Кибер Бэкап носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которые предоставлены данной учетной записи.
7. В строке **Отображаемое имя** укажите имя, которое будет отображаться для этой машины в веб-консоли Кибер Бэкап. Если это поле будет оставлено пустым, в качестве отображаемого имени будет указано одно из следующих:
   - Если машина ранее была зарегистрирована на сервере управления, у нее будет то же имя.
   - В ином случае будет использовано полное доменное имя (FQDN) или IP-адрес машины.
8. Нажмите кнопку **ОК**.

Операции с загрузочным носителем

Операции с загрузочным носителем подобны операциям резервного копирования и восстановления, которые выполняются при запущенной операционной системе. Отличия состоят в следующем:

1. Если используется загрузочный носитель с представлением томов по типу Windows, том имеет такую же букву диска, как в Windows. Томам, которые не имеют букв диска в Windows (например, том ”Зарезервировано системой”), присваиваются свободные буквы в порядке их следования на диске.

   Если загрузочный носитель не обнаруживает ОС Windows на машине или обнаруживает несколько систем, всем томам (даже если они не имеют букв дисков), присваиваются буквы в порядке их следования на диске. Поэтому буквы томов могут отличаться от букв томов, отображаемых в Windows. Например, диск D: на загрузочном носителе может соответствовать диску E: в Windows.

   Примечание

   Рекомендуем назначить уникальные имена томам.

2. Загрузочный носитель с представлением томов по типу Linux отображает локальные диски и тома

как отключенные (sda1, sda2...).

3. Резервным копиям, созданным с помощью загрузочного носителя, присваиваются упрощенные имена файлов. Стандартные имена назначаются резервным копиям только в случае, если эти резервные копии добавляются к существующему архиву со стандартными именами файлов или если место сохранения не поддерживает упрощенные имена файлов.
4. Загрузочному носителю с представлением томов по типу Linux не удается записать резервные копии на том в формате NTFS. При необходимости сделать это переключитесь на носитель с представлением томов по типу Windows. Чтобы перейти к представлениям томов загрузочного носителя, щёлкните **Инструменты** → **Изменить представление томов**.
5. Задания невозможно запланировать в расписании. Если требуется повторить операцию, настройте ее с нуля.
6. Время существования журнала ограничено текущим сеансом. Весь журнал или отфильтрованные записи журнала можно сохранить в файл.
7. Централизованные хранилища не отображаются в дереве папок окна **Архив**.

   Для доступа к управляемому хранилищу введите следующую строку в поле **Путь**: `bsp://адрес_узла/имя_хранилища/`.

   Для доступа к неуправляемому централизованному хранилищу введите полный путь к папке хранилища.

   После ввода учетных данных для доступа будет отображен список архивов, расположенных в хранилище.

Настройка режима отображения

Для машины, которая загружается с загрузочного носителя Linux, режим отображения определяется автоматически в зависимости от конфигурации оборудования (характеристик монитора и видеоплаты). Если видеорежим определен неправильно, сделайте следующее.

1. В меню загрузки нажмите клавишу `F11`.
2. В командной строке введите следующее: `vga=ask`, а затем продолжите загрузку.
3. Из списка поддерживаемых видеорежимов выберите нужный. Для этого введите его номер (например, 318) и нажмите клавишу `Ввод`.

Чтобы не выполнять эту процедуру каждый раз при загрузке данной аппаратной конфигурации, создайте загрузочный носитель заново с номером режима (в вышеуказанном примере `vga=0x318`), указанным в окне **Параметры ядра**.

Резервное копирование

Создать резервную копию данных можно только с использованием загрузочного носителя, который создан в мастере создания загрузочных носителей, и лицензионного ключа Кибер Бэкап. Информацию о том, как создать загрузочный носитель, см. в разделах *Загрузочные носители на основе Linux* или *Загрузочный носитель на основе Windows PE* соответственно.

Порядок восстановления данных с помощью загрузочного носителя

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Чтобы создать резервную копию локальной машины, щёлкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел *Регистрация носителя на сервере управления*.
3. Щёлкните **Создать резервную копию сейчас**.
4. Для создания резервной копии автоматически выбираются все несъемные диски. Чтобы изменить данные для резервного копирования, щёлкните **Элементы для резервного копирования**, а затем выберите желаемые диски или томы.

   При выборе данных для резервного копирования может выводиться следующее сообщение: ”Эту машину нельзя выбрать напрямую. На машине установлена предыдущая версия агента. Чтобы выбрать эту машину для резервного копирования, используйте правила политики”. Сообщение об этой проблеме с графическим интерфейсом пользователя можно проигнорировать. Выберите отдельные диски или томы, для которых необходимо создать резервные копии.

   Примечание

   Если используется загрузочный носитель на основе Linux, буквы диска могут отличаться от букв диска в Windows. Попробуйте определить необходимый диск или раздел по его размеру или метке.

5. Если необходимо выполнить резервное копирование файлов или папок (а не дисков), перейдите к области **Файлы** в разделе **Данные для резервного копирования**.

   С помощью загрузочного носителя можно создать только резервную копию дисков/разделов и файлов/папок. Другие типы резервного копирования, например, резервное копирование базы данных, можно выполнить только в запущенной операционной системе.
6. Щёлкните **Хранилище** и выберите место сохранения резервной копии.
7. Укажите хранилище и имя для резервной копии.
8. Укажите тип резервной копии. Если это первая резервная копия в этом хранилище, будет создана

полная резервная копия. Если же создается очередная резервная копия, для экономии места можно выбрать параметр **Инкрементное** или **Дифференциальное**.

9. [Необязательно] Чтобы проверить файл резервной копии, выберите **Проверить резервную копию сразу после создания**.
10. [Необязательно] Укажите параметры резервного копирования, которые могут вам понадобиться, например, пароль для файла резервной копии, разбивка резервной копии или обработка ошибок.
11. Нажмите кнопку **ОК**, чтобы начать резервное копирование.

    Загрузочный носитель считывает данные с диска, сжимает их в файл .tib, а затем записывает этот файл в выбранное хранилище. Он не создает моментальный снимок диска, поскольку нет запущенных приложений.
12. В появившемся окне можно проверить статус задания резервного копирования и просмотреть дополнительную информацию о резервном копировании.

Восстановление

Операция восстановления доступна как на загрузочных носителях, созданных с помощью мастера создания загрузочных носителей, так и на скачанных готовых загрузочных носителях.

Порядок восстановления данных с помощью загрузочного носителя

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Чтобы восстановить данные на локальную машину, щёлкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел *Регистрация носителя на сервере управления*.
3. Нажмите кнопку **Восстановить**.
4. В разделе **Объект восстановления** щёлкните **Выбрать данные**.
5. Щёлкните **Обзор** и выберите хранилище резервных копий.
6. Выберите файл резервной копии, на основе которой необходимо выполнить восстановление.
7. В левой нижней панели выберите файлы и тома (или файлы и папки), которые необходимо восстановить, и нажмите кнопку **ОК**.
8. [Необязательно] Настройте правила перезаписи.
9. [Необязательно] Настройте исключения восстановления.
10. [Необязательно] Настройте параметры восстановления.
11. Проверьте правильность настроек и нажмите кнопку **ОК**.

Примечание

Для восстановления данных на отличающееся оборудование необходимо использовать *компонент Универсальное восстановление (Universal Restore)*. Он недоступен, если резервная копия находится в Зоне безопасности.

Управление дисками

С помощью загрузочного носителя Киберпротект можно подготовить конфигурацию диска/тома для восстановления образов тома, резервная копия которых создана Кибер Бэкап.

Иногда, когда том скопирован и его образ помещен в безопасное хранилище, конфигурация дисков машины может измениться из-за замены жесткого диска или отказа оборудования. В таких случаях можно воссоздать необходимую конфигурацию диска таким образом, чтобы можно было восстановить образ тома точно таким, каким он был раньше, или с определенными изменениями диска или структуры томов на усмотрение пользователя.

Соблюдайте все необходимые *меры предосторожности*, чтобы избежать возможной потери данных.

Важно

Все операции с дисками и томами создают определенный риск повреждения данных. Операции с системой, загрузочными томами или томами с данными должны выполняться очень аккуратно во избежание проблем с процессом загрузки или хранением данных жесткого диска.

Операции с жесткими дисками и томами занимают определенное время и в случае потери питания во время процедуры (непреднамеренного выключения машины или случайного нажатия кнопки Reset) могут привести к повреждению томов и потере данных.

Операции управления диском можно выполнить на ”голом железе” на машине, которая перестала загружаться или работает не под управлением Windows. Вам понадобится загрузочный носитель, который создан в мастере создания загрузочных носителей с использованием лицензионного ключа Кибер Бэкап. Информацию о том, как создать загрузочный носитель, см. в разделах *Загрузочные носители на основе Linux* или *Загрузочный носитель на основе Windows PE* соответственно.

Примечание

Для выполнения операций управления дисками в ОС Windows 10 и более поздних версий необходимо установить Управление Дисками.

Порядок выполнения операций управления дисками

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Для работы с локальной машиной щёлкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел *Регистрация носителя на сервере управления*.
3. Щёлкните **Управление дисками**.

> **Примечание**
>
> Операции по управлению дисками при загрузке с загрузочных носителей могут работать неправильно, если на машине настроены дисковые пространства.

Поддержка файловых систем

Загрузочный носитель поддерживает управление диском со следующими файловыми системами:

- FAT 16/32,
- NTFS.

Основные меры предосторожности

Во избежание возможного повреждения структуры тома или диска или потери данных следует принимать все необходимые меры предосторожности и следовать приведенным ниже простым рекомендациям.

1. Создайте резервную копию диска, на котором планируете создавать тома и управлять ими. Создание резервной копии самых важных данных на другом жестком диске, общем сетевом ресурсе или съемном носителе позволит работать с томами диска, не опасаясь за сохранность данных.
2. Проверьте диск, чтобы убедиться в его полной функциональности и отсутствии поврежденных секторов и ошибок файловой системы.
3. Не выполняйте операции с дисками/томами во время работы других программ, осуществляющих доступ к дискам на низком уровне.

Выбор операционной системы для управления дисками

На машине с двумя или несколькими операционными системами представление дисков и томов зависит от того, какая операционная система сейчас запущена. Один том в разных операционных системах может иметь разные буквы.

При выполнении операции управления дисками необходимо указать структуру диска, для которой будет отображаться операционная система. Для этого щёлкните имя операционной системы рядом с меткой **Структура диска** и выберите нужную операционную систему в открывшемся окне.

Операции с дисками

Используя загрузочный носитель, можно выполнить следующие операции управления диском:

- *Инициализация диска*: инициализация нового оборудования, добавленного в систему.
- *Клонирование базового диска*: передача всех данных с базового MBR-диска источника на целевой диск.
- *Преобразование диска: MBR в GPT*: преобразование таблицы разделов MBR в GPT.
- *Преобразование диска: GPT в MBR*: преобразование таблицы разделов GPT в MBR
- *Преобразование диска: базовый в динамический*: преобразование базового диска в динамический
- *Преобразование диска: динамический в базовый*: преобразование динамического диска в базовый.

Инициализация диска

Загрузочный носитель отображает неинициализированный диск в виде серого блока с серым значком, означающим, что диск не может использоваться системой.

Порядок инициализации диска

1. Правой кнопкой мыши щёлкните нужный диск и выберите пункт **Инициализировать**.
2. В окне **Инициализация диска** задайте схему разделов диска (MBR или GPT) и тип диска (базовый или динамический).
3. После нажатия кнопки **ОК** будет добавлена ожидающая операция инициализации диска.
4. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.
5. После инициализации пространство диска останется нераспределенным. Чтобы использовать его, необходимо *создать том* на нем.

Клонирование базового диска

Располагая полнофункциональным загрузочным диском на основе Linux, можно клонировать базовые MBR-диски. Клонирование диска недоступно на готовых загрузочных носителях, которые можно скачать, или на загрузочных носителях, созданных без использования лицензионного ключа.

Клонирование базовых дисков с носителя

1. Выполните загрузку с загрузочного носителя Киберпротект.
2. Чтобы клонировать диск локальной машины, щёлкните **Локальное управление этой машиной**. Для удаленных подключений см. раздел *Регистрация носителя на сервере управления*.
3. Щёлкните **Управление дисками**.
4. Отобразятся доступные диски. Правой кнопкой мыши щёлкните диск, который необходимо клонировать, и щёлкните **Клонировать базовый диск**.

   > **Примечание**
   >
   > Можно клонировать только полные диски. Клонирование разделов недоступно.

5. Отображается список возможных целевых дисков. Программа позволяет выбрать целевой диск, если его емкость будет достаточной для хранения всех данных диска-источника без потерь. Выберите целевой диск, а затем щёлкните **Далее**.

   Если целевой диск имеет больший размер, можно клонировать его ”как есть” или изменить размеры томов диска-источника с соблюдением пропорций (вариант по умолчанию), чтобы не оставлять нераспределенное пространство на целевом диске.

   Если целевой диск имеет меньший размер, доступно только пропорциональное изменение размера. Если безопасное клонирование невозможно даже с использованием пропорционального изменения размера, вы не сможете продолжить операцию.

   > **Важно**
   >
   > Если на целевом диске есть данные, будет выведено следующее предупреждение: ”*Выбран целевой диск с данными. Данные на его томах будут перезаписаны*”. Если продолжить операцию, все данные, которые в данный момент содержатся на целевом диске, будут безвозвратно утрачены.

6. Выберите, нужно ли копировать NT-подпись.

   При клонировании диска, который содержит системный том, необходимо сохранить загружаемость операционной системы на томе целевого диска. Это означает, что у операционной системы должны быть данные системного тома (например, буква тома) и эти данные должны совпадать с NT-подписью, которая хранится в записи MBR-диска. Однако два диска с одинаковой NT-подписью не могут корректно работать под управлением одной операционной системы.

При наличии двух дисков с одинаковой NT-подписью, на одном из которых находится системный том машины, при загрузке операционная система запускается с первого диска, обнаруживает такую же подпись на втором диске, затем автоматически формирует новую уникальную NT-подпись и назначает ее второму диску. В результате буквы всех томов на втором диске будут утеряны, все пути на этом диске станут недействительными и программы не смогут найти свои файлы. Операционная система на этом диске не сможет загружаться.

Чтобы сохранить загружаемость системы на томе целевого диска, можно выбрать одно из указанных ниже действий:

1. **Копировать NT-подпись**: укажите целевой диск с NT-подписью исходного диска, которая соответствует ключам реестра, которые также будут скопированы на целевой диск.

   Для этого установите флажок **Копировать NT-подпись**.

   Появится следующее предупреждение: ”Если на жестком диске есть операционная система, необходимо до следующего запуска машины удалить с нее диск-источник или целевой диск. В противном случае ОС будет запущена с первого из двух дисков, а ОС на втором диске станет незагружаемой.

   Флажок **Выключите машину после завершения операции** устанавливается и снимается автоматически.

2. **Оставить подпись NT**: для сохранения прежней подписи целевого диска и обновления операционной системы в соответствии с этой подписью.

   Для этого при необходимости снимите флажок **Копировать NT-подпись**.

   Флажок **Выключите машину после завершения операции** снимается автоматически.

7. Щёлкните **Завершить**, чтобы добавить ожидающую операцию клонирования диска.
8. В окне **Ожидающие операции** щёлкните **Подтвердить**, а затем — **Продолжить**. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.
9. Если выбран вариант, предусматривающий копирование NT-подписи, подождите, пока выполнится операция и перезагрузится компьютер, а затем отключите жесткий диск источника или целевой жесткий диск на машине.

Преобразование диска: MBR в GPT

Преобразование базового MBR-диска в базовый GPT-диск нужно в тех случаях, когда требуется:

- более 4 основных томов на одном диске;
- дополнительная защита диска от возможных повреждений данных.

Важно

Базовый MBR-диск, который содержит загрузочный том с текущей запущенной операционной системой, невозможно преобразовать в GPT.

Порядок преобразования базового MBR-диска в базовый GPT-диск

1. Правой кнопкой мыши щёлкните диск, который необходимо клонировать, и щёлкните **Преобразовать в GPT**.
2. Нажатие кнопки **ОК** добавит ожидающую операцию преобразования MBR в GPT.
3. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Примечание

На диске с GPT-разделами в конце области разделов выделяется место для области резервного копирования, в которой хранятся копии заголовка GPT и таблицы разделов. Если диск заполнен и размер тома невозможно уменьшить автоматически, операция преобразования MBR-диска в GPT не произойдет.

Данная операция необратима. Если на MBR-диске есть основной том и сначала диск преобразуется в GPT, а затем обратно в MBR, том станет логическим и не сможет использоваться как системный.

Преобразование динамического диска MBR в GPT

Загрузочный носитель не поддерживает прямое преобразование динамических дисков MBR в GPT. Однако можно достичь цели посредством следующих преобразований:

1. Преобразование *MBR-диска из динамического в базовый* с помощью операции **Преобразовать в базовый**.
2. Преобразование базовых дисков MBR в GPT с помощью операции **Преобразовать в GPT**.
3. Преобразование *GPT-диска из базового в динамический* с помощью операции **Преобразовать в динамический**.

Преобразование диска: GPT в MBR

Если планируется установить операционную систему, которая не поддерживает GPT-диски, их можно преобразовать в MBR-диски.

> **Важно**
>
> Базовый GPT-диск, который содержит загрузочный том с текущей запущенной операционной системой, невозможно преобразовать в MBR.

Порядок преобразования GPT в MBR

1. Правой кнопкой мыши щёлкните диск, который необходимо клонировать, и щёлкните **Преобразовать в MBR**.
2. Если нажать кнопку **ОК**, будет добавлена ожидающая операция преобразования GPT в MBR.
3. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

> **Примечание**
>
> После выполнения операции тома на этом диске станут логическими. Это изменение необратимо.

Преобразование диска из базового в динамический

Необходимость преобразовать базовый диск в динамический может возникнуть, если:

- планируется использовать диск как часть группы динамических дисков;
- для хранения данных требуется более высокий уровень надежности дисков.

Порядок преобразования базового диска в динамический

1. Правой кнопкой мыши щёлкните диск, который необходимо преобразовать, и щёлкните **Преобразовать в динамический**.
2. Нажмите кнопку **ОК**.

Преобразование будет выполнено незамедлительно, и в случае необходимости машина будет перезапущена.

Примечание

Динамический диск занимает последний мегабайт физического диска для хранения базы данных, включая четырехуровневое описание (том-компонент-раздел-диск) для каждого динамического тома. Если при преобразовании базового диска в динамический окажется, что базовый диск полностью заполнен и размер его томов невозможно уменьшить автоматически, операция завершится ошибкой.

Преобразование дисков с системными томами занимает определенное время, и в случае потери питания во время процедуры (непреднамеренного выключения машины или случайного нажатия кнопки Reset) диск может стать незагружаемым.

В отличие от диспетчера дисков Windows, эта программа гарантирует загружаемость **автономной ОС** на диске после выполнения операции.

Преобразование диска из динамического в базовый

Иногда требуется преобразовать динамические диски обратно в базовые (например, чтобы использовать операционную систему, не поддерживающую динамические диски).

Порядок преобразования динамического диска в базовый

1. Правой кнопкой мыши щёлкните диск, который необходимо преобразовать, затем щёлкните **Преобразовать в базовый**.
2. Нажмите кнопку **ОК**.

Преобразование будет выполнено незамедлительно, и в случае необходимости машина будет перезапущена.

Примечание

Эта операция недоступна для динамических дисков с томами следующих типов: составные (Spanned), чередующиеся (Striped) и RAID-5.

После преобразования последние 8 МБ дискового пространства будут зарезервированы для будущего преобразования диска из базового в динамический. В некоторых случаях возможный размер нераспределенного пространства и предлагаемый максимальный размер тома могут отличаться (например, если размер одного зеркала определяет размер другого или последние 8 МБ диска зарезервированы для будущего преобразования диска из базового в динамический).

Примечание

Преобразование дисков с системными томами занимает некоторое время, и в случае потери питания, случайного выключения машины или нажатия кнопки Reset во время процедуры диск может стать незагружаемым.

В отличие от диспетчера дисков Windows, эта программа гарантирует:

- безопасное преобразование динамического диска в базовый, если на нем содержатся тома **с данными** для простых и зеркальных томов;
- в мультизагрузочных системах — загружаемость системы, которая была **отключена от сети** во время операции.

Операции с томами

Используя загрузочный носитель, можно выполнить следующие операции с томами:

- *Создать том*: создает новый том.
- *Удалить том*: удаляет выбранный том.
- *Активировать*: выбранный том становится активным, чтобы машина могла загружаться с помощью установленной здесь ОС.
- *Изменить букву*: изменяет букву выбранного тома.
- *Изменить метку*: изменяет метку выбранного тома
- *Форматировать том*: форматирует том в файловую систему определенного типа

Типы динамических томов

Простой том

Том, созданный из свободного пространства на одном физическом диске. Он может состоять из одной области на диске или из нескольких областей, виртуально объединенных диспетчером логических дисков (LDM). Он не обеспечивает ни дополнительной надежности, ни улучшения скорости, ни увеличения размера.

Составной том

Том, созданный из свободного места на диске, виртуально связанного LDM из нескольких физических дисков. В один том можно включить до 32 дисков, обойдя таким образом аппаратные ограничения размера. Но если хотя бы один диск выйдет из строя, все данные будут потеряны. При этом ни одну часть составного тома нельзя удалить, не разрушив весь том. Таким образом, составной том не обеспечивает ни дополнительной надежности, ни улучшенной скорости ввода-вывода.

Чередующийся том

Том (называемый также RAID 0), который состоит из полос данных одинакового размера, записанных через каждый диск тома. Поэтому, для создания чередующегося тома необходимо два или более динамических дисков. Диски в чередующемся томе не обязательно должны быть идентичными, но на каждом диске, который планируется включить в том, должно быть доступное неиспользуемое пространство. Размер тома будет зависеть от размера наименьшего пространства. Доступ к данным на чередующемся томе обычно осуществляется быстрее, чем доступ к тем же данным на одном физическом диске, так как ввод-вывод распределяется более чем по одному диску.

Чередующиеся тома создаются для улучшения производительности, но не надежности — они не содержат избыточной информации.

Зеркальный том

Устойчивый к сбоям том, также называемый RAID 1, данные которого дублируются на два идентичных физических диска. Все данные с одного диска копируются на другой диск, обеспечивая избыточность данных. Зеркальным можно сделать почти любой том, включая системные и загрузочные тома, и, если один из дисков выйдет из строя, доступ к данным все равно можно будет получить с оставшихся дисков. К сожалению, аппаратные ограничения на размер и производительность при использовании зеркальных томов еще строже.

Зеркальный чередующийся том

Устойчивый к сбоям том, также иногда называемый RAID 1+0, сочетающий преимущества высокой скорости ввода-вывода чередующегося тома и надежность зеркального тома. Недостатком остается неотъемлемое следствие зеркальной архитектуры — низкое соотношение размера диска к размеру тома.

RAID-5

Устойчивый к сбоям диск, данные которого чередуются по всему массиву из трех или более дисков. Идентичность дисков необязательна, но на них должны быть одинакового размера блоки нераспределенного пространства, доступного на каждом диске тома. Четность (вычисляемое значение, с помощью которого можно реконструировать данные в случае сбоя) также чередуется по всему дисковому массиву и всегда хранится на другом диске отдельно от данных. В случае сбоя физического диска часть тома RAID-5, которая на нем находилась, можно воссоздать на основе оставшихся данных и четности. Том RAID-5 обеспечивает надежность и позволяет обойти ограничения размера физических дисков с более высоким соотношением размера диска к размеру тома, чем у зеркальных томов.

Создание тома

Новый том может потребоваться, чтобы:

- восстановить имеющуюся резервную копию именно в той конфигурации, которая существовала в момент копирования;
- хранить отдельно коллекции аналогичных файлов, например коллекцию MP3-файлов или видеофайлов на отдельном томе;
- хранить резервные копии (образы) других томов и дисков в специальном томе;
- установить ОС (или файл подкачки) на новом томе;
- добавить новое оборудование к машине.

Порядок создания тома

1. Правой кнопкой мыши щёлкните любое нераспределенное пространство на диске, затем щёлкните **Создать том**. Откроется мастер **Создание тома**.
2. Выберите тип тома. Доступны следующие параметры:
   - Базовый
   - Простой/составной
   - Чередующийся
   - Зеркальный
   - RAID-5

   Если текущая операционная система не поддерживает выбранный тип тома, будет возвращено предупреждение, а кнопка **Далее** будет отключена. Чтобы продолжить, необходимо выбрать другой тип тома.

3. Укажите нераспределенное пространство или выберите целевые диски.

    - Для основного тома укажите нераспределенное пространство на выбранном диске.
    - Для простого/составного тома выберите один или несколько целевых дисков.
    - Для зеркального тома выберите два целевых диска.
    - Для составного тома выберите два или более целевых дисков.
    - Для тома RAID-5 выберите три целевых диска

    Если создается динамический том и для его создания выбирается один или несколько базовых дисков, появится предупреждение о том, что выбранный диск будет автоматически преобразован в динамический.

4. Задание размера тома.

    Максимальное значение обычно соответствует максимально возможному объему нераспределенного пространства. В некоторых случаях предлагаемое максимальное значение может быть другим — например, если размер одного зеркала определяет размер другого или последние 8 МБ диска зарезервированы для будущего преобразования диска из базового в динамический.

    Можно выбрать расположение нового основного тома на диске, если объем нераспределенного пространства на этом диске превышает объем тома.

5. Настройка параметров тома.

    Можно задать букву тома (по умолчанию это будет первая свободная буква алфавита), а при необходимости и метку (по умолчанию метка не назначается). Кроме того, необходимо указать файловую систему и размер кластера.

    Возможные варианты типа файловой системы:

    - FAT16 (недоступен, если размер тома превышает 2 ГБ);
    - FAT32 (недоступен, если размер тома превышает 2 ТБ);
    - NTFS
    - Оставить том неформатированным.

    Задавая размер кластера, можно выбрать любое из предустановленных значений для каждой файловой системы. Размер кластера, который предлагается по умолчанию, наилучшим образом соответствует тому с выбранной файловой системой. Если задать размер кластера 64 КБ для FAT16/FAT32 или 8–64 КБ для NTFS, Windows сможет подключить том, но некоторые программы (например, программы установки) могут неправильно вычислить пространство на диске.

Если создается основной том, который можно сделать системным, можно будет выбрать тип тома — **Основной** (**Активный основной**) или **Логический**. Обычно для установки операционной системы на том выбирается тип **Основной**. Выберите **Активный** (значение по умолчанию), если нужно установить на этом томе операционную систему для загрузки при запуске машины. Если кнопка **Основной** не нажата, параметр **Активный** будет отключен. Если том предполагается использовать для хранения данных, выберите тип **Логический**.

> **Примечание**
>
> На базовом диске может быть до четырех основных томов. Если они уже существуют, необходимо будет преобразовать диск в динамический. В противном случае параметры **Активный** и **Основной** будут отключены, и можно будет выбрать только тип тома **Логический**.

6. В окне **Ожидающие операции** щёлкните **Подтвердить**, а затем — **Продолжить**. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Удаление тома

Порядок удаления тома

1. Правой кнопкой мыши щёлкните том, который необходимо удалить.
2. Щёлкните **Удалить том**.

> **Примечание**
>
> Вся информация об этом томе будет утрачена без возможности восстановления.

3. После нажатия кнопки **ОК** будет добавлена ожидающая операция удаления тома.
4. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Когда том удаляется, освобожденное пространство добавляется к нераспределенному дисковому пространству, Можно использовать его для создания нового тома или для изменения типа другого тома.

Активный том

Если основных томов несколько, необходимо указать один из них в качестве загрузочного. Для этого необходимо сделать том активным. Диск может иметь только один активный том.

Порядок установки тома как активного

1. Правой кнопкой мыши щёлкните нужный основной том на основном MBR-диске, а затем щёлкните **Пометить активным**.

   Если в системе нет других активных томов, будет добавлена ожидающая операция указания активного тома. Если в системе есть еще один активный том, появится предупреждение о том, что сначала нужно перевести прежний активный том в пассивное состояние.

   > **Примечание**
   >
   > Когда появляется новый активный том, буква прежнего активного тома может измениться и некоторые из установленных программ могут перестать работать.

2. После нажатия кнопки **ОК** в очередь будет добавлена операция установки активного тома.

   > **Примечание**
   >
   > Даже если в новом активном томе есть операционная система, в некоторых случаях будет невозможно загрузить машины с него. Необходимо подтвердить, что вы хотите сделать том активным.

3. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Изменение буквы тома

При загрузке операционная система Windows назначает буквы (C:, D: и т. д.) томам жестких дисков. Эти буквы используются приложениями и операционными системами для поиска файлов и папок в томах. Подключение дополнительного диска, а также создание и удаление тома на существующем диске может привести к изменению конфигурации системы. В результате некоторые приложения могут начать работать неправильно, а пользовательские файлы нельзя будет автоматически найти и открыть. Чтобы этого избежать, можно вручную изменить буквы томов, назначенные автоматически операционной системой.

Порядок изменения буквы тома, назначенной операционной системой:

1. Правой кнопкой мыши щёлкните нужный том и выберите пункт **Изменить букву**.
2. В окне **Изменить букву** выберите новую букву.
3. После нажатия кнопки **ОК** будет добавлена ожидающая операция назначения буквы тома.

4. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Изменение метки тома

Метка тома необязательна. Метка тома — это имя, которое присваивается тому для простоты опознания.

Порядок изменения метки тома:

1. Правой кнопкой мыши щёлкните нужный том и выберите пункт **Изменить метку**.
2. Введите новую метку в текстовом поле окна **Изменить метку** .
3. После нажатия кнопки **ОК** будет добавлена ожидающая операция изменения метки тома.
4. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Форматирование тома

Форматирование тома может потребоваться, если вы хотите изменить файловую систему тома в следующих целях:

- для экономии дополнительного пространства, которое иначе теряется из-за размеров кластеров в файловых системах FAT16 и FAT32;
- для быстрого и более или менее надежного способа уничтожения данных, содержащихся в этом томе.

Порядок форматирования тома

1. Правой кнопкой мыши щёлкните нужный том и выберите пункт **Формат**.
2. Выберите размер кластера и файловую систему. Возможные варианты типа файловой системы:
    - FAT16 (недоступен, если размер тома превышает 2 ГБ);
    - FAT32 (недоступен, если размер тома превышает 2 ТБ);
    - NTFS.
3. После нажатия кнопки **ОК** будет добавлена ожидающая операция форматирования тома.
4. Чтобы выполнить добавленную операцию, *подтвердите* ее. Если выйти из программы, не подтвердив операцию, эта операция будет отменена.

Ожидающие операции

Все операции считаются ожидающими, пока вы не введете и не подтвердите команду **Подтвердить**. Таким образом вы можете контролировать все запланированные операции, проверять все назначенные изменения, а при необходимости и отменять любые операции до их исполнения (при необходимости).

В представлении **Управление дисками** содержится панель инструментов со значками для запуска таких действий, как **Отменить**, **Вернуть** и **Подтвердить** для ожидающих операций. Эти действия можно также выполнить в меню **Управление дисками**.

Все запланированные операции добавляются к списку ожидающих операций.

Действие **Отменить** позволяет отменить последнюю операцию в списке. Это действие доступно для непустого списка.

Действие **Вернуть** позволяет восстановить последнюю ожидающую операцию, которая была отменена.

Действие **Подтвердить** позволяет перейти в окно **Ожидающие операции**, где можно просмотреть список ожидающих операций.

Чтобы выполнить их, щёлкните **Приступить**.

> **Примечание**
>
> После выбора операции **Приступить** отменить какое-либо действие или операцию невозможно.

Чтобы не подтверждать операцию, щёлкните **Отмена**. После отмены никакие изменения в список ожидающих операций не вносятся. Если выйти из программы, не подтвердив операции, ожидающие выполнения, эти операции будут отменены.

Настройка устройств iSCSI

В этом разделе описана настройка устройств iSCSI при работе с загрузочного носителя. После выполнения описанных ниже этапов можно использовать эти устройства так, как если бы они были подключены локально к машине, загружаемой с помощью загрузочного носителя.

Целевой сервер iSCSI (или **целевой портал**) — это сервер, на котором находится устройство iSCSI. **Целевое устройство iSCSI** — это компонент на целевом сервере; этот компонент обеспечивает совместное использование устройства и составляет список инициаторов iSCSI, которым разрешен доступ к устройству. **Инициатор iSCSI** — это компонент на машине; этот компонент обеспечивает взаимодействие между машиной и целевым устройством iSCSI. При настройке доступа к устройству iSCSI на машине, загруженной с помощью загрузочного носителя, необходимо указать целевой портал iSCSI устройства, а также один из инициаторов iSCSI, перечисленный на целевом устройстве. Если в

целевом объекте предоставлен общий доступ к нескольким устройствам, вы получите доступ ко всем ним.

Для добавления устройства iSCSI на загрузочный носитель на основе Linux

1. Нажмите **Инструменты** → **Настроить устройства iSCSI/NDAS**.
2. Нажмите кнопку **Добавить хост**.
3. Укажите IP-адрес и порт портала целевого устройства iSCSI, а также имя любого инициатора iSCSI, который разрешил доступ к устройству.
4. Если хост требует проверки подлинности, укажите имя пользователя и пароль.
5. Нажмите кнопку **ОК**.
6. Выберите целевое устройство iSCSI в списке и нажмите кнопку **Подключиться**.
7. Если в настройках целевого устройства iSCSI включена проверка подлинности CHAP, поступит запрос на учетные данные для доступа к целевому устройству iSCSI. Укажите имя пользователя и секрет целевого устройства, которые указаны в настройках целевого устройства iSCSI. Нажмите кнопку **ОК**.
8. Нажмите кнопку **Закрыть**, чтобы закрыть окно.

Для добавления устройства iSCSI на загрузочный носитель на основе PE

1. Нажмите **Инструменты** → **Запустить установку iSCSI**.
2. Выберите вкладку **Обнаружение**.
3. Под пунктом **Целевые порталы** нажмите кнопку **Добавить**, а затем укажите IP-адрес и порт портала целевого устройства iSCSI. Нажмите кнопку **ОК**.
4. Откройте вкладку **Общие**, нажмите кнопку **Изменить**, а затем укажите имя инициатора iSCSI, который разрешил доступ к устройству.
5. Откройте вкладку **Цели**, нажмите кнопку **Обновить**, выберите целевое устройство iSCSI в списке, а затем нажмите кнопку **Подключить**. Нажмите кнопку **ОК**, чтобы подключиться к целевому устройству iSCSI.
6. Если в настройках целевого устройства iSCSI включена проверка подлинности CHAP, отобразится ошибка **Сбой аутентификации**. В этом случае щёлкните **Подключиться**, затем щёлкните **Дополнительно**, установите флажок **Включить вход CHAP** и укажите имя пользователя и секрет целевого устройства, которые указаны в настройках целевого устройства iSCSI. Нажмите кнопку **ОК**, чтобы закрыть окно, затем нажмите кнопку **ОК**, чтобы подключиться к целевому устройству iSCSI.

7. Нажмите кнопку **ОК**, чтобы закрыть окно.

Диспетчер восстановления при загрузке (Startup Recovery Manager)

Диспетчер восстановления при загрузке — это загрузочный компонент, находящийся на системном диске Windows или в разделе `/boot` Linux и настроенный на запуск во время загрузки системы при нажатии клавиши `F11`. При его использовании не требуется отдельный носитель или сетевое подключение для запуска загрузочной утилиты аварийного восстановления.

Диспетчер восстановления при загрузке особенно полезен для мобильных пользователей. В случае сбоя перезагрузите машину, дождитесь появления запроса ”Press F11 for Startup Recovery Manager...” и нажмите клавишу `F11`. Программа запустится, и можно будет выполнить восстановление.

Кроме того, с помощью диспетчера можно ”на ходу” выполнять резервное копирование.

Некоторые производители оборудования резервируют за клавишей `F11` при включении или перезагрузке компьютера загрузку других компонентов, например, старт загрузочного меню. В этом случае сначала выберите в меню соответствующий пункт. Далее последует старт загрузчика Киберпротект, и на экране появится подсказка; после этого нажмите вновь `F11` для запуска диспетчера.

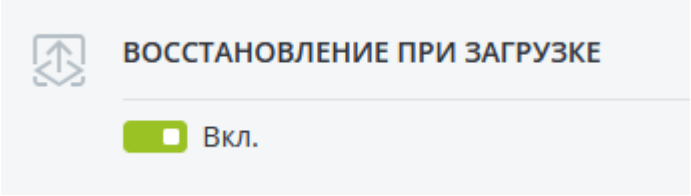
На машинах с установленным загрузчиком GRUB пользователь не нажимает клавишу `F11`, а выбирает **Startup Recovery Manager** в меню загрузки.

Активация диспетчера восстановления при загрузке

На машине, где запущен агент для Windows или агент для Linux, диспетчер восстановления при загрузке можно активировать с помощью веб-консоли Кибер Бэкап.

Порядок активации диспетчера восстановления при загрузке в веб-консоли Кибер Бэкап

1. Выберите машину, на которой нужно активировать диспетчер восстановления при загрузке.
2. Нажмите **Сведения**.
3. Включите переключатель **Восстановление при загрузке**.



4. Дождитесь окончания активации.

Порядок активации диспетчера восстановления при загрузке на машине без агента

1. Загрузите машину с загрузочного носителя.
2. Щёлкните **Инструменты** → **Активировать Восстановление при загрузке**.
3. Дождитесь окончания активации.

Что происходит при активации диспетчера восстановления при загрузке

Активация включает при загрузке подсказку ”Press F11 for Startup Recovery Manager...” (при отсутствии загрузчика GRUB) или добавляет пункт **Startup Recovery Manager** в меню загрузчика GRUB (при его наличии).

В некоторых случаях при нажатии клавиши `F11` используется встроенный в оборудование загрузчик меню. Тогда дождитесь старта встроенного загрузчика, в его меню выберите пункт с загрузчиком Киберпротект. В процессе старта с загрузчика Киберпротект при нажатии клавиши `F11` активируется загрузка диспетчера.

> **Примечание**
>
> Для активации диспетчера восстановления при загрузке системный диск (или раздел `/boot` в Linux) должен иметь по крайней мере 100 МБ свободного пространства.

За исключением случая, когда используется загрузчик GRUB и он установлен в основную загрузочную запись (MBR), активация диспетчера восстановления при загрузке перезаписывает основную загрузочную запись (MBR) своим собственным загрузочным кодом. Таким образом, при использовании загрузчиков сторонних производителей может потребоваться их повторное активирование.

В ОС Linux при использовании загрузчика, отличного от GRUB (такого как LILO), возможна его установка в загрузочную запись корневого (или загрузочного) раздела Linux вместо MBR до активации диспетчера восстановления при загрузке. В противном случае измените конфигурацию этого загрузчика вручную после активации.

Деактивация диспетчера восстановления при загрузке

Деактивация выполняется аналогично активации.

Деактивация отключает подсказку ”Press F11 for Startup Recovery Manager…” при загрузке (или пункт меню в GRUB).

Если **Восстановление при загрузке** не активировано, для восстановления системы, которая не смогла загрузиться, требуется выполнить одно из следующих действий:

- загрузить машину с отдельного загрузочного носителя;
- использовать сеть, чтобы загрузиться с PXE-сервера или службы удаленной установки Microsoft (RIS).

PXE-сервер Киберпротект

PXE-сервер Киберпротект служит для загрузки машин в загрузочные компоненты Киберпротект через сеть.

Загрузка по сети:

- устраняет потребность в специалисте для установки загрузочного носителя в систему, которая должна быть загружена;
- при групповых операциях снижает количество времени, требуемого для загрузки нескольких машин, по сравнению с использованием физического загрузочного носителя.

Загрузочные компоненты загружаются на PXE-сервер Киберпротект при помощи мастера создания загрузочных носителей Киберпротект. Чтобы загрузить загрузочные компоненты, запустите мастер создания загрузочных носителей и следуйте пошаговым инструкциям, описанным в разделе *Загрузочные носители на основе Linux*.

Загрузка нескольких машин с PXE-сервера Киберпротект имеет смысл, если в сети присутствует DHCP-сервер. При этом сетевые интерфейсы загруженных машин автоматически получат IP-адреса.

Установка PXE-сервера

> **Примечание**
>
> PXE-сервер может быть установлен только на машине с ОС Windows.

Порядок установки PXE-сервера

1. Войдите как администратор и запустите программу установки Кибер Бэкап.
2. [Необязательно] Чтобы изменить язык программы установки, щёлкните **Язык установки** (или **Setup language**).
3. Примите условия лицензионного соглашения и нажмите **Продолжить**.
4. Щёлкните **Настройка параметров установки**.

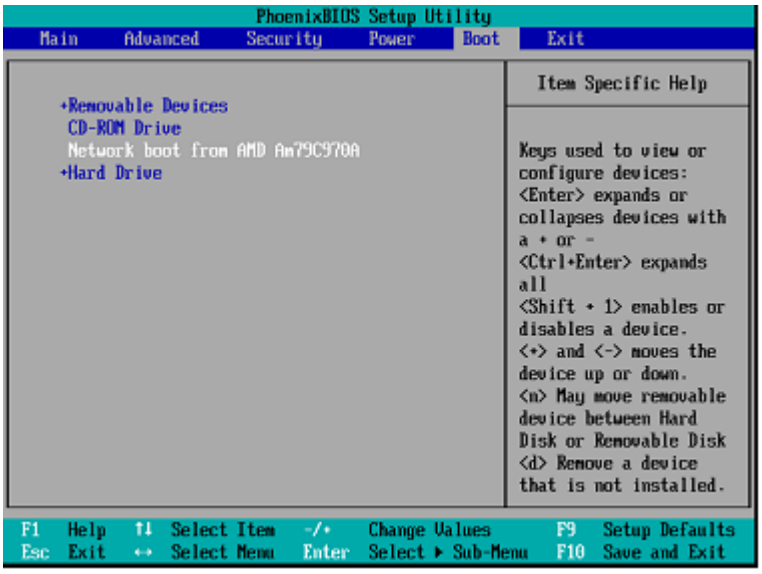
5. Рядом с пунктом **Устанавливаемые компоненты** щёлкните **Изменить**.
6. Установите флажок **PXE-сервер**. Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки. Чтобы продолжить, нажмите кнопку **Готово**.
7. [Необязательно] Измените другие настройки установки.
8. Нажмите **Установка**, чтобы продолжить установку.
9. После завершения установки нажмите кнопку **Закрыть**.

PXE-сервер Киберпротект запускается в виде службы сразу же после установки. Позже он автоматически стартует при каждом запуске операционной системы. Остановить или запустить PXE-сервер можно так же, как службу Windows.

Настройка машины на загрузку с PXE

В случае ”голого железа” достаточно, чтобы система BIOS машины поддерживала сетевую загрузку.

На тех машинах, операционная система которых расположена на жестком диске, система BIOS должна быть настроена так, чтобы сетевая интерфейсная плата была первым загрузочным устройством либо чтобы она предшествовала жесткому диску в приоритете загрузки. На следующем примере показана одна из приемлемых конфигураций BIOS. Если в машину не вставлен загрузочный носитель, будет производиться загрузка по сети.



В некоторых версиях BIOS необходимо сохранить изменения BIOS после включения сетевой интерфейсной платы, чтобы плата появилась в списке загрузочных устройств.

Если установлено несколько сетевых интерфейсных плат, убедитесь, что к плате, поддерживаемой BIOS, подключен сетевой кабель.

Работа в подсетях

Чтобы PXE-сервер мог работать в другой подсети (подключенной через коммутатор), необходимо настроить коммутатор для передачи трафика PXE. IP-адреса PXE-сервера настраиваются отдельно для каждого интерфейса с помощью вспомогательной службы IP таким же способом, как адреса DHCP-сервера. Дополнительные сведения см. в архиве документации Microsoft.

Защита приложений, сервисов, баз данных

В разделе описаны способы резервного копирования и восстановления данных различных приложений, сервисов и баз данных.

Защита приложений Microsoft

Защита Microsoft SQL Server и Microsoft Exchange Server

Есть два метода для защиты этих приложений:

- **Резервная копия базы данных**

  Это резервное копирование на уровне файлов базы данных и метаданных, связанных с ней. Базы данных можно восстановить в запущенное приложение или как файлы.

- **Резервное копирование с поддержкой приложений**

  Это резервное копирование на уровне дисков, при котором также выполняется сбор метаданных приложений. Эти метаданные позволяют выполнить обзор и восстановление данных приложений, не восстанавливая весь диск или том. Диск или том также можно восстановить полностью. Это означает, что можно использовать единое решение и один план защиты как для аварийного восстановления, так и для защиты данных.

Для Microsoft Exchange Server вы можете выбрать **Резервное копирование почтового ящика**. При выборе данного параметра будут созданы резервные копии отдельных почтовых ящиков посредством протокола Exchange Web Services. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server. Резервное копирование почтовых ящиков поддерживается для Microsoft Exchange Server 2013 и более поздних версий.

Защита Microsoft SharePoint

Ферма Microsoft SharePoint состоит из серверов веб-интерфейса, на которых выполняются службы SharePoint, серверов баз данных, на которых выполняется Microsoft SQL Server и (необязательно) серверов приложений, которые разгружают серверы веб-интерфейса от некоторых служб SharePoint. Некоторые серверы веб-интерфейса и серверы приложений могут быть идентичны друг другу.

Чтобы защитить всю ферму SharePoint, выполните указанные ниже действия:

- Создайте резервные копии серверов базы данных, выполнив резервное копирование с поддержкой приложений.

- Создайте резервные копии всех уникальных серверов веб-интерфейса и серверов приложений, выполнив обычное резервное копирование на уровне дисков.

Резервные копии всех серверов должны быть выполнены по одному расписанию.

Чтобы защитить только содержимое, можно создать резервные копии баз данных по отдельности.

Защита контроллера домена

Машину под управлением доменных служб Active Directory можно защитить резервным копированием с поддержкой приложений. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

Восстановление приложений

В таблице приведена сводка доступных методов восстановления приложений.

	Из резервной копии базы данных	**Из резервной копии с поддержкой приложений**	**Из резервной копии диска**
Microsoft SQL Server	• *Базы данных в запущенный экземпляр SQL Server* • *Базы данных как файлы*	• *Вся машина* • *Базы данных в запущенный экземпляр SQL Server* • *Базы данных как файлы*	*Вся машина*
Microsoft Exchange Server	• *Базы данных в запущенный Exchange* • *Базы данных как файлы* • *Фрагментарное восстановление в запущенный Exchange*[1]	• *Вся машина* • *Базы данных в запущенный Exchange* • *Базы данных как файлы* • *Фрагментарное восстановление в запущенный Exchange**	*Вся машина*

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

	Из резервной копии базы данных	Из резервной копии с поддержкой приложений	Из резервной копии диска
Серверы базы данных Microsoft SharePoint	• *Базы данных в запущенный экземпляр SQL Server* • *Базы данных как файлы* • Фрагментарное восстановление с использованием SharePoint Explorer	• *Вся машина* • *Базы данных в запущенный экземпляр SQL Server* • *Базы данных как файлы* • Фрагментарное восстановление с использованием SharePoint Explorer	*Вся машина*
Интерфейсные веб-серверы Microsoft SharePoint	—	—	*Вся машина*
Доменные службы Active Directory	—	*Вся машина*	—

Предварительные требования

Перед настройкой резервного копирования приложений убедитесь, что перечисленные ниже требования выполнены.

Чтобы проверить состояние модуля записи VSS, используйте команду `vssadmin list writers`.

Общие требования

Для Microsoft SQL Server убедитесь, что выполнены указанные ниже требования:

- Запущен хотя бы один экземпляр Microsoft SQL Server.
- Модуль записи SQL для VSS включен.

Для Microsoft Exchange Server убедитесь, что выполнены указанные ниже требования:

- Запущена служба банка данных Microsoft Exchange.
- Установлена оболочка Windows PowerShell версии 2.0 или новее.
- Установлена платформа Microsoft .NET Framework версии 3.5 или новее.
- Модуль записи Exchange для VSS включен.

[1] Фрагментарное восстановление также доступно из резервной копии почтового ящика.

Примечание

Для работы агента для Exchange требуется временное хранилище данных. По умолчанию временные файлы находятся в папке `%ProgramData%\Acronis\Temp`. Убедитесь, что объем свободного пространства на томе, где расположена папка `%ProgramData%`, составляет как минимум 15 % от размера базы данных Exchange. Как вариант, можно изменить расположение временных файлов перед созданием резервных копий Exchange.

На контроллере домена убедитесь, что модуль записи Active Directory для VSS включен.

При создании плана защиты убедитесь в следующем:

- Для физических машин включен параметр резервного копирования *Служба теневого копирования томов (VSS)*.
- Для виртуальных машин включен параметр резервного копирования *Служба теневого копирования томов (VSS) для виртуальных машин*.

Дополнительные требования для операций резервного копирования с поддержкой приложений

При создании плана защиты убедитесь, что для резервного копирования выбран параметр **Вся машина**. В плане защиты необходимо отключить параметр резервного копирования **Sector-by-sector (Посекторно)**; в противном случае невозможно будет восстановить данные приложения из таких резервных копий. Если данный план выполнен в режиме **Sector-by-sector (Посекторно)** из-за автоматического перехода в этот режим, то и в этом случае восстановить данные приложения будет невозможно.

Требования для виртуальных машин ESXi

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для VMware, убедитесь, что выполнены следующие условия:

- Виртуальная машина для резервного копирования соответствует требованиям совместимого с приложениями резервного копирования и восстановления, которые перечислены в статье Windows Backup Implementations (Реализации резервного копирования Windows) из документации для VMware.
- На машине установлен и обновлен набор утилит VMware Tools.
- Учетные записи пользователей (UAC) отключены на машине. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

Требования для виртуальных машин Hyper-V

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для Hyper-V, убедитесь, что выполнены следующие условия:

- В качестве гостевой операционной системы используется Windows Server.
- Виртуальная машина не имеет динамических дисков.
- Между хостом Hyper-V и гостевой операционной системой установлено сетевое подключение. Это необходимо для выполнения удаленных запросов WMI в виртуальной машине.
- Учетные записи пользователей (UAC) отключены на машине. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).
- Конфигурация виртуальной машины соответствует следующем критерию:
  - Службы интеграции Hyper-V установлены и обновлены. Должно быть установлено критическое обновление
  - В настройках виртуальной машины включен параметр **Управление** → **Службы интеграции** → **Резервное копирование (контрольная точка тома)**.
  - Для Hyper-V 2012 R2 и более поздних версий: виртуальная машина не имеет контрольных точек.
  - Для Hyper-V 2012 R2 и более поздних версий: виртуальная машина имеет контроллер SCSI (проверьте **Настройки** → **Оборудования**).

Резервное копирование баз данных Microsoft SQL Server и Microsoft Exchange Server

Прежде чем приступить к созданию резервных копий баз данных, убедитесь, что выполнены требования, перечисленные в разделе *Предварительные требования*.

Выберите базы данных, как указано ниже, а затем укажите другие настройки плана защиты *как требуется*.

Выбор баз данных Microsoft SQL Server

Резервная копия базы данных Microsoft SQL Server содержит файлы базы (.mdf, .ndf), журналы (.ldf) и другие связанные файлы. Их резервные копии создаются с помощью службы SQL Writer. Она должна быть запущена в момент, когда служба теневого копирования томов (VSS) отправляет запрос на резервное копирование или восстановление.

После каждого успешного резервного копирования выполняется сокращение журналов транзакций Microsoft SQL Server. Усечение журнала Microsoft SQL Server можно отключить в *параметрах плана защиты*.

Порядок выбора баз данных Microsoft SQL Server

1. Нажмите **Устройства** → **Microsoft SQL**.

   Программное обеспечение отобразит дерево групп Always On Availability Groups (AAG) сервера SQL Server, машины, на которых запущен Microsoft SQL Server, экземпляры SQL Server и базы данных.

2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щёлкните элементы списка, расположенного справа от дерева.

3. Выберите данные, резервную копию которых необходимо создать. Выберите AAGs, машины, на которых запущен Microsoft SQL Server, экземпляры Microsoft SQL Server или отдельные базы данных.

   - При выборе AAG, для всех баз данных, включенных в выбранную AAG, будет создана резервная копия. Дополнительные сведения о резервном копировании групп AAG или отдельных баз данных AAG см. в разделе *Защита групп Always On Availability Groups (AAG)*.
   - При выборе машины, на которой запущен SQL Server, будет создана резервная копия всех баз данных, подключенных к экземпляру Microsoft SQL Server.
   - При выборе экземпляра Microsoft SQL Server для всех баз данных, подключенных к выбранному экземпляру, будет создана резервная копия.
   - Если выбрать отдельные базы, будут созданы резервные копии только для них.

4. Нажмите кнопку **Резервное копирование**. Если потребуется, введите учетные данные для доступа к SQL Server. Соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **системный администратор** в каждом из экземпляров, для которых создается резервная копия.

Выбор данных Microsoft Exchange Server

Кибер Бэкап позволяет выполнить резервное копирование следующих элементов данных Microsoft Exchange Server: баз данных, групп обеспечения доступности баз данных (DAG). Перечень поддерживаемых версий Microsoft Exchange Server приведён в разделе *Поддерживаемые почтовые сервисы*.

При полном резервном копировании в копию включаются все выбранные данные Exchange.

Инкрементная резервная копия содержит измененные блоки файлов баз данных, файлы контрольных точек, а также небольшое количество файлов журналов, более новых по отношению к соответствующим контрольным точкам базы. Поскольку в резервную копию включаются изменения, внесенные в базу данных, добавлять в нее все записи из журналов транзакций с момента предыдущего резервного копирования не нужно. После восстановления воспроизводится только журнал, более новый, чем контрольная точка. Это позволяет ускорить восстановление и обеспечить резервное копирование базы, даже если включено циклическое ведение журнала.

После каждого успешного резервного копирования выполняется усечение файлов журнала транзакций.

Порядок выбора данных Exchange

1. Нажмите **Устройства** → **Microsoft Exchange**.

   Программное обеспечение отобразит дерево групп обеспечения доступности баз данных (DAG) Exchange, машины, на которых запущен Exchange, и базы данных Exchange. Если агент для Exchange настроен, как описано в разделе *Резервная копия почтового ящика*, в этом дереве также отображаются почтовые ящики.

2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щёлкните элементы списка, расположенного справа от дерева.

3. Выберите данные, резервную копию которых необходимо создать.

   - При выборе DAG создаются резервные копии одной из копий каждой кластеризованной базы данных. Дополнительные сведения о резервном копировании групп DAG см. в разделе:doc:*Защита групп обеспечения доступности базы данных (DAG) <protecting-database-availability-groups>*.
   - При выборе машины, на которой запущен сервер Exchange, будет создана резервная копия всех баз данных, подключенных к серверу.
   - Если выбрать отдельные базы, будут созданы резервные копии только для них.
   - Если агент для Exchange настроен, как описано в разделе *Резервное копирование почтовых ящиков*, можно *выбрать почтовые ящики для резервного копирования*.

4. Если потребуется, введите учетные данные для доступа к информации.

5. Щёлкните **Защитить**.

Защита группы Always On Availability Groups (AAG)

Функция отказоустойчивой кластеризации Windows Server (WSFC) позволяет настроить Microsoft SQL Server с высоким уровнем доступности посредством избыточности на уровне экземпляра (экземпляр отказоустойчивого кластера, FCI) или на уровне базы данных (Always On Availability Group, AAG). Оба метода можно сочетать.

В экземпляре отказоустойчивого кластера базы данных Microsoft SQL Server расположены в общем хранилище. Доступ к этому хранилищу возможен только с активного узла кластера. При сбое активного узла происходит переход, и активным становится другой узел.

В группе обеспечения доступности все реплики баз данных располагаются на разных узлах. Если основная реплика становится недоступна, основная роль назначается дополнительной реплике, расположенной на другом узле.

Таким образом, уже сами кластеры являются решением по аварийному восстановлению. Однако в некоторых случаях кластеры не могут обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера.

Поддерживаемые конфигурации кластеров

Это программное обеспечение поддерживает *только* группы обеспечения доступности Always On SQL Server (AAG) для SQL Server 2012 или более поздних версий. Прочие конфигурации кластеров, такие как, например, Failover Cluster Instances, зеркальное отображение базы данных и доставка журналов, *не* поддерживаются.

Число агентов для резервного копирования и восстановления данных кластера

Для успешного резервного копирования и восстановления данных кластера необходимо установить агент для SQL на каждом узле кластера WSFC.

В AAG включено резервное копирование баз данных

1. Установите агент для SQL на каждый узел кластера WSFC.

> **Примечание**
>
> После установки агента на одном из узлов программное обеспечение отобразит AAG и ее узлы в поле **Устройства** → **Microsoft SQL** → **Базы данных**. Для установки агента для SQL на остальных узлах выберите AAG, нажмите **Сведения**, после чего нажмите **Установить агент** возле каждого

узла.

2. Выберите AAG или набор баз данных для создания резервной копии в соответствии с инструкциями *Выбор баз данных Microsoft SQL Server*.

   Чтобы создать резервную копию всех баз данных AAG, необходимо выбрать саму AAG. Чтобы создать резервную копию набора баз данных, определите этот набор во всех узлах AAG.

   Предупреждение

   Набор баз данных должен быть одним на всех узлах. Если хотя бы один набор будет отличаться от всех остальных или будет определен не на всех узлах, резервное копирование кластера будет работать неправильно.

3. Настройте параметр резервного копирования *Способ резервного копирования кластера*.

Восстановление баз данных, включенных в AAG

1. Выберите базы данных, которые необходимо восстановить, а затем выберите желаемую точку восстановления данных.

   При переходе **Устройства** → **Microsoft SQL** → **Базы данных**, выборе кластеризованной базы данных и нажатии **Восстановить**, программное обеспечение отобразит только те точки восстановления, которые соответствуют временам создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных — выбор резервной копии всей AAG *на вкладке "Хранилища резервных копий"*. Имена резервных копий AAG помечены особым значком и составляются по следующему шаблону: `<имя AAG> - <имя плана защиты>`.

2. Для конфигурирования восстановления выполните действия, описанные в разделе *Восстановление баз данных Microsoft SQL Server* (начиная с шага 5).

   Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

   Важно

   База данных, включенная в группу Always On Availability Group, не может быть перезаписана во время восстановления, поскольку это запрещено правилами Microsoft SQL Server. Необходимо

> восстановить базу данных как новую, не входящую в AAG. После завершения восстановления можно воссоздать исходную конфигурацию AAG.

Рекомендуется следующая последовательность действий, чтобы восстановить базу данных, входящую в AAG:

1. Восстановить базу данных как новую (то есть под другим именем и в отдельную пустую папку).
2. Проверить восстановленную базу данных средствами SQL Server Management Studio.
3. Удалить старую базу данных.
4. Переименовать восстановленную базу данных.
5. Добавить восстановленную базу данных в AAG.

Защита групп обеспечения доступности базы данных (DAG)

Обзор кластеров Exchange Server

Основная идея кластеров Exchange — обеспечить высокую доступность базы данных с быстрым переходом к реплике и без потери данных. Обычно для этого одна или несколько копий баз данных находятся на элементах (узлах) кластера. В случае отказа узла кластера, на котором находится активная копия базы данных, или самой активной копии базы данных, другой узел кластера, содержащий пассивную копию, автоматически берет на себя операции с отказавшего узла и предоставляет доступ к службам Exchange с минимальным простоем. Таким образом, уже сами кластеры являются решением по аварийному восстановлению.

Однако в некоторых случаях решение с использованием отказоустойчивых кластеров не может обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера.

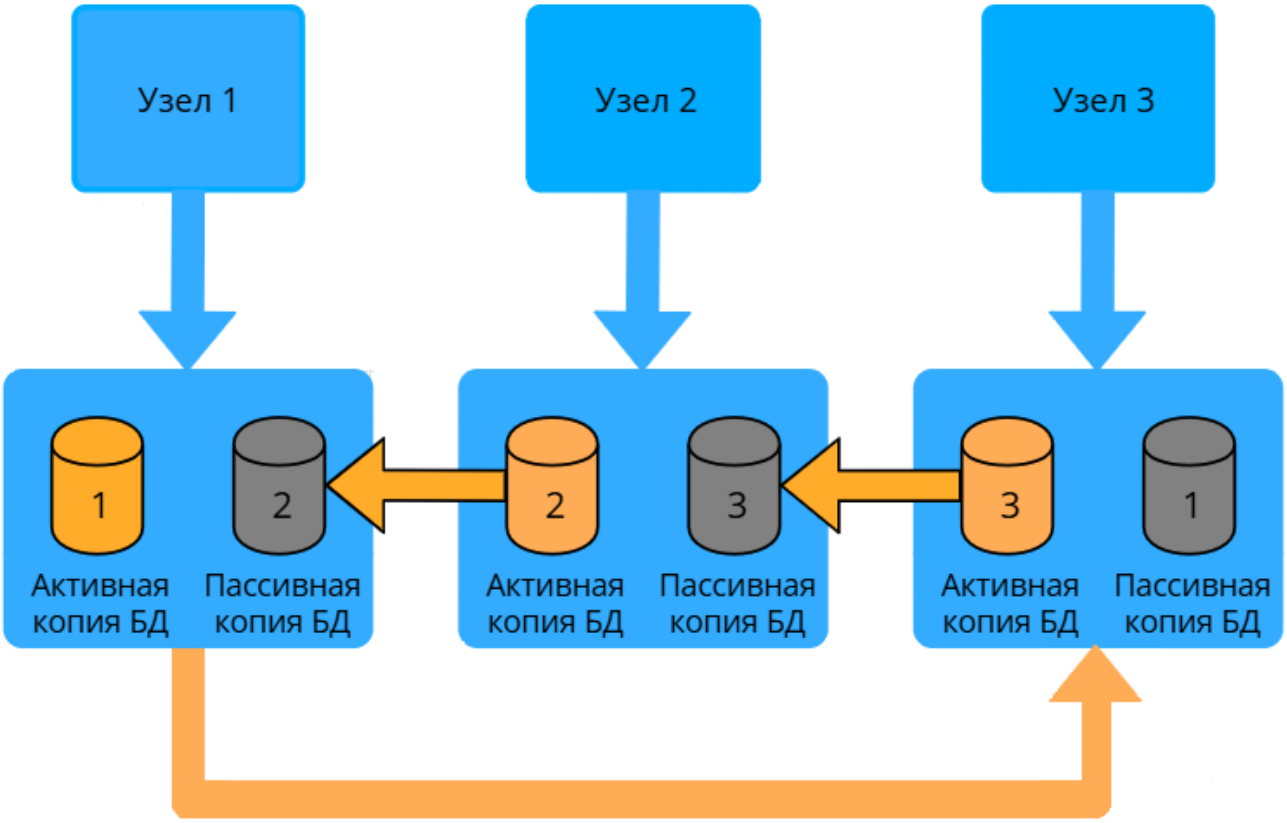
Резервное копирование с поддержкой кластеров

Используя резервное копирование с поддержкой кластеров, вы создаете только одну копию кластеризированных данных. Если данные меняют свое расположение в кластере (например, из-за переключения или перехода к реплике), программное обеспечение отслеживает все перемещения этих данных и благополучно создает их резервную копию.

Поддерживаемые конфигурации кластеров

Резервное копирование с поддержкой кластеров поддерживается *только* для группы обеспечения доступности баз данных (DAG) в Microsoft Exchange Server 2013 или более поздних версиях. При этом поддерживаются базы данных с включенной функцией MetaCache Database (MCDB), в том числе гранулярное восстановление писем из таких баз данных.

Группа DAG включает до 16 серверов почтовых ящиков Exchange. На любом узле может располагаться копия базы данных почтовых ящиков с любого другого узла. Каждый узел может содержать пассивные и активные копии базы данных. Может быть создано до 16 копий каждой базы данных.



Число агентов для резервного копирования и восстановления данных кластера

Для успешного резервного копирования и восстановления кластеризованных баз данных необходимо установить агент для Exchange на каждом узле кластера Exchange.

Примечание

После установки агента на одном из узлов веб-консоль Кибер Бэкап отобразит DAG и ее узлы в поле **Устройства** → **Microsoft Exchange** → **Базы данных**. Для установки агента для Exchange на остальных

узлах выберите DAG, нажмите **Сведения**, после чего нажмите **Установить агент** возле каждого узла.

Создание резервной копии данных кластера Exchange

1. При создании плана защиты выберите DAG в соответствии с инструкциями в разделе *Выбор данных Microsoft Exchange Server*.
2. Настройте параметр резервного копирования *Способ резервного копирования кластера*.
3. Укажите другие *необходимые* настройки плана защиты.

Важно

Для резервного копирования с поддержкой кластеров необходимо выбрать саму группу обеспечения доступности баз данных. Если выбрать отдельные узлы или базы данных в группе обеспечения доступности баз данных, то будет создана резервная копия только для выбранных элементов, а параметр **Способ резервного копирования кластера** будет проигнорирован.

Восстановление данных кластера Exchange

1. Выберите точку восстановления для базы данных, которую необходимо восстановить. Резервное копирование всего кластера для восстановления невозможно.

   Если в разделе **Устройства** → **Microsoft Exchange** → **Базы данных** → **<имя кластера>** → **<имя узла>** выбрать копию кластеризованной базы данных и нажать кнопку **Восстановить**, будут показаны только те точки восстановления, которые соответствуют времени создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных — выбор соответствующей резервной копии *на вкладке "Хранилища резервных копий"*.

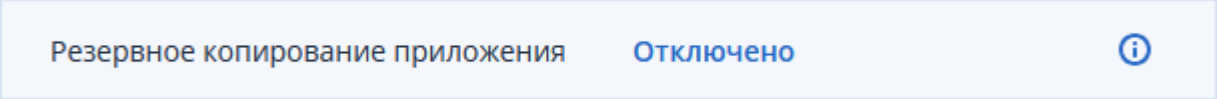
2. Выполните действия, описанные в разделе "Восстановление баз данных Exchange", начиная с шага 5.

   Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

Резервное копирование с поддержкой приложений

Резервная копия на уровне дисков с поддержкой приложений доступна для физических машин, виртуальных машин ESXi и виртуальных машин Hyper-V.

При резервном копировании машины, на которой выполняется Microsoft SQL Server, Microsoft Exchange Server или доменные службы Active Directory, включите **Резервное копирование приложения** для дополнительной защиты данных этих приложений.



Необходимость резервного копирования с поддержкой приложений

Используя резервное копирование с поддержкой приложений, вы обеспечиваете следующее:

1. Резервные копии приложений в согласованном состоянии, поэтому доступны немедленно после восстановления машины.
2. Можно восстановить базы данных SQL и Exchange, почтовые ящики и элементы почтовых ящиков без восстановления всей машины.
3. После каждого успешного резервного копирования выполняется сокращение журналов транзакций SQL. Усечение журнала SQL можно отключить в *параметрах плана защиты*. Журналы транзакций Exchange сокращаются только на виртуальных машинах. Чтобы урезать размер журналов транзакций Exchange на физической машине, можно включить *параметр полного резервного копирования VSS*.
4. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

Требования резервного копирования с поддержкой приложений

На физической машине кроме агента для Windows должен быть установлен агент для SQL и (или) агент для Exchange.

На виртуальной машине наличие установленного агента не требуется. Предполагается, что резервная копия виртуальной машины создана агентом для VMware (Windows) или агентом для Hyper-V.

Агент для VMware (виртуальное устройство) может создать резервные копии с поддержкой приложений, но не может восстановить из них данные приложения. Чтобы восстановить данные приложения в виде файлов, созданных этими агентами, необходимо иметь агент для VMware (Windows), агент для SQL (Windows) или агент для Exchange (Windows) на машине с доступом к хранилищу, в котором хранятся

резервные копии. При настройке восстановления данных приложения выберите точку восстановления на вкладке **Хранилища резервных копий**, а затем выберите эту машину в списке **Машина для обзора**. Для восстановления данных Microsoft SQL Server или Microsoft Exchange Server в рабочий экземпляр приложения необходима установка соответствующих агентов на сервер с запущенным приложением.

Другие требования перечислены в разделах *Предварительные требования* и *Необходимые права пользователя*.

Требуемые права пользователя

Резервные копии с поддержкой приложений содержат метаданные приложений с поддержкой VSS, которые представлены на диске. Чтобы агент мог получить доступ к метаданным, для него необходима учетная запись с соответствующими правами, которые перечислены ниже. Пользователю поступает запрос на указание учетной записи при включении резервного копирования приложений.

- Для SQL Server: соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **sysadmin** в каждом из экземпляров, для которых создается резервная копия.
- Для Active Directory: данная учетная запись должна быть администратором домена.

Дополнительные требования для виртуальных машин

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для VMware или агентом для Hyper-V, убедитесь, что на этой машине отключен контроль учетных записей (UAC). Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

Резервная копия почтового ящика

Резервное копирование почтовых ящиков поддерживается для Microsoft Exchange Server 2013 и более поздних версий.

Резервная копия почтового ящика доступна, если на сервере управления зарегистрирован по меньшей мере один агент для Exchange. Этот агент должен быть установлен на машине, которая находится в одном лесу Active Directory с сервером Microsoft Exchange Server.

Перед выполнением резервного копирования почтовых ящиков вы должны подключить агент для Exchange к машине с серверной ролью (CAS) **Client Access** сервера Microsoft Exchange Server. В Exchange 2016 и более поздних версиях роль CAS не устанавливается отдельно. Она устанавливается автоматически как часть роли сервера почтовых ящиков. Таким образом, можно подключить агент к любому серверу, которому присвоена **роль почтовых ящиков**.

Как подключить агент для Exchange к CAS

1. Нажмите **Устройства** → **Добавить**.
2. Нажмите **Microsoft Exchange Server**.
3. Щёлкните **Почтовые ящики Exchange**.

   Если на сервере управления не зарегистрировано ни одного агента для Exchange, программное обеспечение попросит вас установить агент. После установки повторите эту процедуру с шага 1.
4. [Необязательно] Если на сервере управления зарегистрировано несколько агентов для Exchange, щёлкните **Агент** и измените агент, который выполнит резервное копирование.
5. На сервере **Client Access Server** укажите полное доменное имя машины (FQDN), на которой включена роль **Клиентский доступ** Microsoft Exchange Server.

   В Exchange 2016 и более поздних версиях службы клиентского доступа автоматически устанавливаются в рамках роли сервера почтовых ящиков. Таким образом, можно указать любой сервер, которому присвоена **роль почтовых ящиков**. В этом разделе подобный сервер обозначается аббревиатурой CAS.
6. В пункте **Тип аутентификации**, выберите тип аутентификации, используемый CAS. Можно выбрать **Kerberos** (по умолчанию) или **Базовый**.
7. [Только для базовой аутентификации] Выберите используемый протокол. Можно выбрать **HTTPS** (по умолчанию) или **HTTP**.
8. [Только для базовой аутентификации с протоколом HTTPS] Если CAS использует сертификат SSL, полученный от сертифицирующей организации, и вы желаете, чтобы программное обеспечение проверяло сертификат SSL при подключении к CAS, установите флажок **Проверять сертификат SSL**. В противном случае пропустите этот шаг.
9. Укажите учетные данные учетной записи, которые будут использоваться для доступа к CAS. Требования к этой учетной записи указаны в разделе *Требуемые права пользователя*.
10. Нажмите кнопку **Добавить**.

В результате почтовый ящик будет находиться по пути **Устройства** → **Microsoft Exchange** → **Почтовые ящики**.

Выбор почтовых ящиков сервера Exchange

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана защиты *как требуется*.

Выбор почтовых ящиков Exchange

1. Нажмите **Устройства** → **Microsoft Exchange**.

   Программное обеспечение отобразит дерево баз данных и почтовых ящиков Exchange

2. Нажмите **Почтовые ящики**, после чего выберите почтовые ящики, для которых необходимо создать резервные копии.

3. Нажмите кнопку **Резервное копирование**.

Требуемые права пользователя

Чтобы получить доступ к почтовым ящикам, агенту для Exchange необходима учетная запись с соответствующими правами. При настройке различных операций с почтовыми ящиками пользователю поступает запрос на указание учетной записи.

Членство учетной записи в группе ролей **Управление организацией** позволяет получить доступ к любому почтовому ящику, включая почтовые ящики, которые будут созданы в будущем.

Восстановление баз данных Microsoft SQL Server

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить базы данных SQL в экземпляр SQL Server, если на машине с этим экземпляром установлен агент для SQL. Для этого потребуется указать данные учетной записи, которая входит в группу **Операторы архива** или **Администраторы** на этой машине, а также имеет роль **sysadmin** на целевом экземпляре.

Базы данных также можно восстанавливать в виде файлов. Это может быть полезным при необходимости извлечь данные для интеллектуального анализа данных, аудита или дальнейшей обработки с использованием инструментов сторонних поставщиков. Можно присоединить файлы базы данных SQL к экземпляру SQL Server, как описано в теме *Подключение баз данных SQL Server*.

Если используется только агент для VMware (Windows), то единственный доступный метод восстановления — восстановить базы данных как файлы. Невозможно восстановить базы данных с помощью агента для VMware (виртуальное устройство).

Системные базы данных восстанавливаются в целом так же, как и пользовательские. Особенности этой

процедуры описаны в разделе *Восстановление системных баз данных*.

Восстановление базы данных в запущенный экземпляр SQL Server

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** → **Microsoft SQL** и затем выберите базы данных, которые необходимо восстановить.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для SQL, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** → **Базы данных SQL**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** → **Базы данных в экземпляр**.
5. По умолчанию данные восстанавливаются в исходных базах. Если исходная база данных не существует, она будет создана. Можно выбрать другой экземпляр сервера SQL Server (запущенный на той же машине), в который требуется восстановить базы данных.

   Восстановление данных в другой базе на том же экземпляре

   1. Щёлкните имя базы данных.

2. В поле **Восстановить в** выберите вариант **Новая база данных**.
3. Укажите имя новой базы данных.
4. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов. В противном случае возникнет ошибка из-за конфликта новых и существующих файлов с идентичными именами.

6. [Необязательно] [Недоступно для базы данных, восстановленной в другой экземпляр базы данных или в свой исходный экземпляр как новая база данных] Чтобы изменить состояние базы данных после восстановления, щёлкните ее имя и выберите один из перечисленных ниже вариантов.

   - **Готово к использованию (RESTORE WITH RECOVERY)** (по умолчанию)

     После завершения восстановления база данных будет готова к использованию. Пользователи будут иметь к ней полный доступ. Программа выполнит откат всех незафиксированных транзакций восстановленной базы данных, хранящихся в журналах транзакций. Вы не сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL.

   - **В нерабочем состоянии (RESTORE WITH NORECOVERY)**

     Использовать базу данных после завершения восстановления будет невозможно. Пользователи не будут иметь к ней доступа. Программа сохранит все незафиксированные транзакции восстановленной базы данных. Вы сможете восстановить дополнительные журналы транзакций из резервных копий в собственном формате Microsoft SQL и таким образом достичь нужной точки восстановления (Point-in-Time Recovery, PITR).

     Восстановление дополнительных журналов транзакций из резервных копий в формате Microsoft SQL Server доступно при отключении в плане резервного копирования параметра *Сокращение журнала Microsoft SQL Server*. Сведения о восстановлении журналов транзакций см. в документации Microsoft.

   - **Только чтение (RESTORE WITH STANDBY)**

     После завершения восстановления база данных будет доступна пользователям только для чтения. Программа выполнит откат всех незафиксированных транзакций. Однако действия по откату будут сохранены во временный резервный файл, чтобы можно было вернуть базу данных в состояние до восстановления.

     Это значение в основном используется для определения точки во времени, где произошла ошибка SQL Server.

7. Щёлкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

Восстановление баз данных SQL в виде файлов

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** → **Microsoft SQL** и затем выберите базы данных, которые необходимо восстановить.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для SQL или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления баз данных SQL.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** → **Базы данных SQL**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить как файлы**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** → **Базы данных как файлы**.
5. Нажмите **Обзор** и затем выберите локальную или сетевую папку, в которую требуется сохранить файлы.
6. Щёлкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

Восстановление системных баз данных

Все системные базы данных экземпляра восстанавливаются одновременно. При восстановлении системных баз программа автоматически перезапускает целевой экземпляр в однопользовательском режиме. После завершения восстановления программа перезапускает экземпляр и восстанавливает другие базы данных (если есть).

При восстановлении системной базы данных также обращайте внимание на перечисленные ниже моменты.

- Системные базы данных можно восстановить только на экземпляре той же версии, что и исходный.
- Системные базы данных всегда восстанавливаются в состоянии ”готово к использованию”.

Восстановление базы данных master

В число системных баз данных входит база master. В базе данных master содержатся сведения обо всех базах данных экземпляра. Это означает, что база данных master в резервной копии содержит информацию о базах данных, существовавших в экземпляре на момент резервного копирования. После восстановления базы данных master может потребоваться следующее.

- Базы данных, которые появились в экземпляре после выполнения резервного копирования, становятся невидимыми для экземпляра. Чтобы снова перевести их в режим эксплуатации, прикрепите их к экземпляру вручную с помощью SQL Server Management Studio.
- Базы данных, которые были удалены после выполнения резервного копирования, отображаются в экземпляре как находящиеся в автономном режиме. Удалите эти базы данных с помощью SQL Server Management Studio.

Подключение баз данных Microsoft SQL Server

В этом разделе описывается процедура подключения базы данных в Microsoft SQL Server с помощью среды SQL Server Management Studio. Одновременно может быть подключена только одна база данных.

Для подключения базы данных необходимо иметь любое из следующих разрешений: **CREATE DATABASE** (Создание базы данных), **CREATE ANY DATABASE** (Создание любой базы данных) или **ALTER ANY DATABASE** (Изменение любой базы данных). Обычно эти разрешения предоставляются роли **sysadmin** экземпляра.

Как подключить базу данных

1. Запустите среду SQL Server Management Studio.
2. Подключитесь к требуемому экземпляру Microsoft SQL Server и разверните его.
3. Правой кнопкой мыши щёлкните пункт **Базы данных** и щёлкните **Подключить**.
4. Нажмите кнопку **Добавить**.
5. В диалоговом окне **Поиск файлов баз данных** найдите и выберите MDF-файл базы данных.
6. В разделе **Сведения о базе данных** убедитесь, что остальные файлы базы данных (NDB-файлы и LDF-файлы) также найдены.

   Файлы базы данных Microsoft SQL Server могут быть не найдены автоматически, если:

   - Они находятся в расположении, отличном от расположения по умолчанию, или они не находятся в одной папке с основным файлом базы данных (MDF). Решение: Укажите путь к требуемым файлам вручную в столбце **Путь к текущему файлу**.
   - Вы восстановили неполный набор файлов, составляющих базу данных. Решение: Восстановите отсутствующие файлы базы данных Microsoft SQL Server из резервной копии.
7. Когда все файлы будут найдены, нажмите кнопку **ОК**.

Восстановление баз данных Microsoft Exchange Server

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить данные Exchange в работающий Exchange. Это может быть исходный Exchange или Exchange той же версии, выполняющийся на машине с таким же полным доменным именем (FQDN). Агент для Exchange должен быть установлен на целевой машине.

В таблице ниже приведены основные сведения о том, какие именно данные Exchange можно выбрать для восстановления, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2010/2013/2016/2019	Базы данных	Участие в группе ролей **Управление сервером**.

Базы данных также можно восстанавливать в виде файлов. Файлы баз данных и журналы транзакций извлекаются из резервной копии в указанную папку. Это может оказаться полезно, если необходимо извлечь данные для аудита или дальнейшей обработки средствами сторонних производителей либо в случае, когда выполнить восстановление по какой-либо причине не удается и требуется обходное решение для *подключения баз данных вручную*.

Если используется только агент для VMware (Windows), то единственный доступный метод восстановления — восстановить базы данных как файлы. Невозможно восстановить базы данных с помощью агента для VMware (виртуальное устройство).

Для восстановления баз данных Exchange на запущенный сервер Exchange

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** → **Microsoft Exchange** → **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления данных Exchange.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** → **Базы данных Exchange**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить**.
   - При восстановлении из резервной копии базы данных выберите **Восстановить** → **Базы данных на сервер Exchange**.
5. По умолчанию данные восстанавливаются в исходных базах. Если исходная база данных не существует, она будет создана.

   Восстановление данных в другой базе:

1. Щёлкните имя базы данных.
2. В поле **Восстановить в** выберите вариант **Новая база данных**.
3. Укажите имя новой базы данных.
4. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов.

6. Щёлкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

Восстановление баз данных Exchange в виде файлов

1. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** → **Microsoft Exchange** → **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. Выполните одно из следующих действий:
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.

   Машина, выбранная для обзора любым из двух вышеописанных действий, становится целевой машиной для восстановления данных Exchange.
4. Выполните одно из следующих действий:
   - При восстановлении из резервной копии с поддержкой приложений нажмите **Восстановить** → **Базы данных Exchange**, выберите базу данных, которую нужно восстановить, и затем нажмите **Восстановить как файлы**.

- При восстановлении из резервной копии базы данных выберите **Восстановить** → **Базы данных как файлы**.

5. Нажмите **Обзор** и затем выберите локальную или сетевую папку, в которую требуется сохранить файлы.
6. Щёлкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке **Действия**.

Подключение баз данных Microsoft Exchange Server

После восстановления файлов базы данных можно включить базы данных, подключив их. Подключение выполняется с использованием консоли управления Exchange, диспетчера Exchange или командной консоли Exchange.

Восстановленные базы данных будут в состоянии ”Неправильное отключение”. База данных в состоянии ”Неправильное отключение” может быть подключена системой, если она восстанавливается в исходное хранилище (то есть, информация об исходной базе данных присутствует в Active Directory). Если база данных восстанавливается в другое расположение (в новую базу данных или базу данных восстановления), она не может быть подключена, пока не будет приведена в состояние ”чистого отключения” с помощью команды `Eseutil /r <Enn>`. `<Enn>` указывает префикс файлов журнала для базы данных (или группы хранения, содержащей эту базу данных), где необходимо применить файлы журнала транзакций.

Учетной записи, которая используется для подключения базы данных, необходимо делегировать роль администратора сервера Exchange и локальную группу администраторов для данного целевого сервера.

Подробную информацию о том, как подключить базы данных, см. в статье <http://technet.microsoft.com/en-us/library/aa998871.aspx.

Восстановление почтовых ящиков Exchange и элементов почтового ящика

В этом разделе описана процедура восстановления почтовых ящиков Exchange и элементов почтового ящика из резервных копий базы данных, резервных копий с поддержкой приложений и из резервных копий почтового ящика. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server.

Можно восстановить следующие элементы:

- почтовые ящики, в том числе архивные;
- общие папки;

- элементы общих папок;
- папки электронной почты;
- сообщения электронной почты;
- события календаря;
- задания;
- контакты;
- записи журнала;
- заметки.

Чтобы найти эти элементы, можно воспользоваться поиском.

Восстановление на Exchange Server

Фрагментарное восстановление можно выполнить в Microsoft Exchange Server 2013 и более поздних версиях. Исходная резервная копия может содержать базы данных или почтовые ящики любой поддерживаемой версии Exchange.

Фрагментарное восстановление может быть выполнено агентом для Exchange или агентом для VMware (Windows). Целевой Exchange Server и машина с выполняющимся агентом должны быть в одном лесу Active Directory.

Если почтовый ящик восстанавливается в существующий почтовый ящик, существующие элементы с одинаковыми идентификаторами перезаписываются.

При восстановлении элементов почтового ящика перезапись не происходит. Вместо этого в целевой папке заново создается полный путь к элементу почтового ящика.

Требования к учетным записям пользователей

Почтовый ящик, восстанавливаемый из резервной копии, должен иметь связанную с ним учетную запись пользователя в Active Directory.

Пользовательские почтовые ящики и их содержимое можно восстановить, только если *включены* связанные с ними учетные записи пользователей. Общие почтовые ящики, почтовые ящики помещения и оборудования могут быть восстановлены, только если соответствующие учетные записи пользователей *отключены*.

Почтовый ящик, не соответствующий этим условиям, при восстановлении будет пропущен.

Если некоторые почтовые ящики будут пропущены, восстановление продолжится с предупреждением. Если все почтовые ящики будут пропущены, восстановление завершится сбоем.

Восстановление почтовых ящиков

Порядок восстановления почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. Выполните одно из следующих действий:

   - При восстановлении из резервной копии с поддержкой приложений: в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** → **Microsoft Exchange** → **Базы данных** и затем выберите базу данных, в которой изначально располагались данные, которые необходимо восстановить.

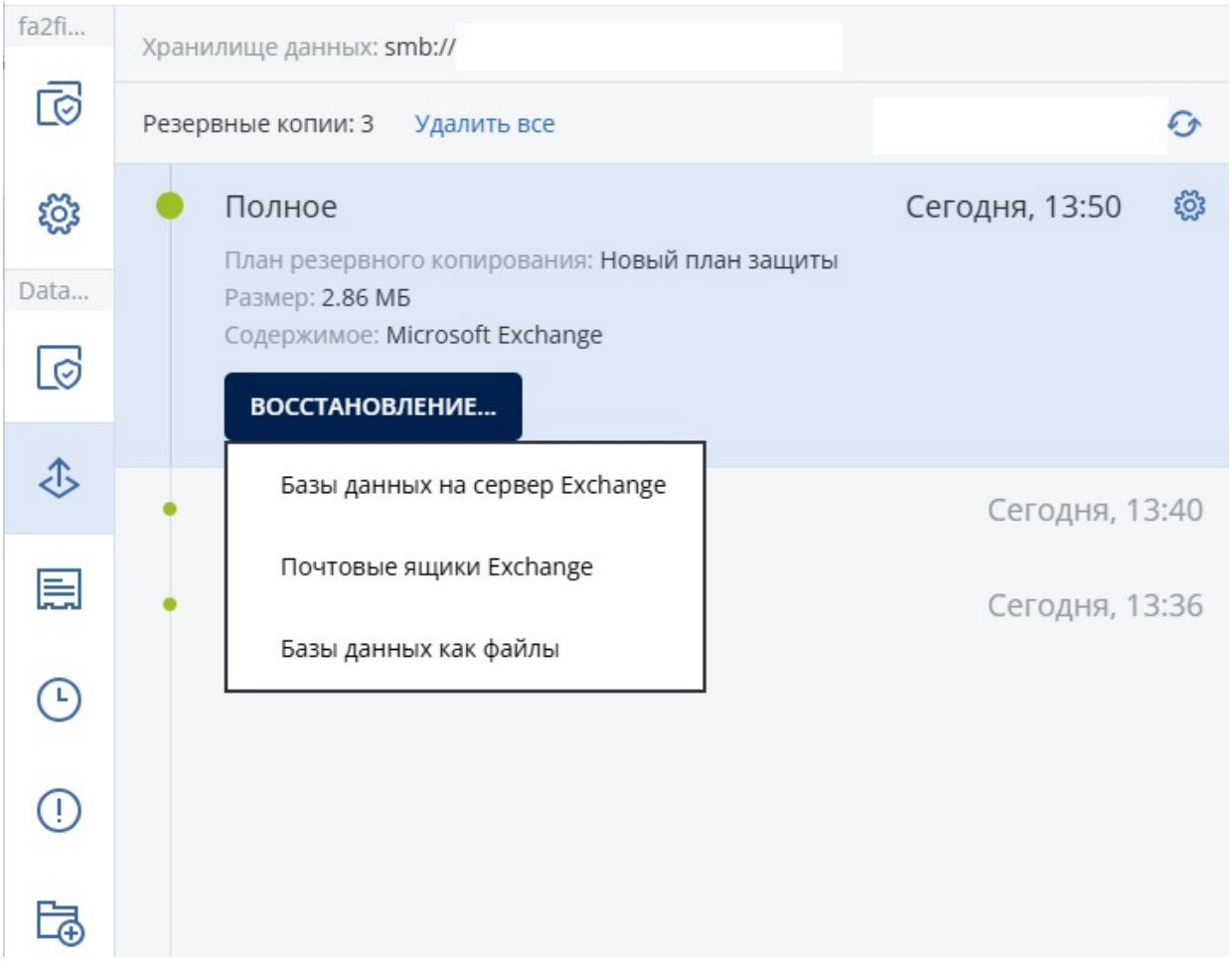
2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.

   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.

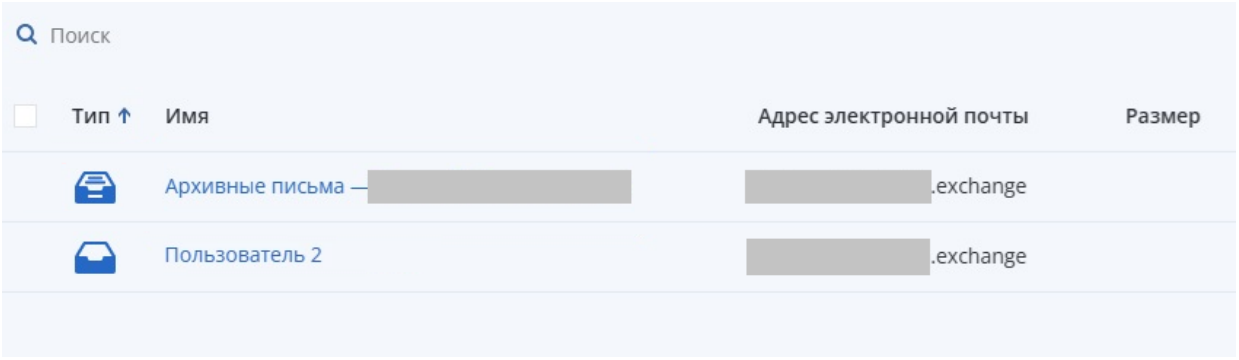
   Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбрана для просмотра одним из двух указанных выше действий.

4. Щёлкните **Восстановление** → **Почтовые ящики Exchange**.



5. Выберите почтовые ящики, которые необходимо восстановить. Архивные почтовые ящики имеют специальную иконку и имя, состоящее из названия архива писем и псевдонима пользователя.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.



6. Нажмите кнопку **Восстановить**.

7. Чтобы выбрать или изменить целевую машину, щёлкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

   Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в

Microsoft Exchange Server 2013) или **Роль почтовых ящиков** (в Microsoft Exchange Server 2016 или более поздних версиях). Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

При поступлении соответствующего запроса укажите данные учетной записи, которая будет использоваться для доступа к машине. Требования к этой учетной записи указаны в разделе *Требуемые права пользователя*.

8. При восстановлении архивных почтовых ящиков щёлкните **База данных для воссоздания отсутствующих почтовых ящиков** и укажите активную базу данных.
9. Нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

Порядок восстановления почтового ящика из резервной копии почтового ящика

1. Нажмите **Устройства** → **Microsoft Exchange** → **Почтовые ящики**.
2. Выберите почтовый ящик для восстановления и щёлкните **Восстановить**.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.

   Если почтовый ящик был удален, выберите его на вкладке *Хранилища резервных копий* и щёлкните **Показать резервные копии**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** → **Почтовый ящик**.
5. Выполняйте шаги 7-9 вышеописанной процедуры.

Восстановление элементов почтовых ящиков

Порядок восстановления элементов почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных

1. Выполните одно из следующих действий:

   - При восстановлении из резервной копии с поддержкой приложений: в пункте **Устройства** выберите машину, на которой изначально располагались данные, которые необходимо восстановить.
   - При восстановлении из резервной копии базы данных нажмите **Устройства** → **Microsoft**

Exchange → **Базы данных** и затем выберите базу данных, в которой изначально располагались данные, которые необходимо восстановить.

2. Щёлкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.

   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в общем хранилище (т. е., другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.

   Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.
4. Щёлкните **Восстановление** → **Почтовые ящики Exchange**.
5. Щёлкните почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить.
6. Выберите элементы, которые необходимо восстановить.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

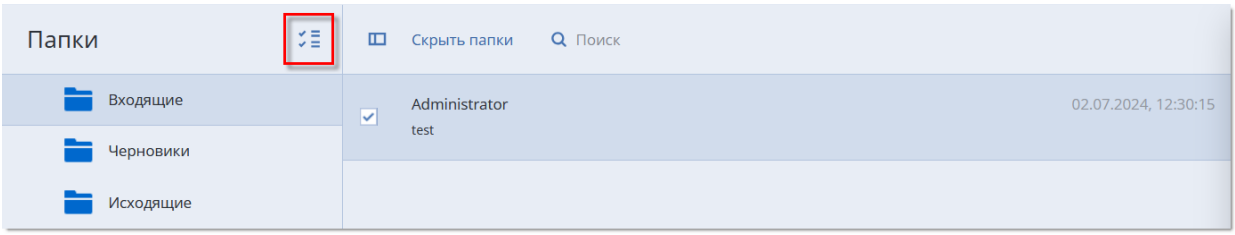
   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю и дате.
   - Для событий: выполните поиск по заголовку и дате.
   - Для задач: выполните поиск по теме и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.

   Когда выбрано это сообщение электронной почты, можно щёлкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

   Примечание

   Чтобы загрузить вложенный файл, щёлкните его имя.

   Чтобы иметь возможность выбрать папки, щёлкните значок восстановления папок.



7. Нажмите кнопку **Восстановить**.
8. Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.
9. Чтобы выбрать или изменить целевую машину, щёлкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

   Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2013) или **Роль почтовых ящиков** (в Microsoft Exchange Server 2016 или более поздних версиях). Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

   При поступлении соответствующего запроса укажите данные учетной записи, которая будет использоваться для доступа к машине. Требования к этой учетной записи указаны в разделе *Требуемые права пользователя*.
10. Раздел **Целевой почтовый ящик** позволяет просмотреть, изменить или указать целевой почтовый ящик.

    По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана целевая машина, которая не является исходной, необходимо указать целевой почтовый ящик.

    При восстановлении архивного почтового ящика укажите действующий почтовый ящик, в который будут восстановлены данные.
11. [Только при восстановлении сообщений электронной почты] В поле **Целевая папка** просмотрите или измените целевую папку в целевом почтовом ящике. По умолчанию выбрана папка **Восстановленные элементы**. Из-за ограничений Microsoft Exchange события, задачи, примечания и контакты восстанавливаются в их оригинальное расположение независимо от папки, заданной параметром **Целевая папка**.
12. Нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

Порядок восстановления элемента почтового ящика из резервной копии почтового ящика

1. Нажмите **Устройства** → **Microsoft Exchange** → **Почтовые ящики**.
2. Выберите почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить, и нажмите кнопку **Восстановить**.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.

   Если почтовый ящик был удален, выберите его на вкладке *Хранилища резервных копий* и щёлкните **Показать резервные копии**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** → **Сообщения электронной почты**.
5. Выберите элементы, которые необходимо восстановить.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю и дате.
   - Для событий: выполните поиск по заголовку и дате.
   - Для задач: выполните поиск по теме и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.

   Если выбрано сообщение электронной почты, можно щёлкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

   > **Примечание**
   >
   > Чтобы загрузить вложенный файл, щёлкните его имя.

   Если выбрано сообщение электронной почты, можно щёлкнуть **Отправить как сообщение электронной почты**, чтобы отправить сообщение по адресу электронной почты. Сообщение отправляется с адреса электронной почты администратора учетной записи.

   Чтобы иметь возможность выбрать папки, щёлкните значок восстановления папок .
6. Нажмите кнопку **Восстановить**.

7. Выполните шаги 8–12 вышеописанной процедуры.

Копирование библиотек Microsoft Exchange Server

Скопируйте указанные ниже файлы в соответствии с версией Microsoft Exchange Server, для которой создана резервная копия.

Версия Microsoft Exchange Server	Ленточные библиотеки	Хранилище по умолчанию
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Библиотеки необходимо поместить в папку `%ProgramData%\Acronis\ese`. Если папка не существует, создайте ее вручную.

Изменение учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server

Можно изменить учетные данные для доступа к Microsoft SQL Server или Microsoft Exchange Server без переустановки агента.

Изменение учетных данных для доступа к Microsoft SQL Server или Microsoft Exchange Server:

1. Щёлкните **Устройства**, а затем щёлкните **Microsoft SQL** или **Microsoft Exchange**.
2. Выберите группу обеспечения доступности Always On, группу обеспечения доступности баз данных, экземпляр Microsoft SQL Server или Microsoft Exchange Server, для которых необходимо изменить учетные данные.
3. Щёлкните **Укажите учетные данные**
4. Укажите новые учетные данные для доступа, а затем щёлкните **ОК**.

Изменение учетных данных Microsoft Exchange Server для доступа к резервной копии почтового ящика:

1. Щёлкните **Устройства** → **Microsoft Exchange** и разверните узел **Почтовые ящики**.
2. Выберите Microsoft Exchange Server, для которого необходимо изменить учетные данные для доступа.
3. Щёлкните **Настройки**.
4. Ниже поля **Учетная запись администратора Exchange** укажите новые учетные данные для доступа, а

затем щёлкните **Сохранить**.

Защита CommuniGate Pro

С помощью Кибер Бэкап можно выполнять резервное копирование данных CommuniGate Pro. При использовании Кибер Бэкап и CommuniGate Pro регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователя. Удаленные элементы можно восстановить из резервной копии.

Условия для резервного копирования CommuniGate Pro

Для резервного копирования данных CommuniGate Pro понадобятся установленные и настроенные продукты:

- Кибер Бэкап 15 обновление 2.7 или новее с лицензией Кибер Бэкап для почтового ящика. Информацию о лицензиях см. в разделе *Издания и лицензии Кибер Бэкап*.
- CommuniGate Pro.

  Поддерживаемые версии CommuniGate Pro указаны в разделе *Поддерживаемые почтовые сервисы*.

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агентов для следующих операционных систем:

- Windows,
- Linux.

Полный список поддерживаемых операционных систем Windows и Linux см. в разделе *Поддерживаемые операционные системы*.

Возможности

Резервное копирование

- Автоматическая и ручная синхронизация ресурсов.
- Резервное копирование данных и настроек.
- Резервное копирование по расписанию.
- Поддержка многоуровневого резервного копирования.
- Перезапись данных хранилища по выбору.
- Настраиваемые правила очистки хранилища.

- Поддержка кластерных конфигураций.

Восстановление

- Гранулярное восстановление, или восстановление следующих элементов:
  - серверы (в случае файлового или дискового резервного копирования);
  - почтовые ящики (включая папки, права на них, письма и вложения);
  - письма;
  - контакты;
  - календари;
  - заметки;
  - задачи;
  - настройки учетной записи.
- Восстановление в исходное и новое месторасположение (сервер, домен, пользователь).
- Поиск элементов в резервной копии.

Известные проблемы и ограничения

- Восстановление на новый хост возможно в случае, если на нем заранее создан домен с исходным именем. Восстановление в домен с новым именем невозможно.
- Не поддерживается сохранение резервных копий на подключенное к узлу хранения ленточное устройство.
- Резервное копирование и восстановление настроек пользователя ограничено резервным копированием и восстановлением его системных настроек.

Предварительные требования для защиты CommuniGate Pro

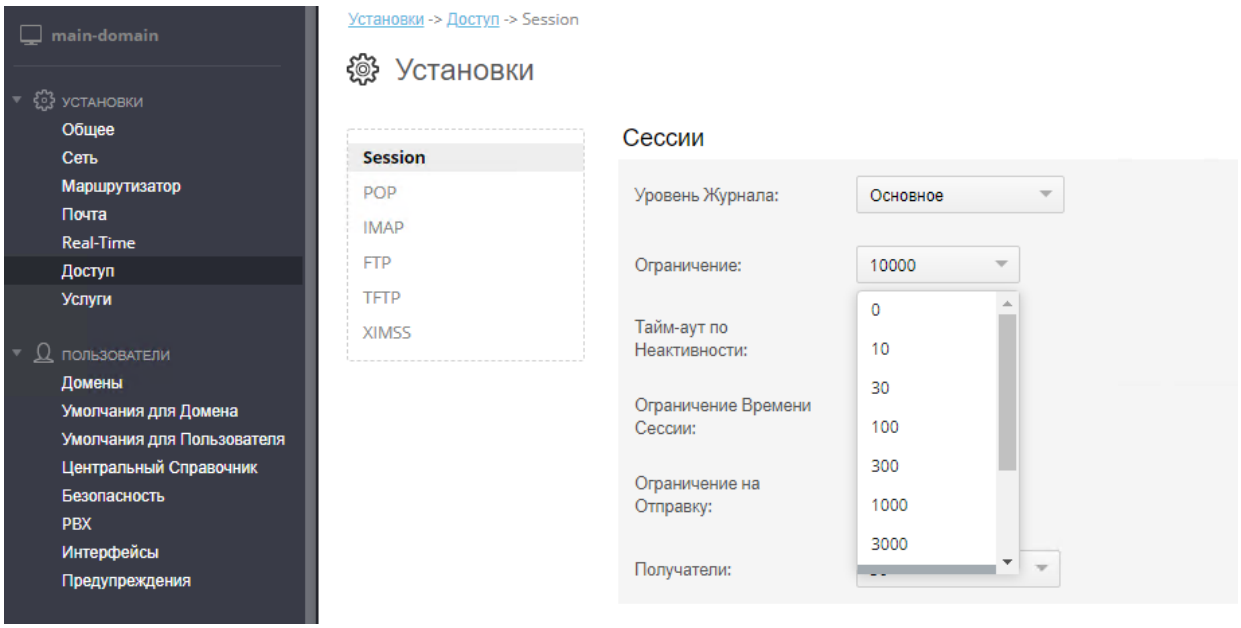
Перед началом использования защиты CommuniGate Pro потребуется выполнить некоторые действия.

Выключение ограничений на количество сессий

Необходимо выключить ограничения на количество сессий в сервере CommuniGate, иначе резервное копирование может завершаться с ошибкой. Для выключения ограничений выполните следующие действия:

1. Откройте CommuniGate Pro.

2. Перейдите в **Установки** → **Доступ**.
3. В подразделе **Сессии** в поле **Ограничение** установите значение, равное 10000.

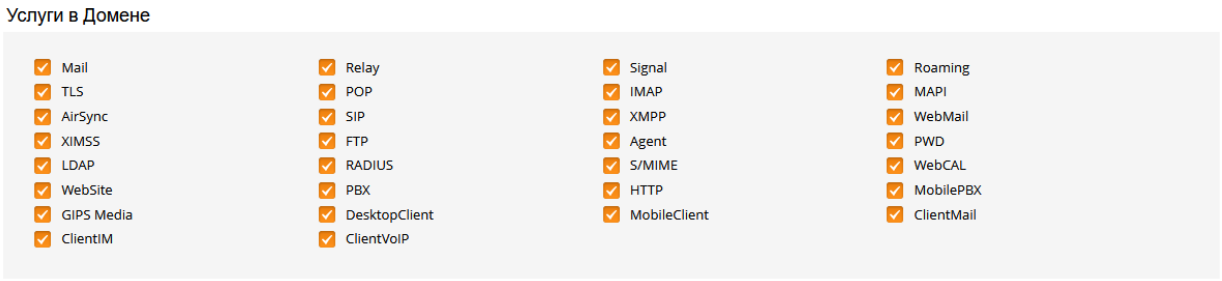


4. Нажмите **Модифицировать**, чтобы сохранить изменения.

Инициализация соединения вручную

Для инициализации соединения Кибер Бэкап с CommuniGate Pro (например, если интерфейс командной строки недоступен) может потребоваться выполнить следующие действия:

1. Откройте CommuniGate Pro.
2. Перейдите в **Пользователи** → **Умолчания для Домена** и убедитесь, что услуга PWD включена.



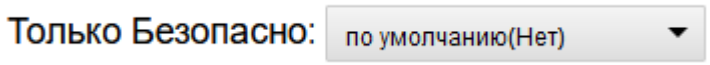
3. Перейдите в **Пользователи** → **Домены** → **<Имя_домена>** → **Установки Домена** и убедитесь, что в настройках домена включена услуга PWD.



4. Перейдите в **Умолчания для пользователя** → **Установки** и убедитесь, что в настройках пользователя включена услуга PWD.



5. Перейдите в **Умолчания для пользователя** → **Установки** и выберите **Нет** в параметре **Только безопасно**.



6. Для сохранения изменений нажмите **Модифицировать**.
7. Щёлкните **Пользователи** и выберите из списка пользователя (домен), который используется для подключения к Кибер Бэкап.
8. Убедитесь, что в настройках пользователя (домена), используемого для подключения к Кибер Бэкап, включены все параметры PWD.

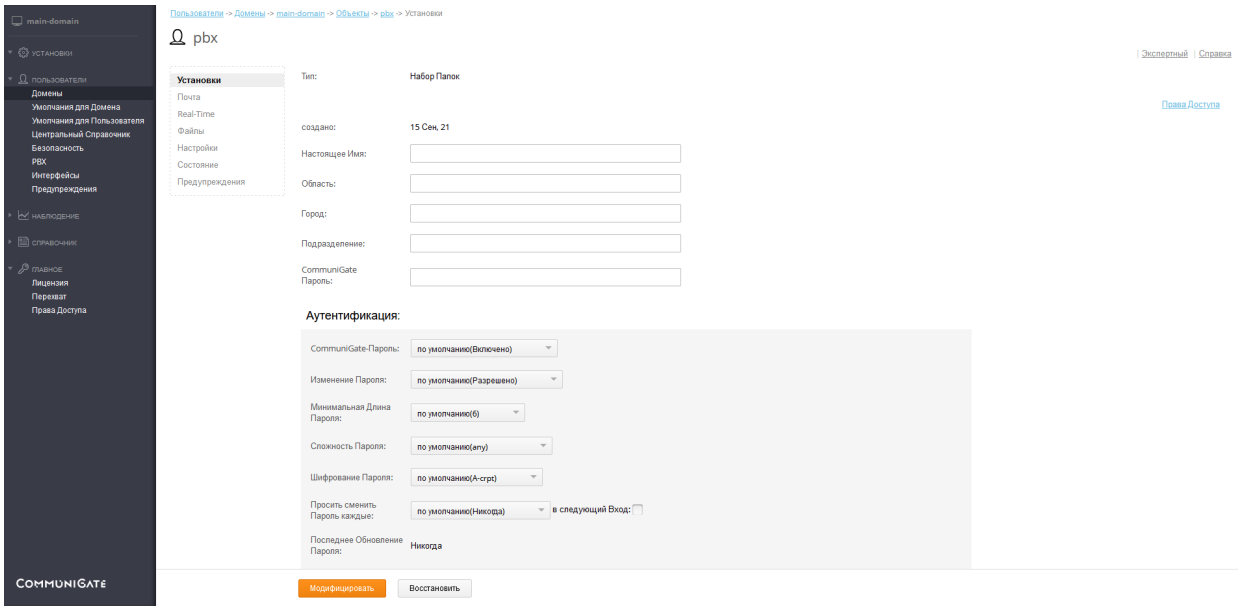
Установка прав пользователя

Для того, чтобы выполнять резервное копирование и восстановление из резервных копий в CommuniGate Pro, пользователь, от имени которого они выполняются, должен обладать следующими свойствами:

- Пользователь должен принадлежать главному домену.
- Права пользователя должны позволять ему менять установки сервера, а также всех доменов и пользователей.

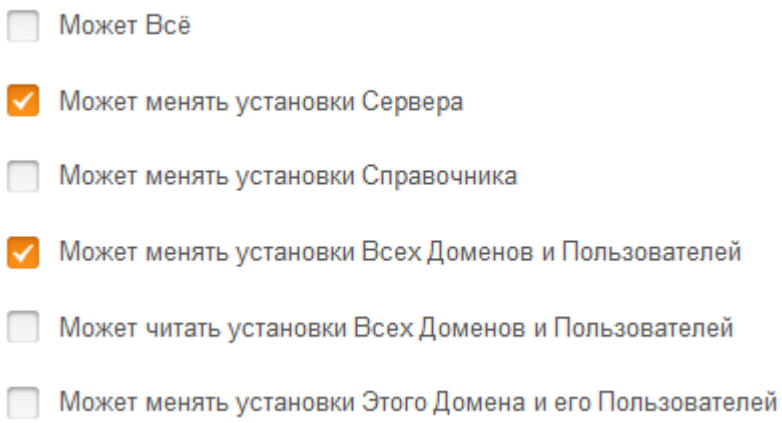
Чтобы установить права пользователя:

1. Откройте CommuniGate Pro.
2. Перейдите в **Пользователи → Домены → Имя главного домена**.
3. Щёлкните по имени пользователя в списке объектов.
4. На странице настроек пользователя нажмите справа вверху **Права доступа**.



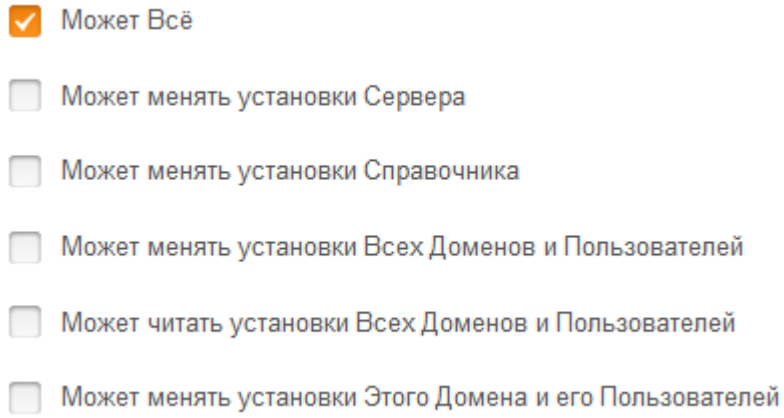
5. Установите права пользователя следующим образом:

   Может менять установки Сервера и **Может менять установки всех Доменов и Пользователей**



   или

   Может Всё



6. Для сохранения изменений нажмите **Модифицировать**.

Разрешение подключения агента к серверу CommuniGate Pro

Для успешной работы агент должен иметь возможность подключаться к серверу CommuniGate Pro через TCP-порты 106 и 993 (по умолчанию):

1. Через порт 106 по протоколу PWD происходит базовое подключение для регистрации и определения параметров сервера.
2. Через порт 993 по протоколу IMAP происходит резервное копирование и восстановлении данных.

В настройках сетевого экрана сервера CommuniGate Pro откройте эти порты и разрешите подключение от агента через них.

Устранение неполадок при подключении

При возникновении проблем с регистрацией или резервным копированием CommuniGate Pro выполните следующие проверки:

1. Проверка сетевой доступности.

   На машине с агентом CommuniGate Pro выполните следующие команды:

   ```
   ping mx.company.local
   telnet mx.company.local 106
   telnet mx.company.local 993
   ```

   где `mx.company.local` — имя или IP-адрес сервера CommuniGate Pro.

2. Проверка прав доступа.

   Подключитесь к CommuniGate Pro в режиме командной строки:

```
telnet mx.company.local 106
```

Выполните команды:

```
user postmaster
pass password
LISTDOMAINS
```

где:

- `postmaster` — имя учетной записи администратора, которую использует агент для подключения к CommuniGate Pro;
- `password` — пароль учетной записи администратора.

Ответ на каждую команду должен сопровождаться кодом 200.

Пример:

```
% telnet ys-cgp-fe1 106
Trying 10.10.100.10...
Connected to ys-cgp-fe1.
Escape character is '^]'.
200 fe1.domain.name CommuniGate Pro PWD Server 6.3.33 ready <18.1712221326@main-domain>
user postmaster
300 please send the PASS
pass password
200 login OK, proceed
LISTDOMAINS
200 data follow
(
fe1.domain.name,
fe2,
host-domain,
qwe.domain.name,
test1.domain.name,
test2.domain.name
)
```

Установка CommuniGate Pro

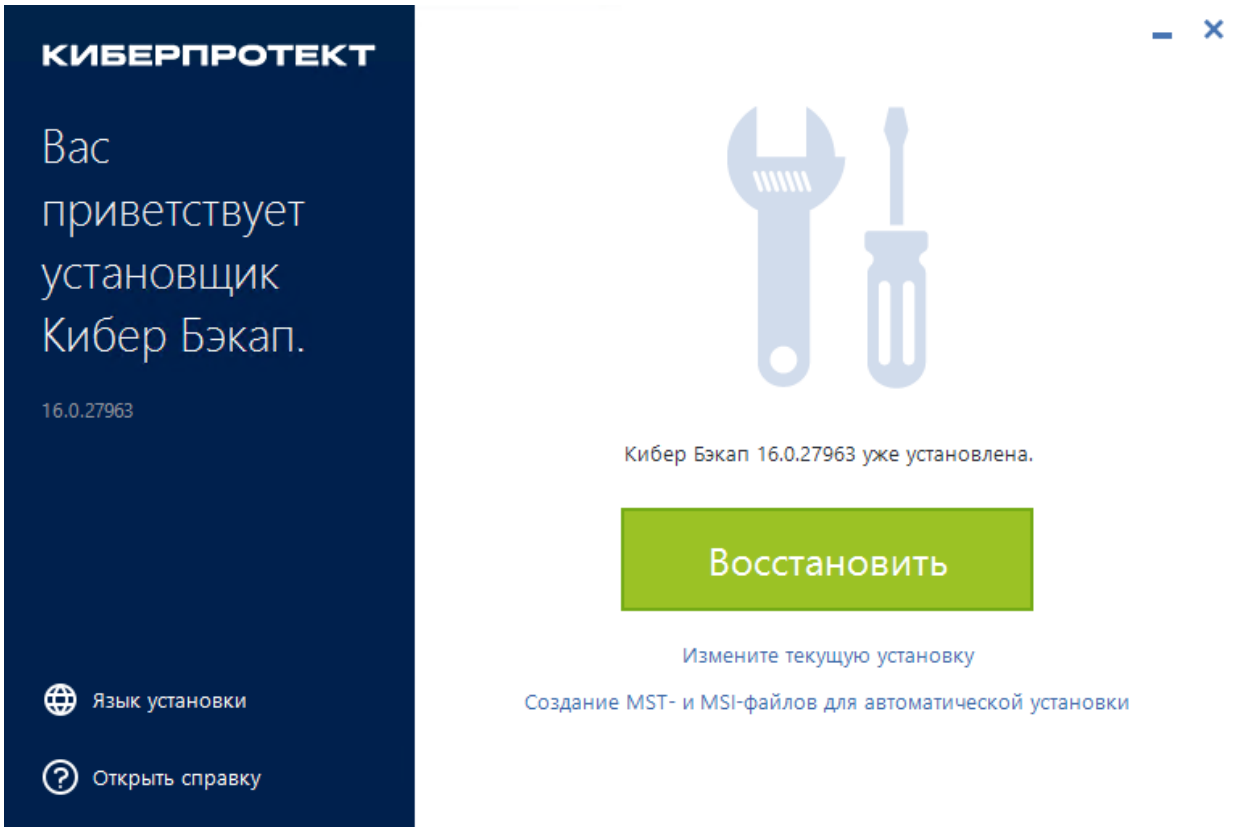
Установка CommuniGate Pro включает в себя установку агента Кибер Бэкап и добавление хоста CommuniGate Pro. Добавление хоста возможно лишь после установки агента.

Агент может быть установлен на машину с почтовым сервером или на отдельно стоящую машину.

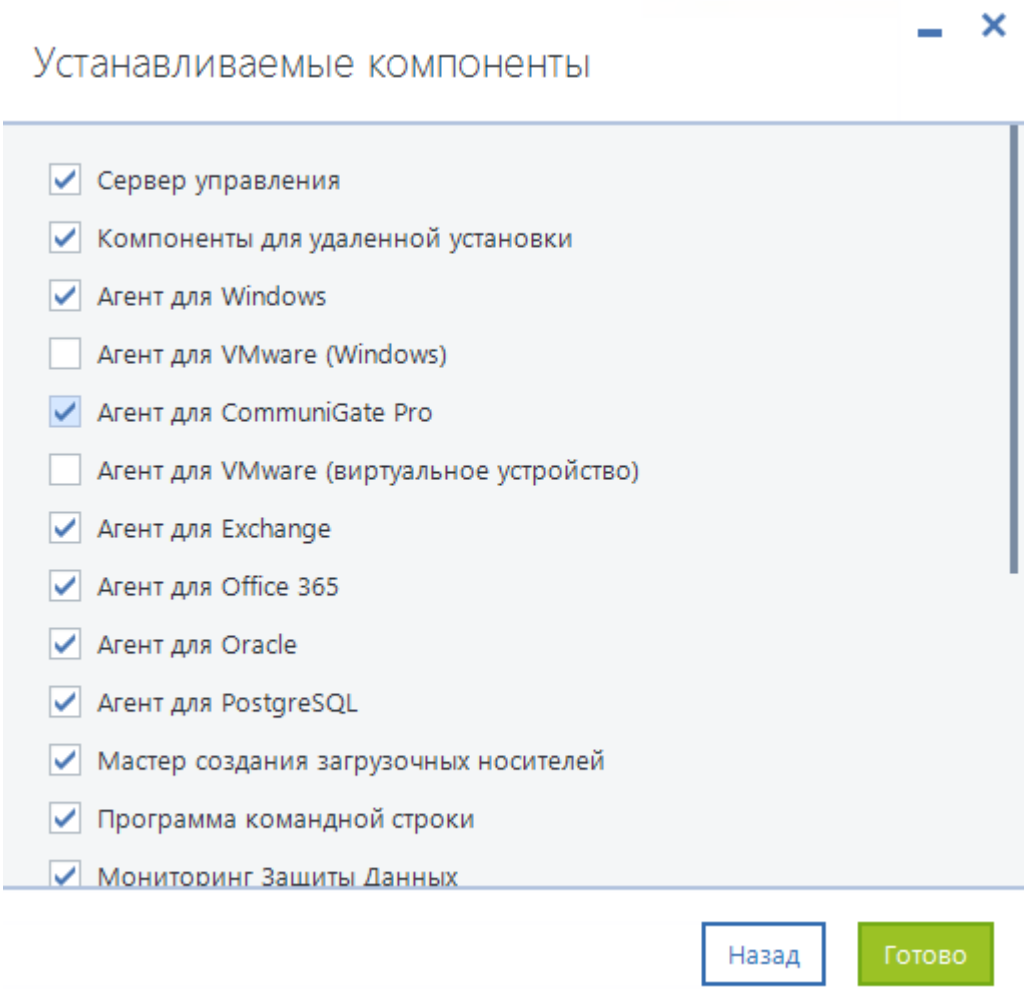
Для каждого хоста должен быть установлен отдельный агент.

Установка агента для CommuniGate Pro

1. Запустите установщик Кибер Бэкап.
2. Выберите **Измените текущую установку**



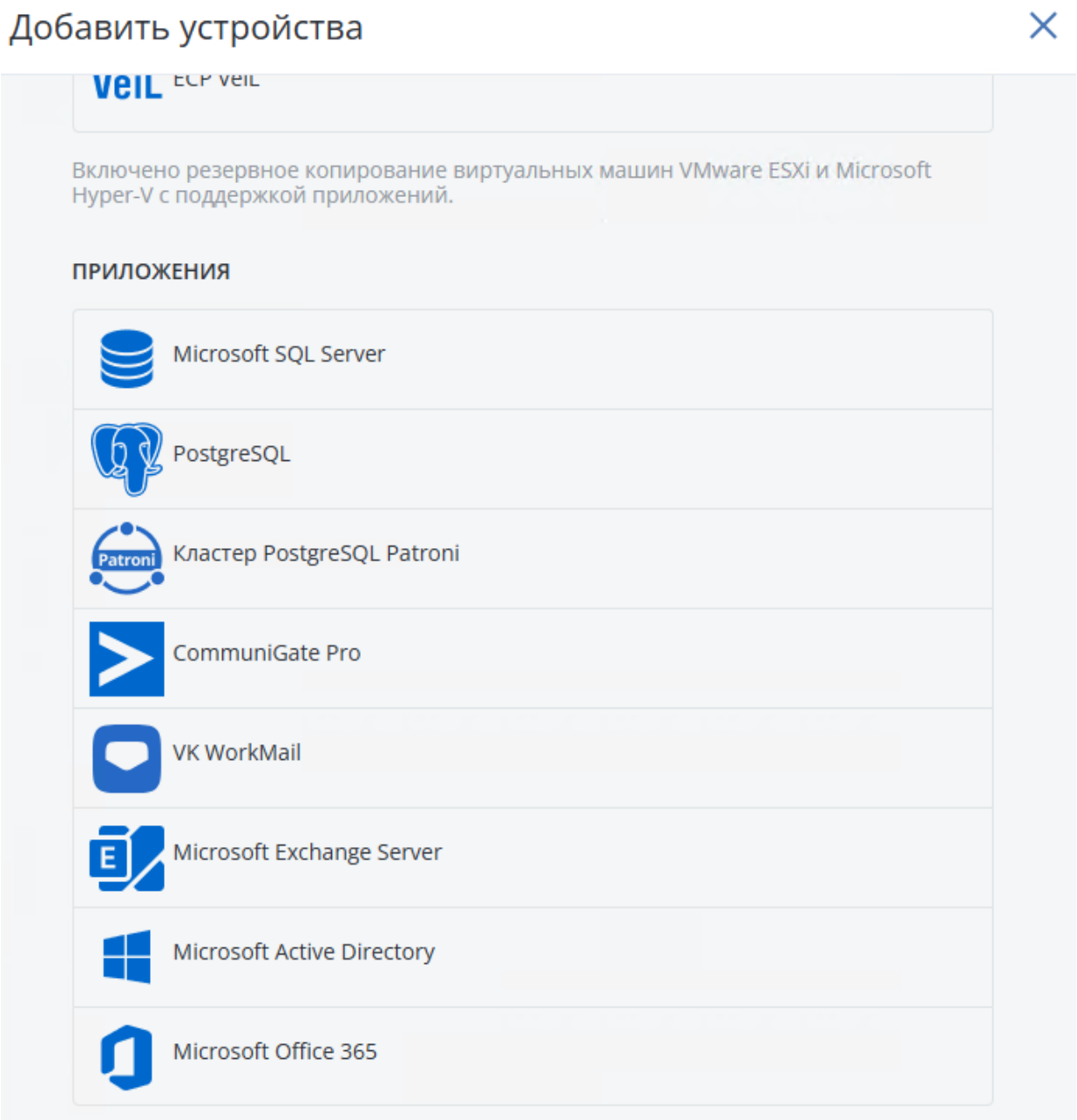
3. Отметьте в списке **Агент для CommuniGate Pro**.



4. Щёлкните **Готово**.

Добавление хоста CommuniGate Pro

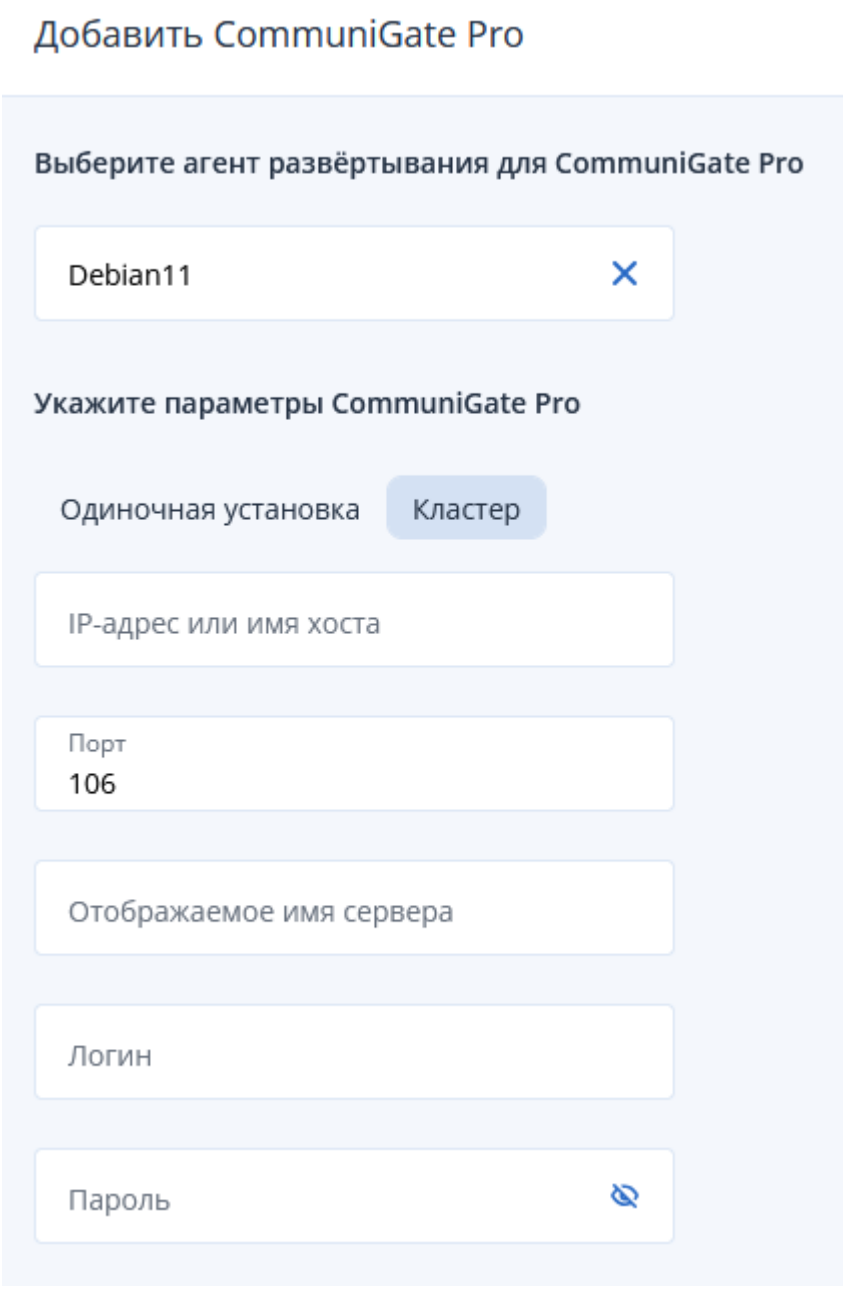
1. В веб-консоли перейдите на вкладку **Устройства** в главном меню слева и нажмите в правом верхнем углу **Добавить**.
2. В окне добавления нового устройства в подразделе **Приложения** щёлкните **CommuniGate Pro**.



3. Заполните поля:

   - в поле подраздела **Выберите агент развертывания для CommuniGate Pro** укажите имя компьютера, на котором установлен агент CommuniGate Pro;
   - в полях подраздела **Укажите параметры CommuniGate Pro** укажите параметры сервера CommuniGate Pro:
     - выберите **Одиночная установка** в случае одиночного сервера или **Кластер** в случае *серверного кластера*;
     - в поле **IP-адрес или имя хоста** укажите IP-адрес или имя регистрируемого сервера;

- в поле **Отображаемое имя сервера** укажите имя, под которым сервер будет отображаться в системе;
- в полях **Логин** и **Пароль** укажите имя и пароль пользователя сервера CommuniGate Pro.



4. По окончании ввода данных нажмите **Добавить**.
5. Убедитесь, что новое устройство отображается в разделе **Устройства** веб-консоли.

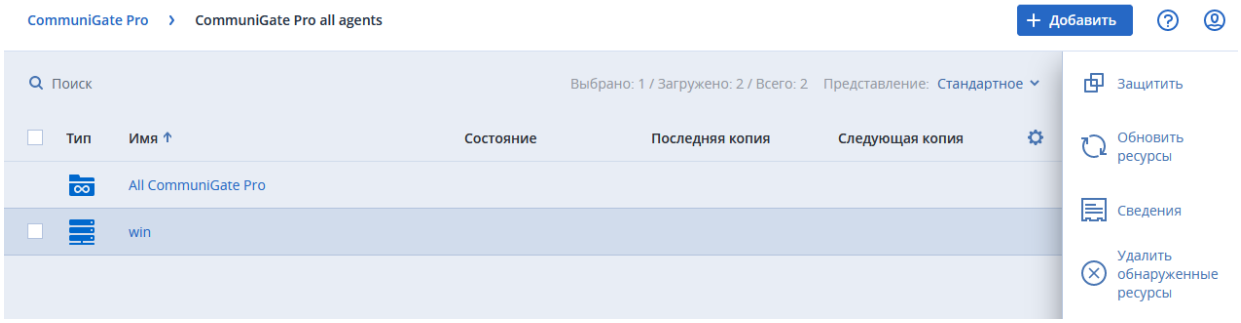
Резервное копирование CommuniGate Pro

Резервное копирование данных CommuniGate Pro позволяет защитить домены и отдельные почтовые ящики. Для защиты данных необходимо сначала создать план защиты.

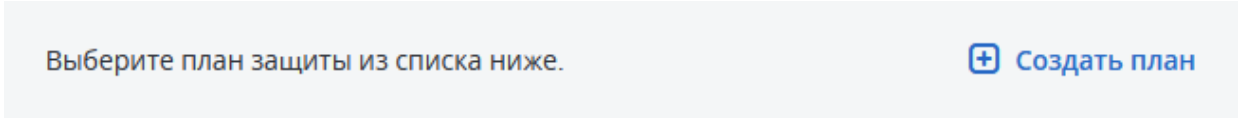
Создание плана защиты для CommuniGate Pro

Для создания плана защиты выполните следующие действия:

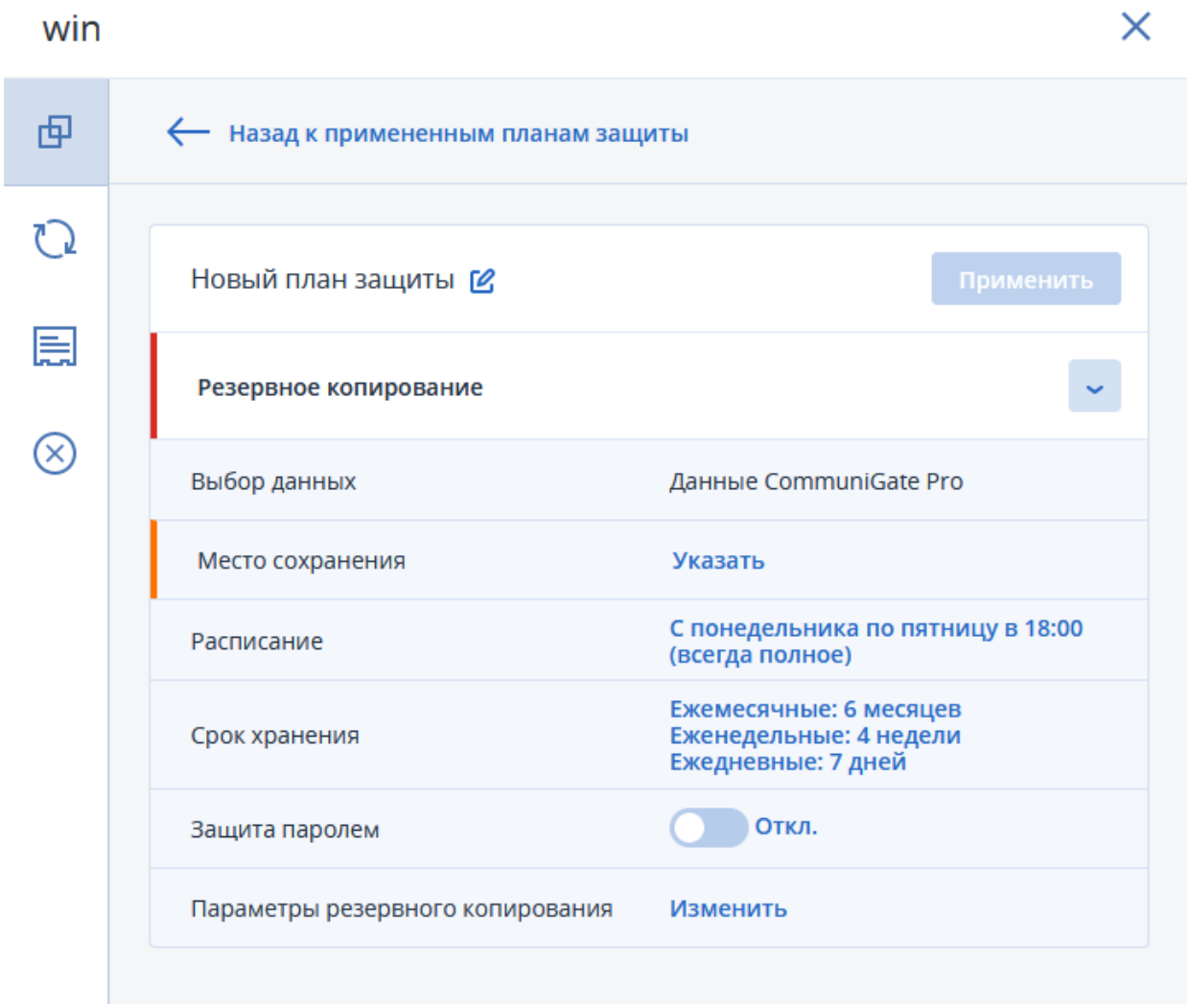
1. Перейдите в **Устройства**.
2. Выберите из списка устройство, которое вы хотите защитить, и щёлкните по строке, в которой находится это устройство.
3. Перейдите на вкладку справа **Защитить**.



4. Нажмите **Создать план**.

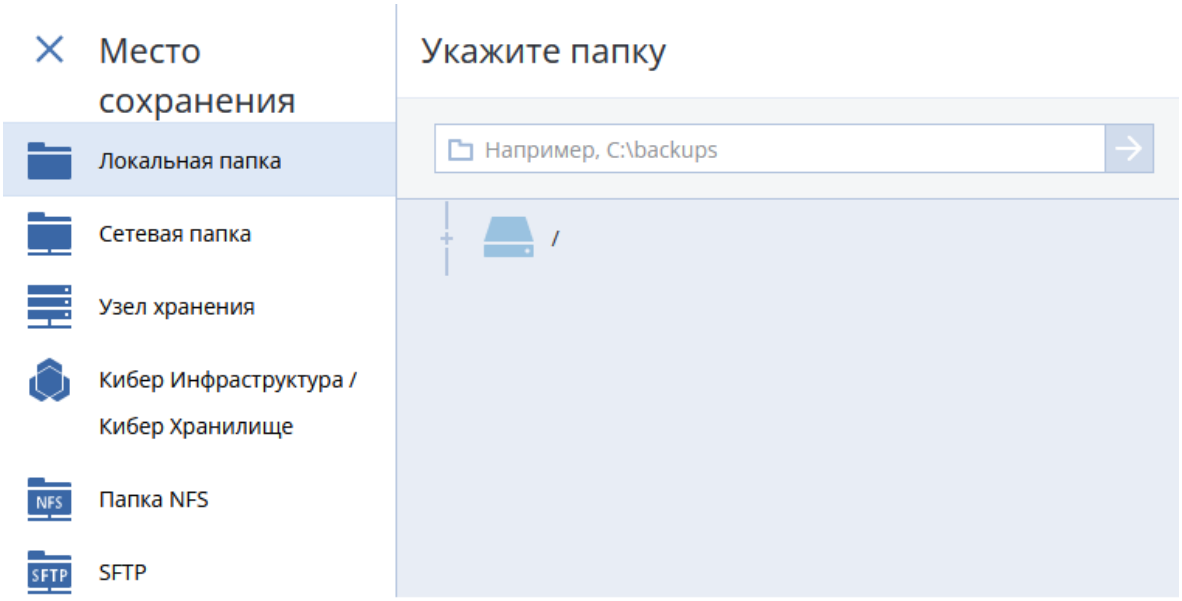


Откроется окно создания плана.



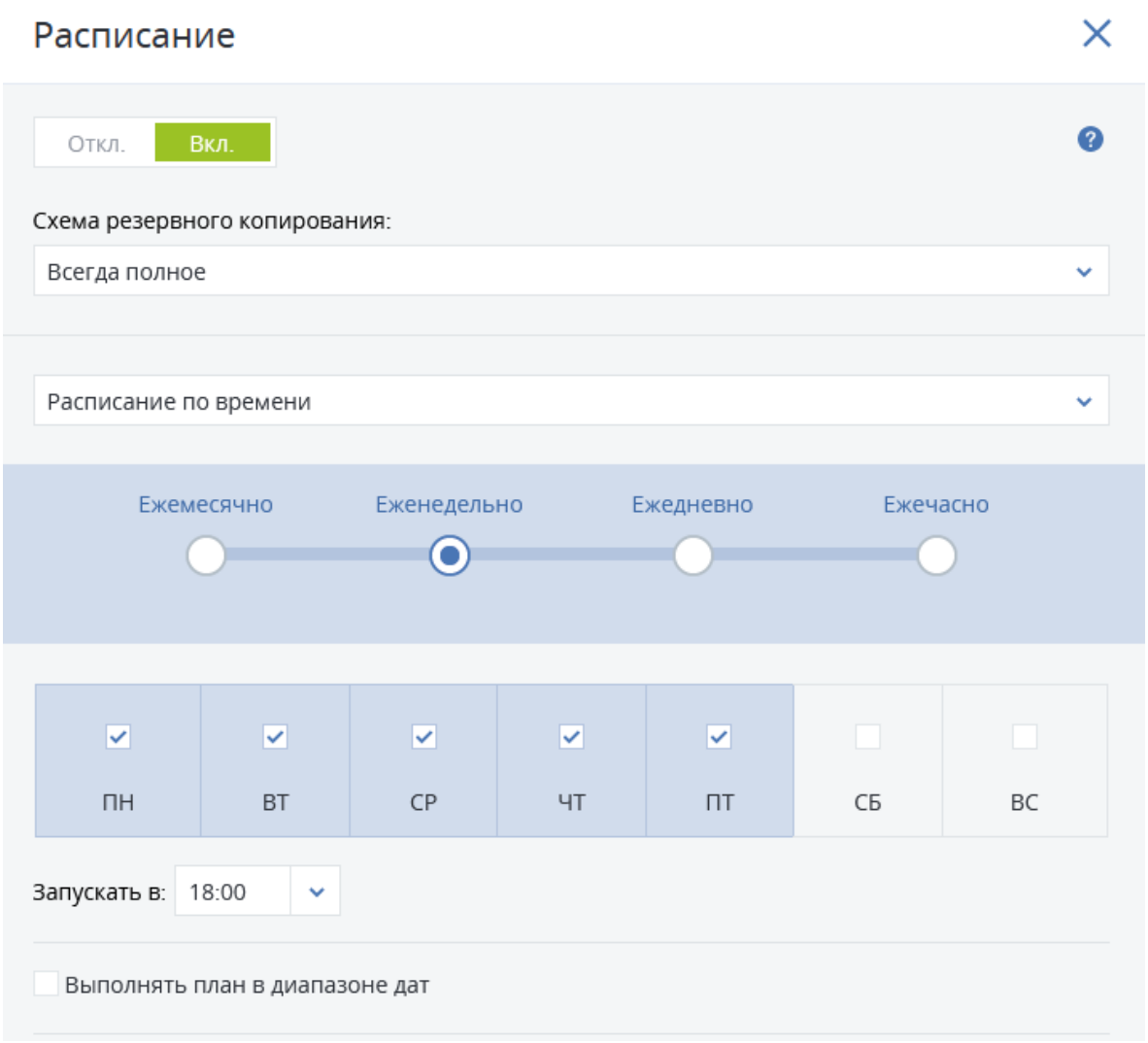
5. Заполните данные в окне создания плана защиты:

   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

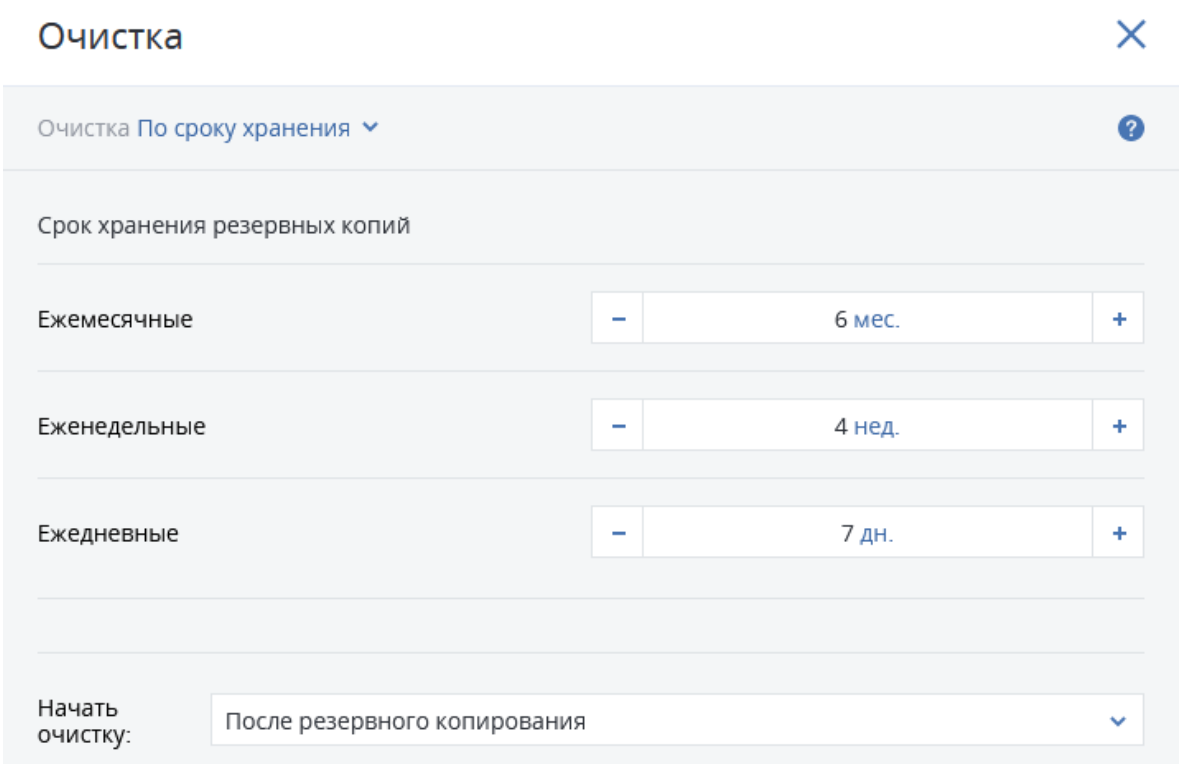


Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

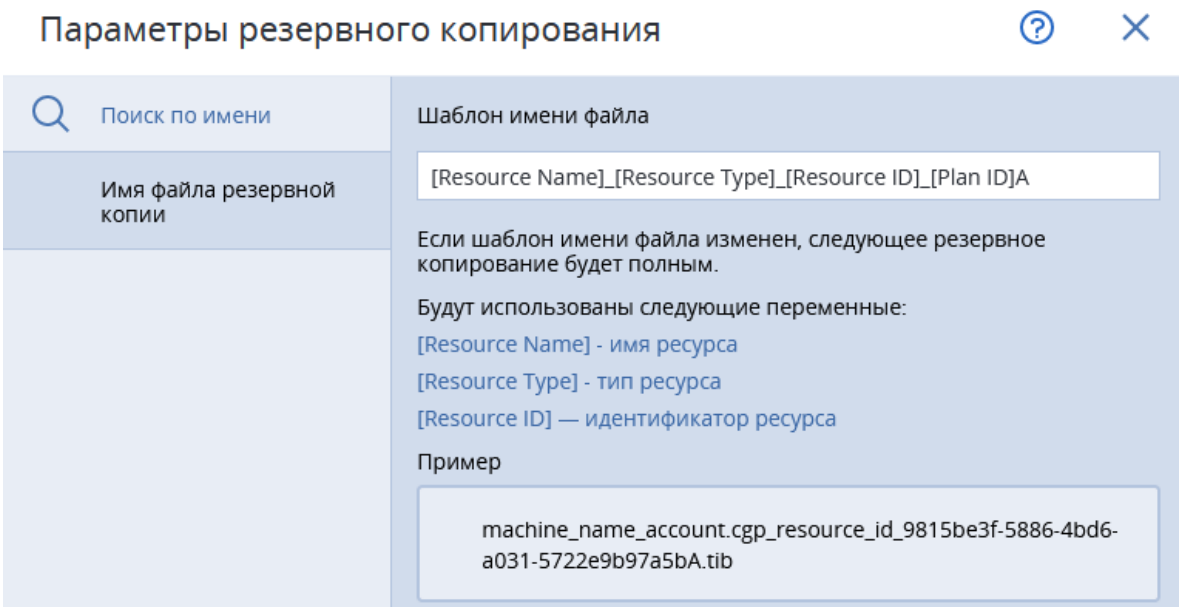
- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.

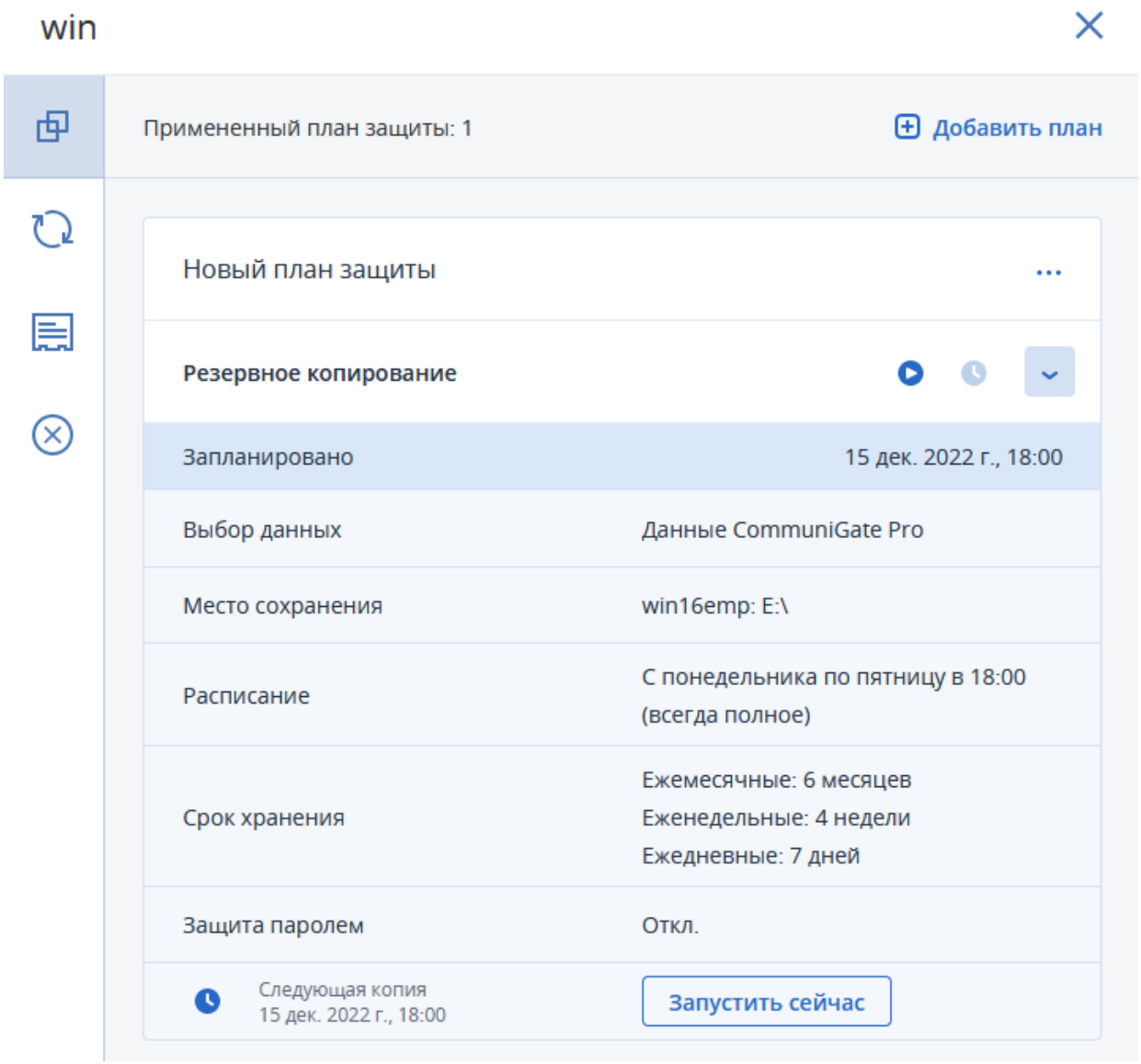


- [Необязательно] В поле **Параметры резервного копирования** укажите параметры для автоматического наименования файла резервного копирования.



Обратите внимание на то, что в случае изменения этих параметров следующее резервное копирование будет полным.

6. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов.



См. также информацию в разделе *План защиты и модули*.

Настройка плана защиты для CommuniGate Pro

Для настройки плана защиты CommuniGate Pro перейдите на вкладку **Планы** в меню веб-консоли.

Отметьте план, который вы хотите настроить. В меню справа появится список действий, доступных для этого плана.

В меню доступны следующие действия:

- **Сведения** - Подробные сведения о плане;
- **Остановить** - Остановка выполнения плана;
- **Изменить** - Изменение плана;

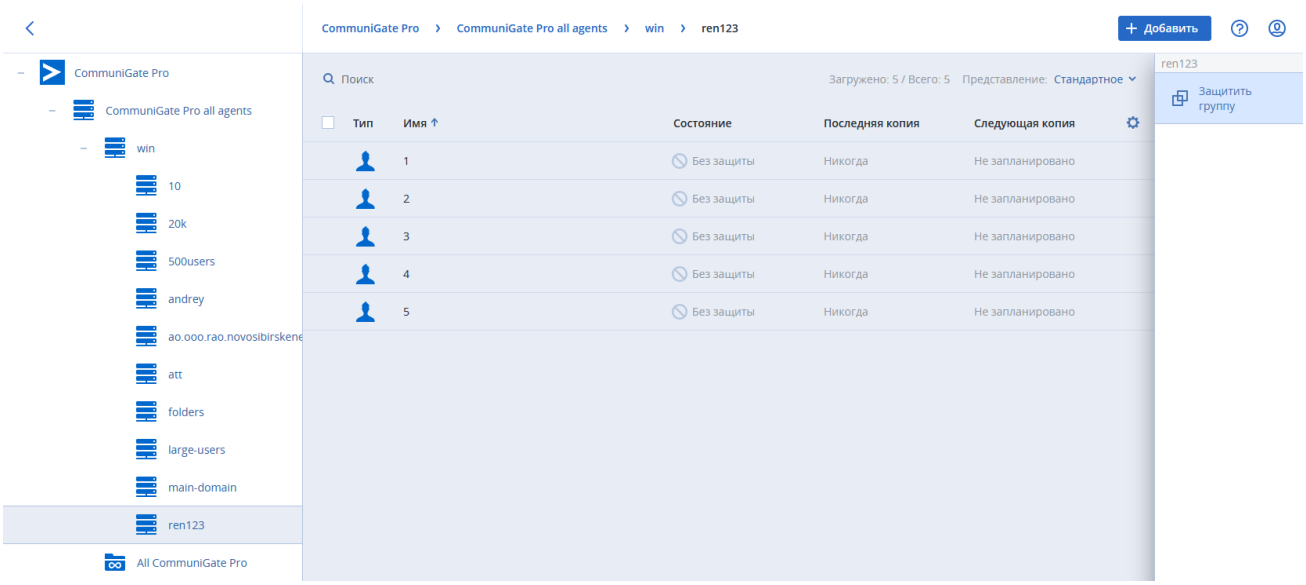
- **Действия** - Список действий, связанных с планом;
- **Оповещения** - Список оповещений, связанных с планом;
- **Клонировать** - Клонирование плана на другое устройство;
- **Экспорт** - Экспорт плана в файл;
- **Отключение (Включение)** - Включение/отключение плана одной кнопкой;
- **Удаление** - Удаление плана.

Подробнее о действиях с планами защиты см. в разделе *Операции с планами защиты*.

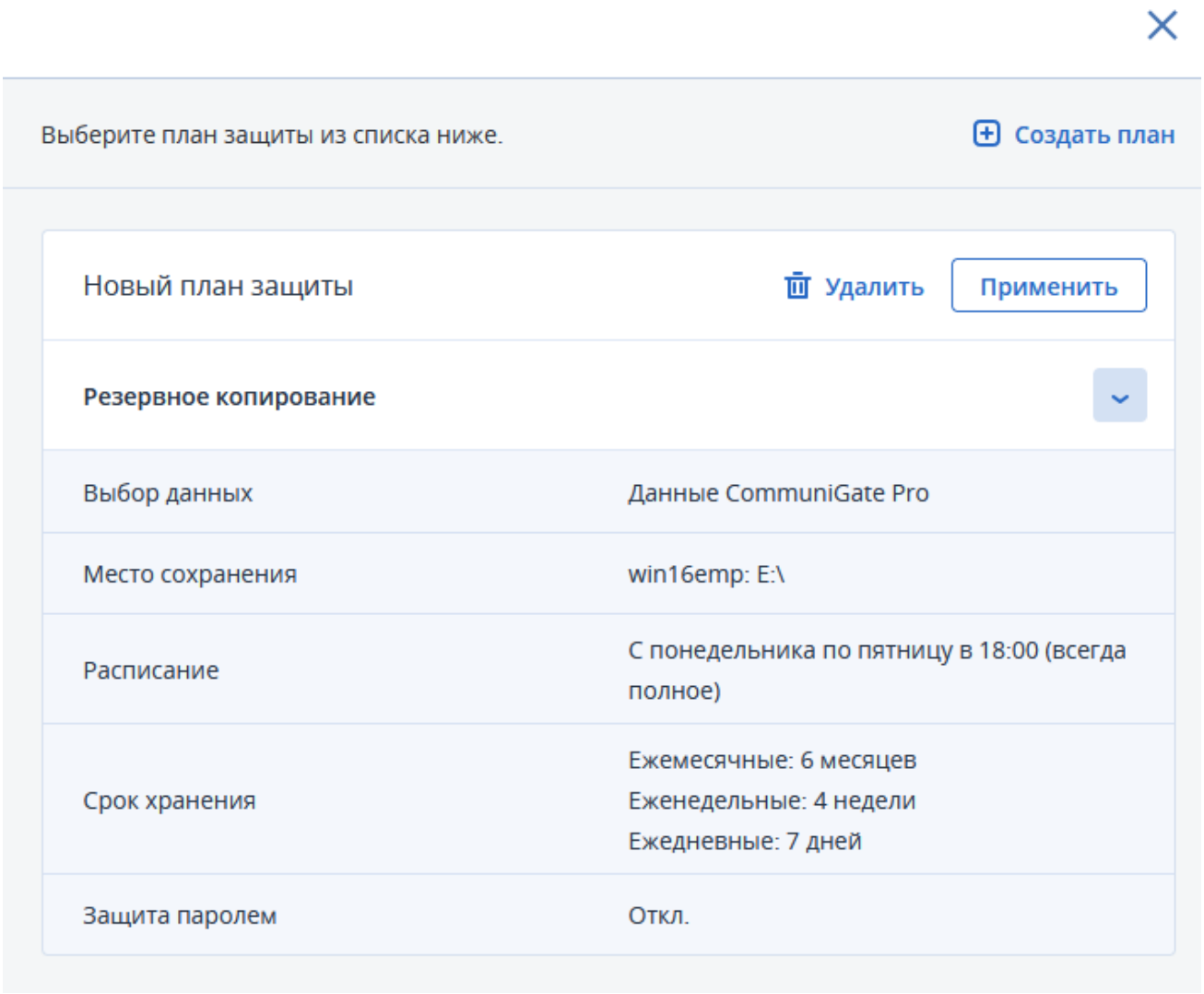
Резервное копирование данных CommuniGate Pro

Резервное копирование домена

Чтобы защитить домен, в списке доменов щёлкните по строке, содержащей название домена, и перейдите на вкладку **Защитить группу** в меню справа.



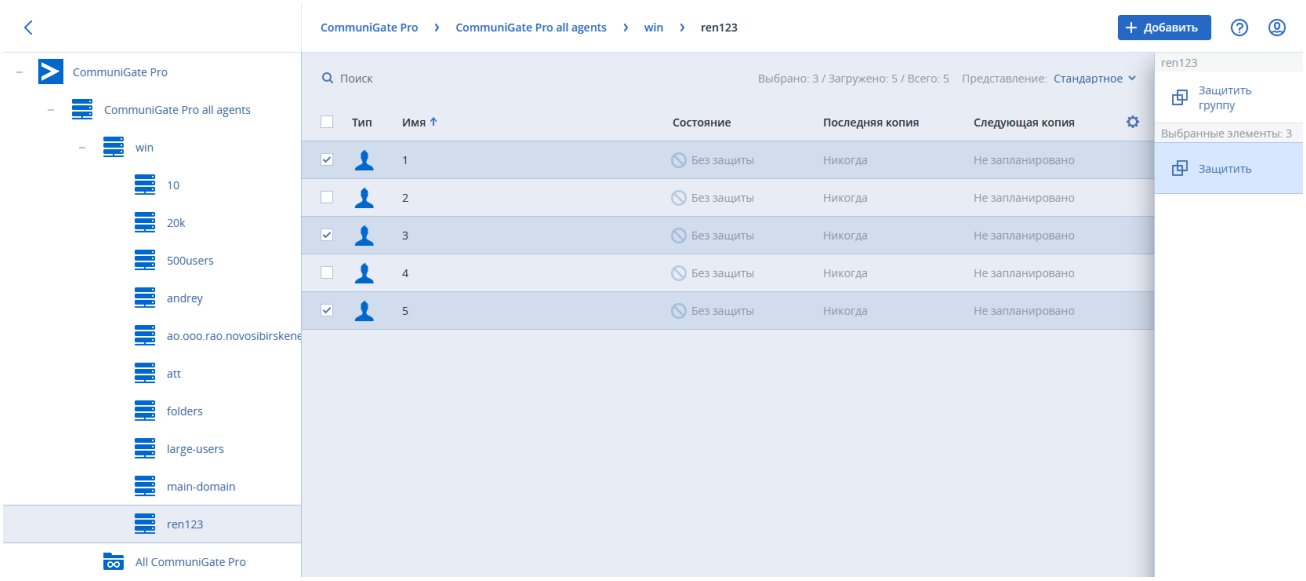
В окне выбора плана защиты в списке планов защиты выберите подходящий план и щёлкните **Применить**.



Резервное копирование почтового ящика

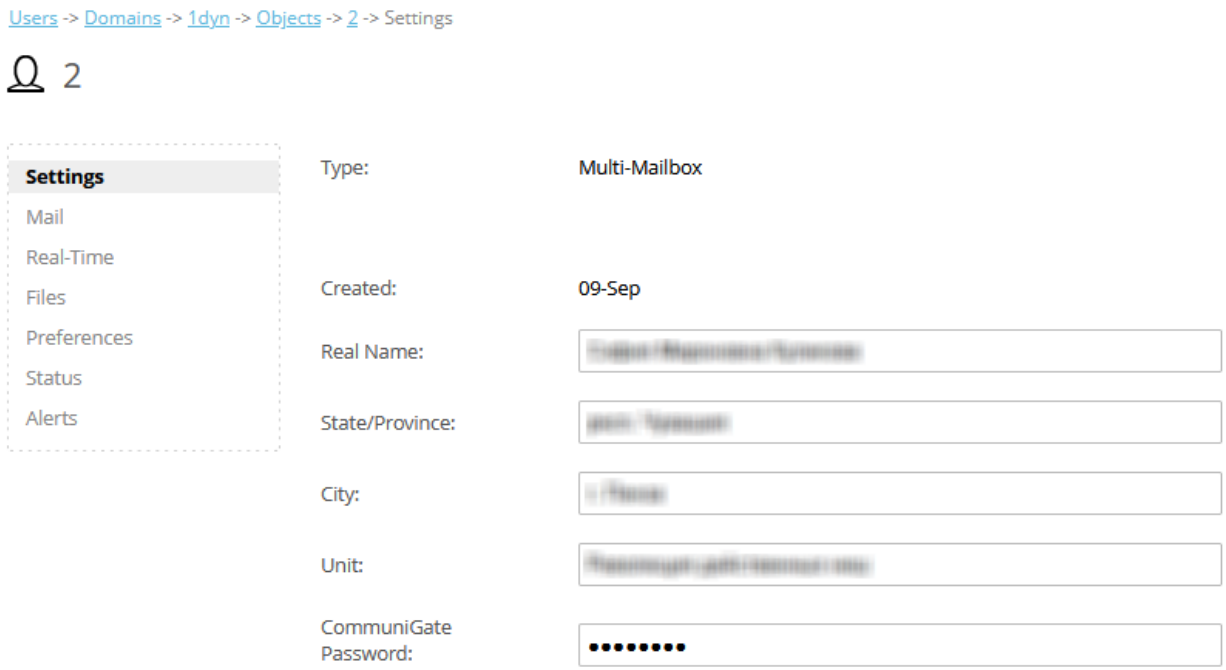
Чтобы защитить почтовый ящик, раскройте список почтовых ящиков в домене, щёлкните по строке, содержащей имя домена, и перейдите на вкладку **Защитить** в меню справа.

Чтобы выбрать несколько почтовых ящиков, входящих в домен, щёлкните по домену, затем отметьте флажок в окошке рядом с полем **Тип** и снимите флажки с почтовых ящиков, которые вы не хотите защищать. Перейдите на вкладку **Защитить** в меню справа.



В окне выбора плана защиты в списке планов защиты выберите подходящий план и щёлкните **Применить**.

> **Примечание**
>
> Защита настроек пользователя выполняется вместе с защитой его данных (почтового ящика). При этом защита касается только системных настроек. Эти настройки расположены в панели администратора CommuniGate Pro на следующей странице: **Users** → **Domains** → **Domain_name** → **Objects** → **Object_name** → **Settings**.



Резервное копирование по требованию

Резервное копирование по требованию представляет собой запуск выбранного плана защиты вне очереди. Чтобы выполнить резервное копирование по требованию:

- щёлкните по строке, содержащей название почтового ящика или домена
- перейдите на вкладку **Защитить** для почтового ящика или **Защитить группу** для домена в меню справа
- в строке **Резервное копирование** или в нижней части вкладки нажмите кнопку **Запустить сейчас**.

Резервное копирование больших объемов данных CommuniGate Pro

В Кибер Бэкап для резервного копирования данных CommuniGate Pro большого объема существуют следующие возможности:

- Резервное копирование с использованием нескольких агентов.
- Резервное копирование кластерных конфигураций.

Использование нескольких агентов

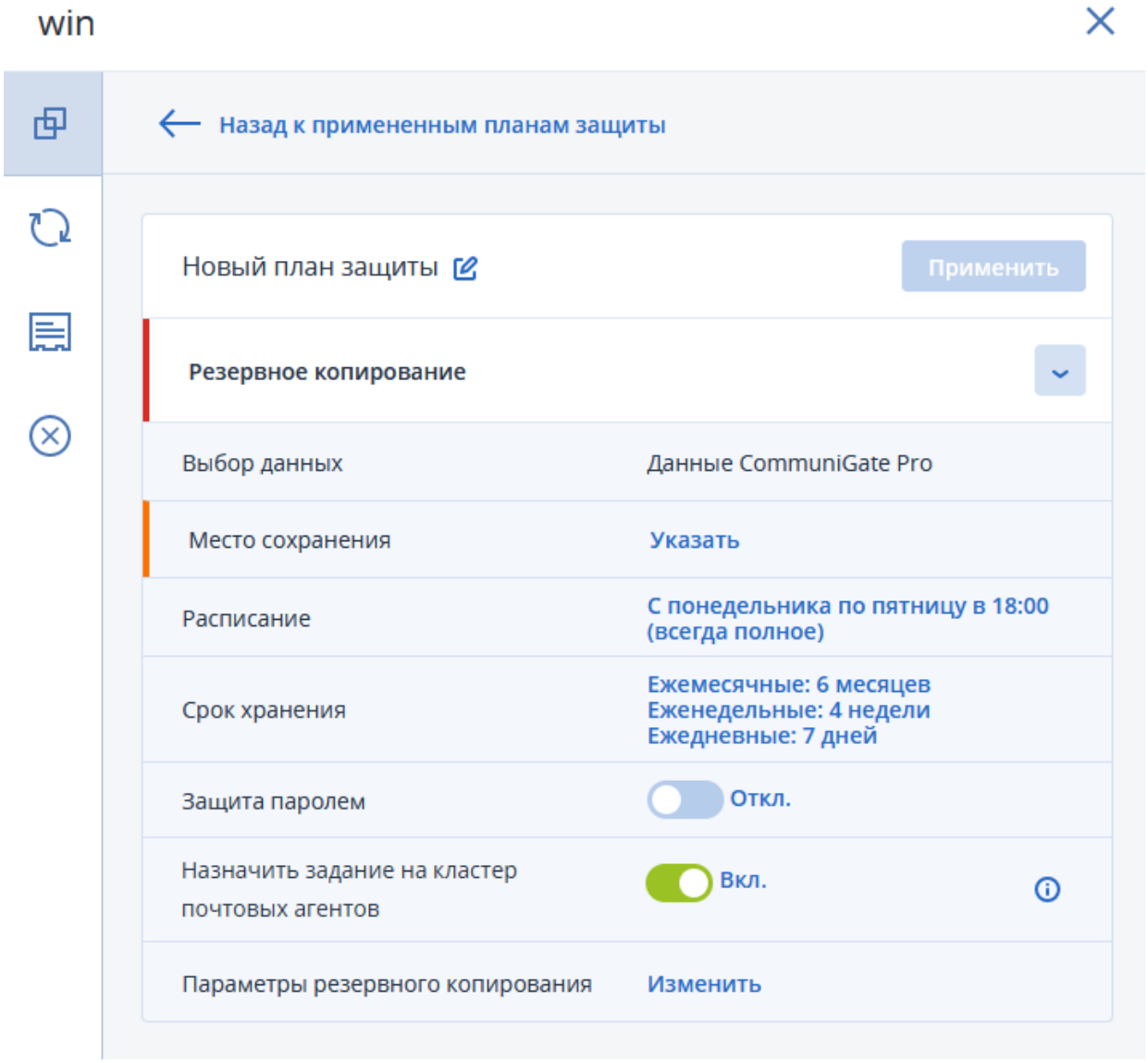
Для резервного копирования большого количества данных можно использовать сразу несколько агентов.

Для этого выполните следующие действия:

1. Зарегистрируйте необходимое количество агентов CommuniGate Pro (см. раздел *Установка CommuniGate Pro*). Агенты должны быть версии 17.3 или новее.
2. Создайте план резервного копирования для агентов. В резервном копировании будут участвовать все агенты CommuniGate Pro, зарегистрированные в Кибер Бэкап.

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** → **CommuniGate Pro**.
2. Выберите ресурсы CommuniGate Pro, для которых вы хотите создать план защиты.
3. На вкладке справа нажмите **Защитить** или **Защитить группу** (если выбрана группа почтовых ресурсов).



4. Введите данные в окне создания плана защиты:

   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, SFTP, папка NFS (только для Linux).

     Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

   - В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.
   - В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
   - В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным агентам.

- [Необязательно] В поле **Параметры резервного копирования** укажите метод разбиения резервных копий на меньшие по размеру фрагменты, параметры обработки ошибок и уровень сжатия резервных копий.

5. По окончании настройки плана нажмите **Применить**.

При резервном копировании несколькими агентами балансировка нагрузки происходит в режиме циклического перебора (round robin).

Резервное копирование кластеров CommuniGate Pro

При необходимости обслуживания большого количества (более 150—200 тыс.) почтовых ящиков пользователей или в случае серьезной сетевой нагрузки становится целесообразным использовать многосерверные кластерные конфигурации.

Кибер Бэкап поддерживает резервное копирование и восстановление серверных кластеров CommuniGate Pro.

Требования

Для резервного копирования кластерных конфигураций вам понадобятся установленные и настроенные системы:

- Кибер Бэкап версии 18.0 и выше;
- CommuniGate Pro версии не ниже 6.5.2.

Поддерживаются операционные системы:

- Windows;
- Linux.

Возможности

- Поддержка динамических и статических кластеров.
- Обнаружение ресурсов автоматически и вручную.
- Все операции, включая обнаружение ресурсов, резервное копирование и восстановление, используют любой из доступных серверов кластера. При неисправности какого-либо сервера следующая операция будет выполнена на одном из доступных серверов кластера.
- При необходимости любой сервер кластера может быть зарегистрирован как отдельный сервер. В этом случае будут доступны как домены кластера, так и локальные домены сервера.
- Поддерживается полное и инкрементальное резервное копирование.

- Поддерживается резервное копирование сервера (с помощью *дискового и файлового резервного копирования*).
- Доступен поиск по именам пользователей в архиве, при условии что имя пользователя содержится в имени архива.

Ограничения

- Агент Кибер Бэкап может работать только с одним сервером (хостом) CommuniGate Pro.
- Все серверы кластера должны иметь доступ к агенту. Если агент не имеет доступа к какому-либо серверу, этот сервер будет помечен как **offline**.
- Все серверы кластера должны разрешать авторизацию одного и того же пользователя с одним и тем же паролем.
- Не поддерживается работа через балансировщик нагрузки кластера.
- При обнаружении ресурсов доступны только ресурсы динамического кластера. Ресурсы, принадлежащие определенному серверу, недоступны для обнаружения.
- Для резервного копирования доступны только домены, принадлежащие динамическому кластеру. Домены, принадлежащие определенному серверу, недоступны для резервного копирования.
- Не поддерживается резервное копирование сервера в кластерной конфигурации (также см. главу ”Возможности”).

Установка

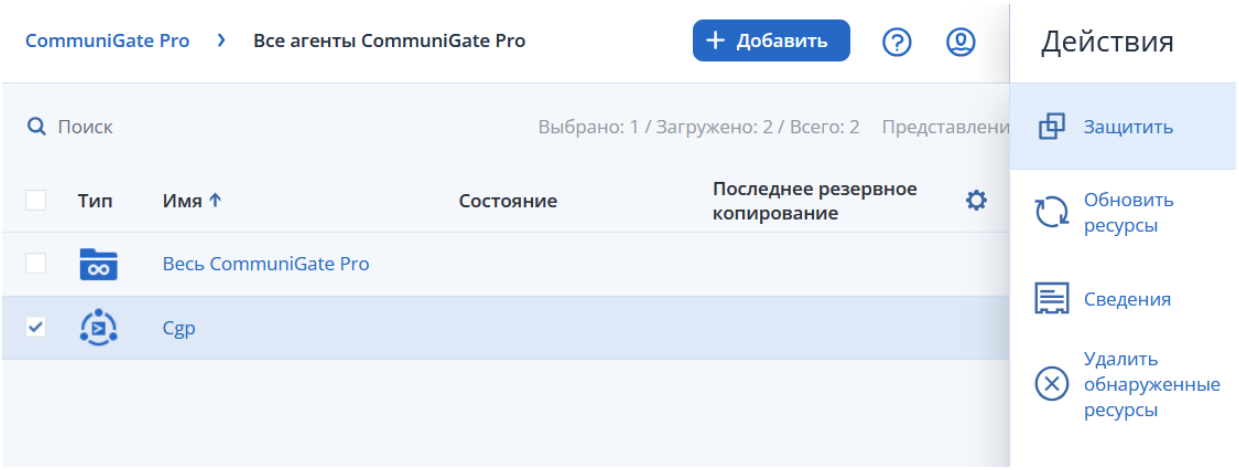
Для установки см. раздел *Установка CommuniGate Pro*.

Для регистрации кластера CommuniGate Pro укажите данные любого сервера, входящего в кластер. Этот сервер должен быть доступен для агента. Процесс регистрации кластерного сервера аналогичен процессу регистрации одиночного сервера.

Резервное копирование кластера

Для резервного копирования кластера выполните следующие действия:

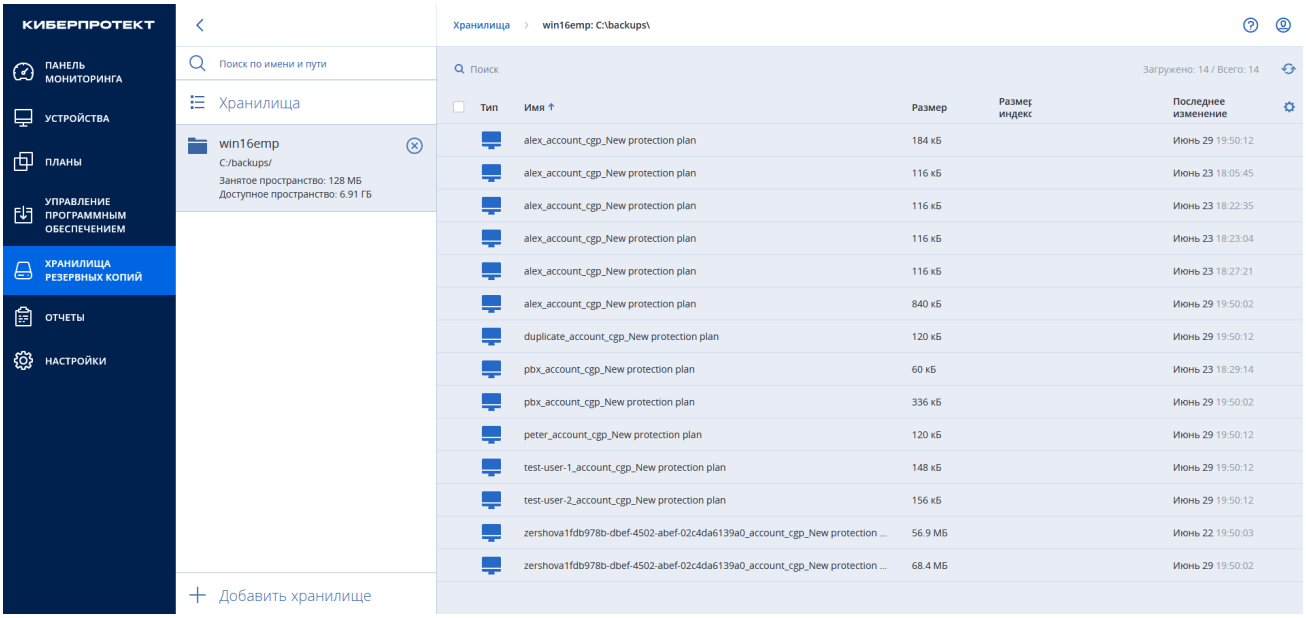
1. В веб-консоли перейдите на вкладку **Устройства** → **CommuniGate Pro**.
2. Выберите в списке кластер, который хотите защитить.



3. [Необязательно] Для обнаружения новых ресурсов нажмите **Обновить ресурсы**.
4. Щёлкните в меню справа **Защитить**.
5. Создайте новый план защиты или выберите существующий.
6. Укажите необходимые настройки плана. Поддерживаются следующие места сохранения: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SMTP.
7. По окончании настройки плана нажмите **Применить**.

Резервные копии CommuniGate Pro

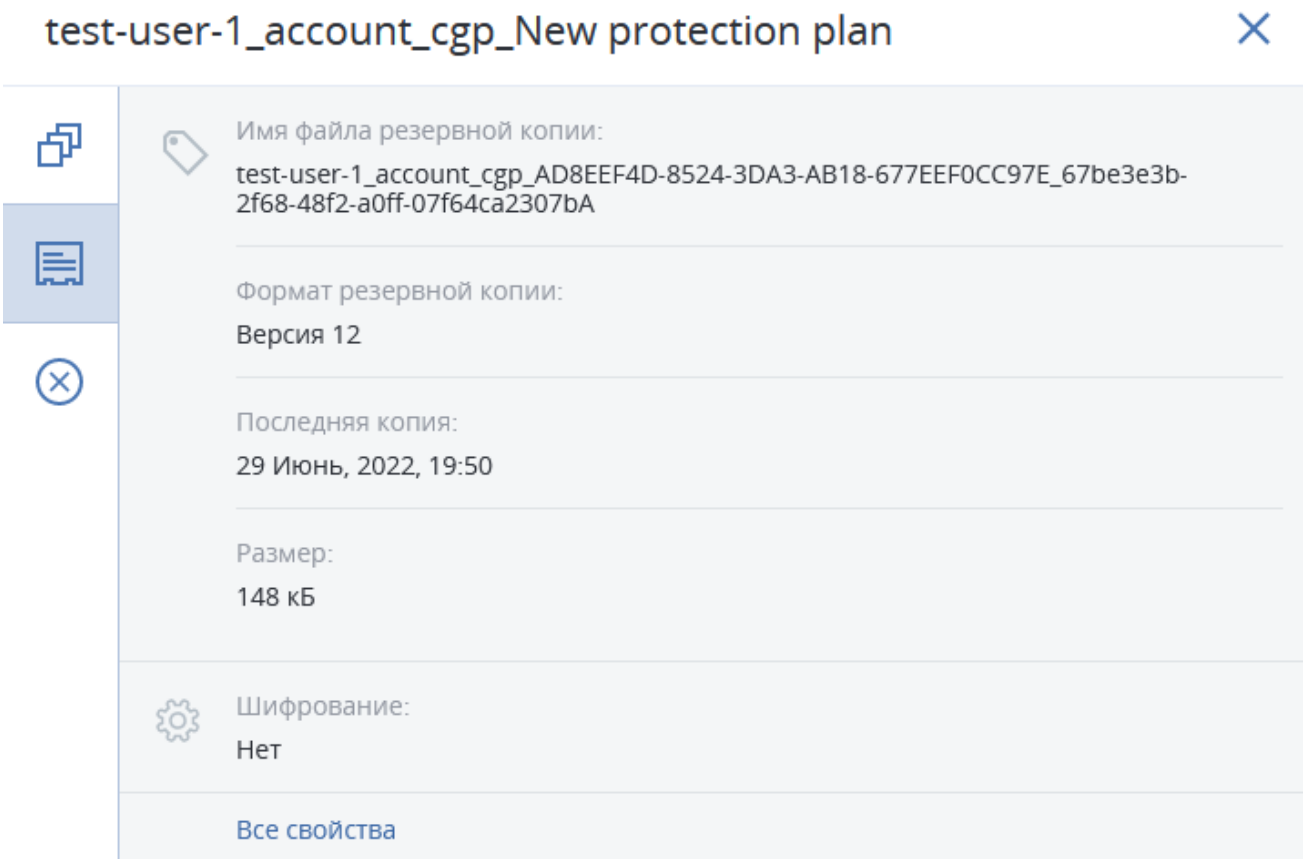
Чтобы посмотреть список резервных копий компьютеров, перейдите на вкладку **Хранилища резервных копий**.



Чтобы посмотреть список резервных копий для компьютера, щёлкните на строку с названием

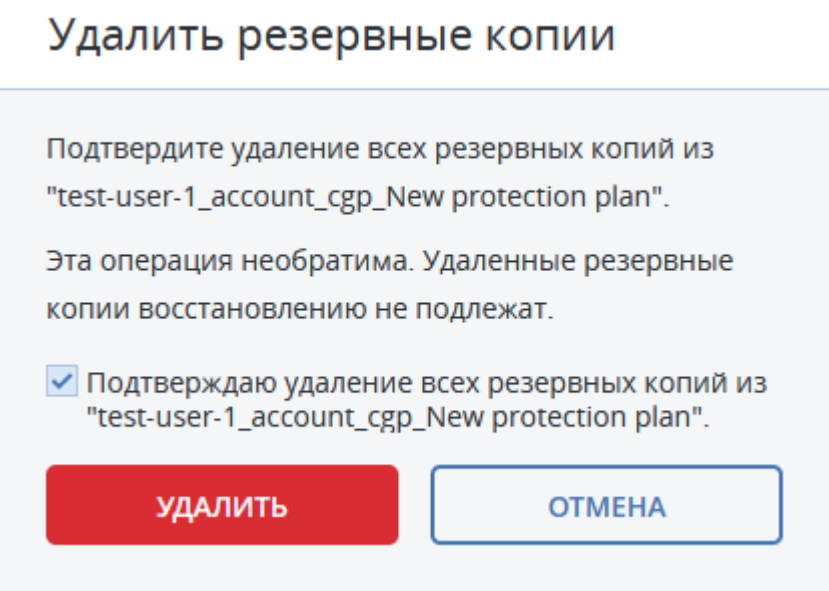
компьютера и затем перейдите на вкладку **Показать резервные копии** в меню справа. Откроется список резервных копий. Из этого меню также можно восстановить одну из резервных копий для этого компьютера.

Чтобы посмотреть сведения о резервной копии, щёлкните по строке, содержащей название резервной копии, и перейдите на вкладку **Сведения** в меню справа.



Подробная информация доступна по ссылке **Все свойства**.

Чтобы удалить резервную копию, перейдите на вкладку **Удалить** в меню справа.



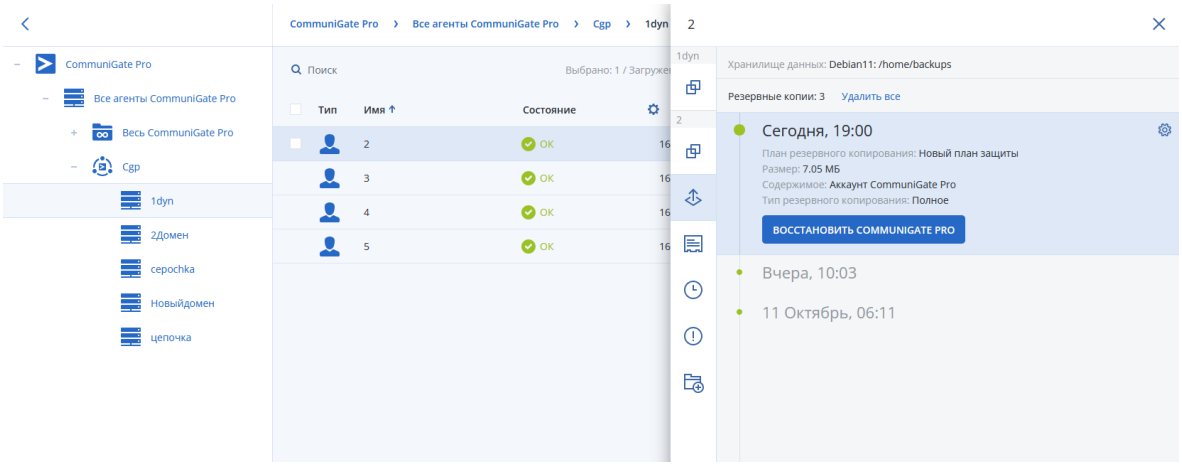
Для подтверждения удаления отметьте флажок в поле и нажмите **Удалить**. Выбранная резервная копия после удаления исчезнет из списка резервных копий.

Для удаления резервной копии см. также *Восстановление CommuniGate Pro*.

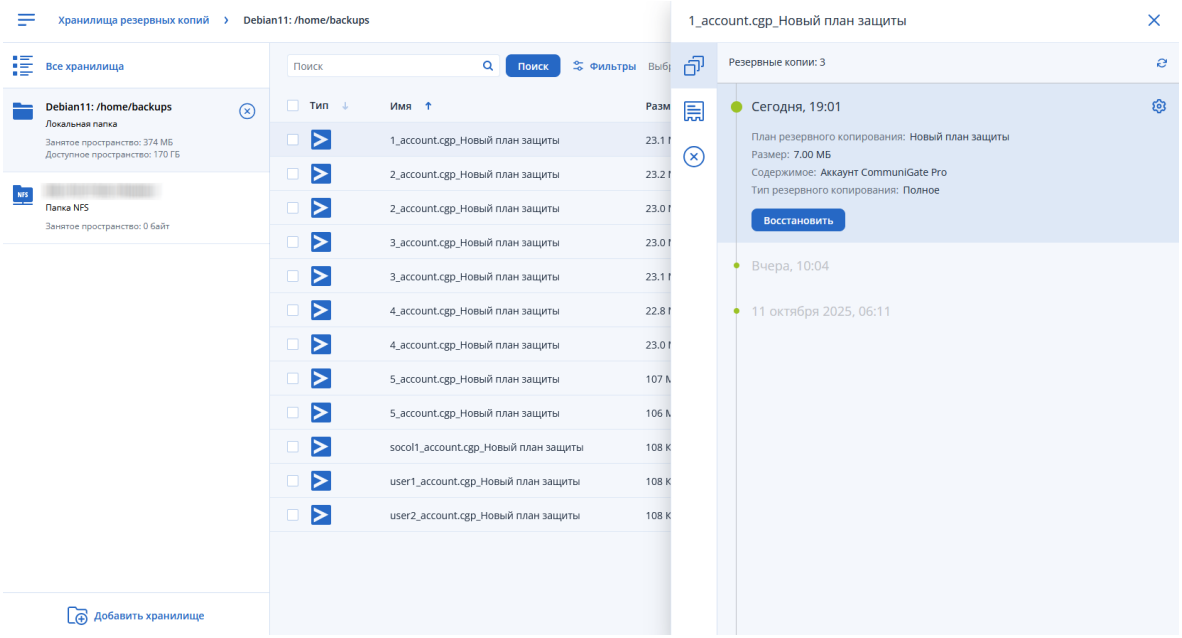
Восстановление CommuniGate Pro

1. Выполните одно из следующих действий:

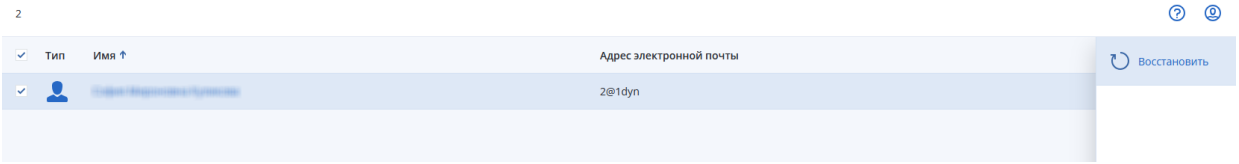
    1. Перейдите в **Устройства** → **CommuniGate Pro**, щёлкните кластер, сервер или домен, данные в котором хотите восстановить, выберите в списке нужный аккаунт (учетную запись), справа в меню щёлкните **Восстановление** и далее **Восстановить CommuniGate Pro**.



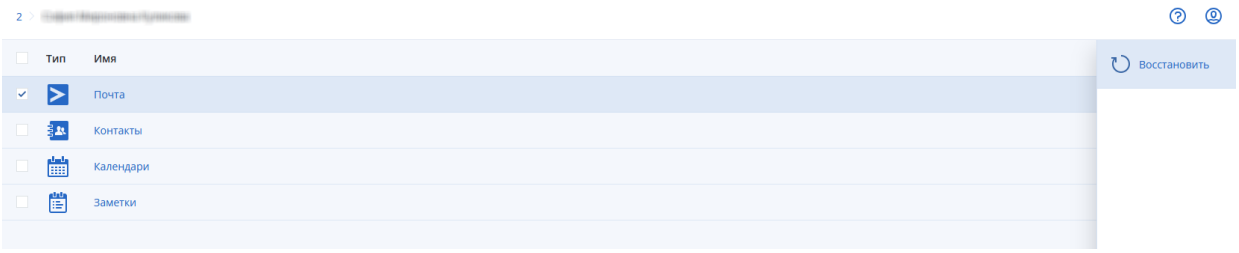
    2. Перейдите в **Хранилище резервных копий**, щёлкните хранилище с резервными копиями, выберите в списке нужный аккаунт и нажмите **Восстановить**.



2. Для восстановления всех данных пользователя отметьте галочкой имя пользователя и нажмите **Восстановить**. Иначе просто щёлкните имя пользователя.

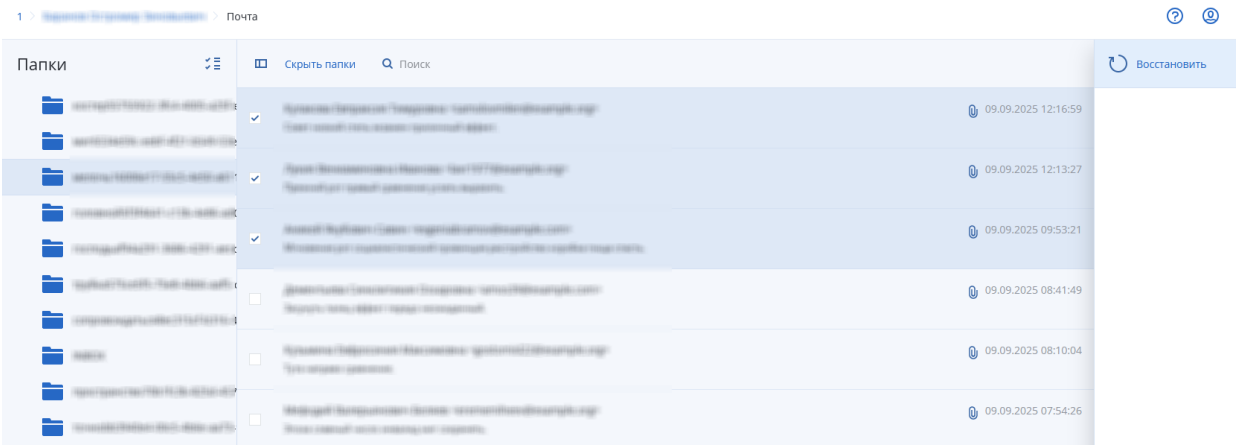


3. Для восстановления всех данных одного типа отметьте галочкой тип восстанавливаемых данных (**Почта**, **Контакты**, **Календари**, **Заметки**).



Для восстановления определенных данных щёлкните на названии типа нужных данных (например, **Почта**) и далее в списке отметьте галочками те данные (например, письма), которые необходимо восстановить.

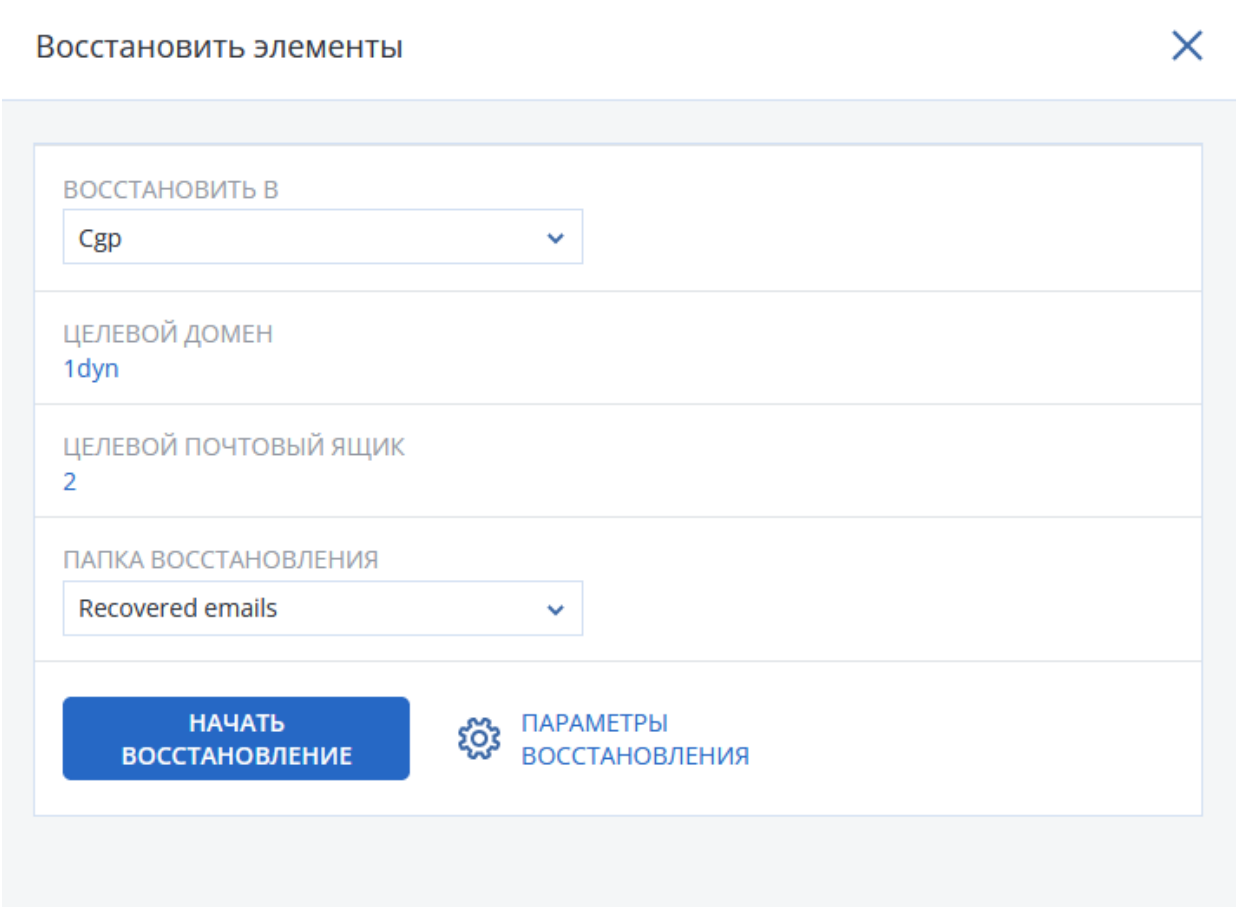
> **Примечание**
>
> Восстановление на новый сервер можно выполнить только при восстановлении всех данных пользователя или всех данных одного типа.



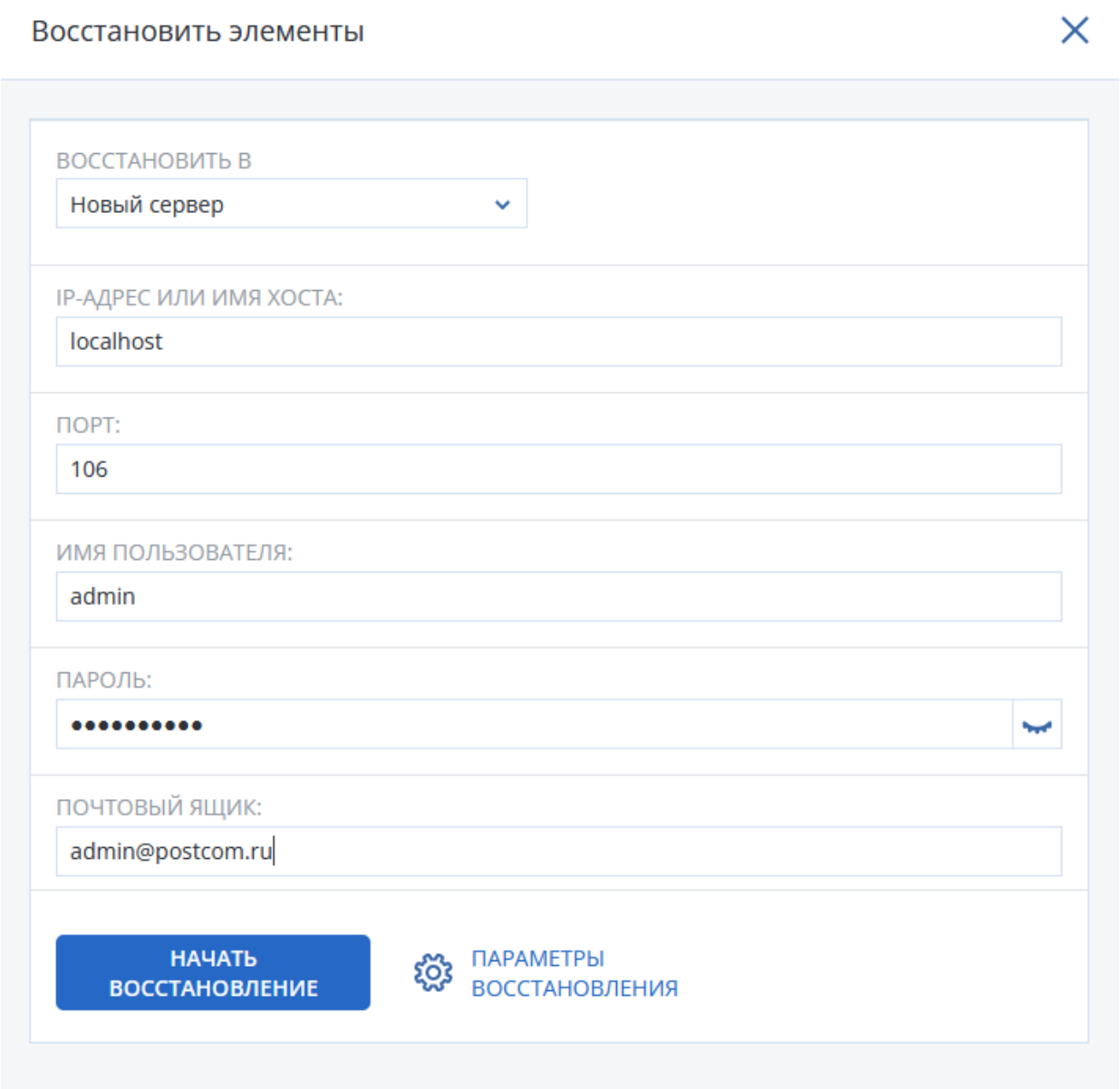
Для просмотра содержимого письма нажмите справа **Показать содержимое**. Для скачивания вложения щёлкните по этому вложению.

Для поиска нажмите значок поиска сверху. Для почты доступен расширенный поиск, для его настройки нажмите значок выпадающего списка в строке поиска.

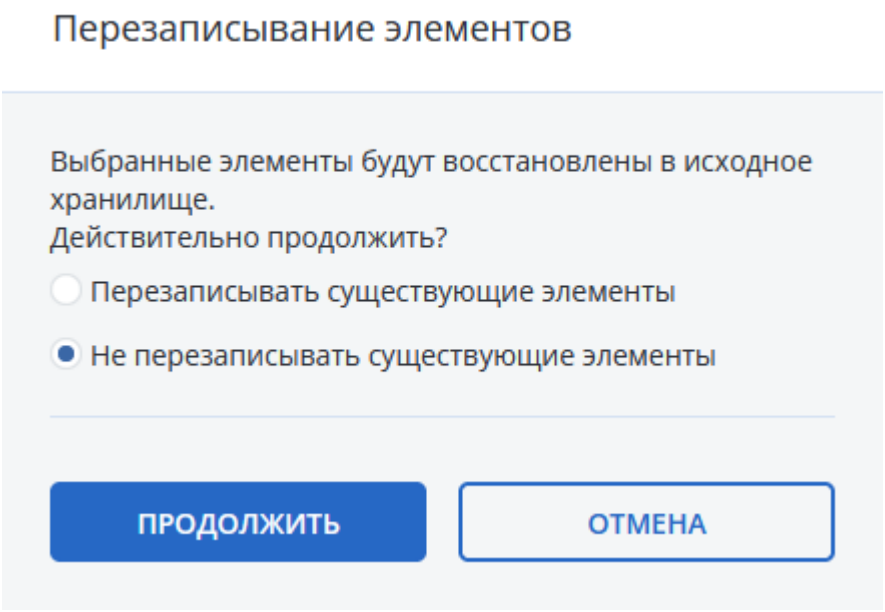
4. Нажмите **Восстановить**.
5. На экране **Восстановить элементы** укажите место для восстановления:
    1. Существующий сервер или новый сервер;
    2. Домен (из существующих);
    3. Почтовый ящик (из существующих);
    4. Папка для восстановления (если происходит восстановление выбранных вами данных одного типа).



При восстановлении на новый сервер укажите параметры нового хранилища.



6. Закончив выбор, нажмите **Начать восстановление**.
7. На экране **Перезаписывание элементов** подтвердите или отклоните перезапись существующих данных при восстановлении.



Примечание

Перезапись draft не работает должным образом из-за ограничений в CommuniGate Pro.

Важно

При выборе перезаписи существующие данные будут уничтожены!

Примечание

При перезаписи уничтожены будут данные, совпадающие с данными из архива. Если в почтовых ящиках с момента создания последней резервной копии появились новые данные, то они не будут уничтожены.

Ход выполнения восстановления показан на вкладке **Действия**.

На вкладке **Восстановление** доступно также удаление резервной копии.

Удаление резервной копии

1. Щёлкните резервную копию, которую хотите удалить.
2. Щёлкните значок настройки справа вверху.
3. Нажмите **Удалить**.

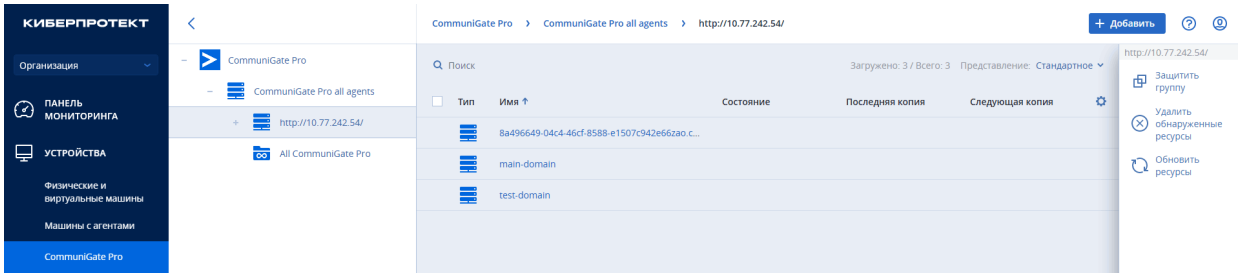
Чтобы удалить все резервные копии, во вкладке **Восстановление** щёлкните **Удалить все**.

Удаление CommuniGate Pro

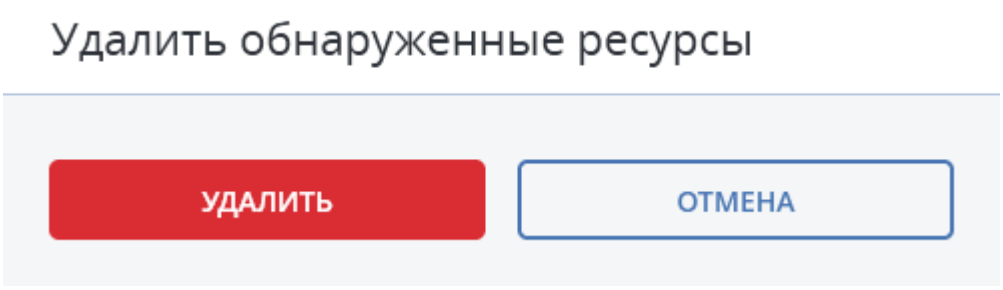
Вы можете удалить хост CommuniGate Pro отдельно, не удаляя сам агент и резервные копии.

Порядок удаления хоста CommuniGate Pro

1. В веб-консоли перейдите на вкладку **Устройства** → **CommuniGate Pro**.
2. Отметьте хост CommuniGate Pro в списке.
3. В меню справа щёлкните **Удалить обнаруженные ресурсы**.



4. В окне подтверждения удаления нажмите **Удалить**.



Устройство будет удалено из списка.

Примечание

Удаление машины не затрагивает агента и хранящиеся на ней резервные копии.

Защита VK WorkMail и VK WorkDisk

VK WorkMail — масштабируемое и отказоустойчивое решение корпоративного класса для работы с почтой, календарем, контактами и для просмотра документов.

VK WorkDisk — облачное хранилище, которое предоставляет возможность безопасного хранения и обмена файлами внутри организации.

С помощью Кибер Бэкап можно выполнять резервное копирование данных VK WorkMail и VK WorkDisk. Резервное копирование данных VK WorkDisk производится для пользователей, которые используют почтовый сервис VK WorkMail. При использовании Кибер Бэкап регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователей и различных сбоев. Удаленные элементы можно восстановить из резервной копии.

Условия для резервного копирования

Для резервного копирования данных VK WorkMail понадобятся установленные и настроенные продукты:

- Кибер Бэкап 16.5 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе *Издания и лицензии Кибер Бэкап*).
- VK WorkMail.

Для резервного копирования данных VK WorkDisk понадобятся установленные и настроенные продукты:

- Кибер Бэкап 17.1 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе *Издания и лицензии Кибер Бэкап*).
- VK WorkMail с подключенными ресурсами VK WorkDisk.

Поддерживаемые версии VK WorkMail указаны в разделе *Поддерживаемые почтовые сервисы*.

Для лицензирования VK WorkDisk используется лицензия VK WorkMail. Она автоматически подключается при создании плана защиты данных пользователя VK WorkDisk.

Для выполнения резервного копирования требуется установка агента.

Поддерживается установка агента для следующих операционных систем:

- Windows,
- Linux.

Полный список поддерживаемых операционных систем Windows и Linux см. в разделе *Поддерживаемые операционные системы*.

Возможности

Кибер Бэкап обеспечивает резервное копирование и восстановление:

- данных пользователя VK WorkMail (почтовый ящик, календарь, профиль пользователя и адресная книга пользователя),

  > **Примечание**
  >
  > При резервном копировании профиля пользователя создаются копии следующих настроек пользователя: **Имя отправителя**, **Автоответчик**, **Уведомления**, **Отправка писем**, **После удаления письма**, **Адресная книга**, **Права доступа к почте**.
  >
  > Резервное копирование файлов, прикрепленных к событиям в календаре, происходит при резервном копировании VK WorkDisk пользователя. При резервном копировании календаря создаются только копии ссылок прикрепленных событий на место хранения событий в VK WorkDisk пользователя.

- отдельных писем пользователей VK WorkMail,
- глобальных адресных книг VK WorkMail,
- данных пользователя VK WorkDisk,
- серверов VK WorkMail и VK WorkDisk.

Также возможно скачивать отдельные файлы или данные пользователей из существующих резервных копий.

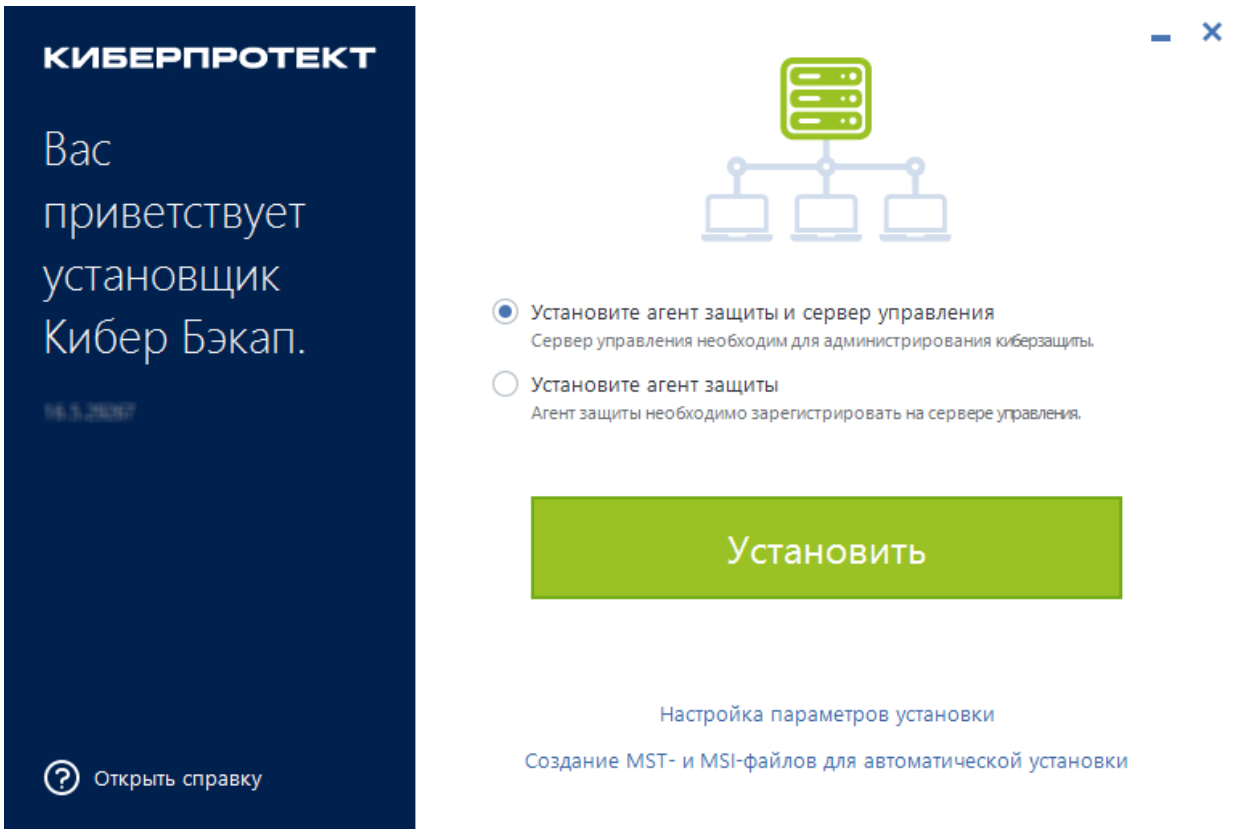
Установка VK WorkMail

Установка VK WorkMail включает в себя установку агента Кибер Бэкап и добавление хоста VK WorkMail. Добавление хоста возможно лишь после установки агента.

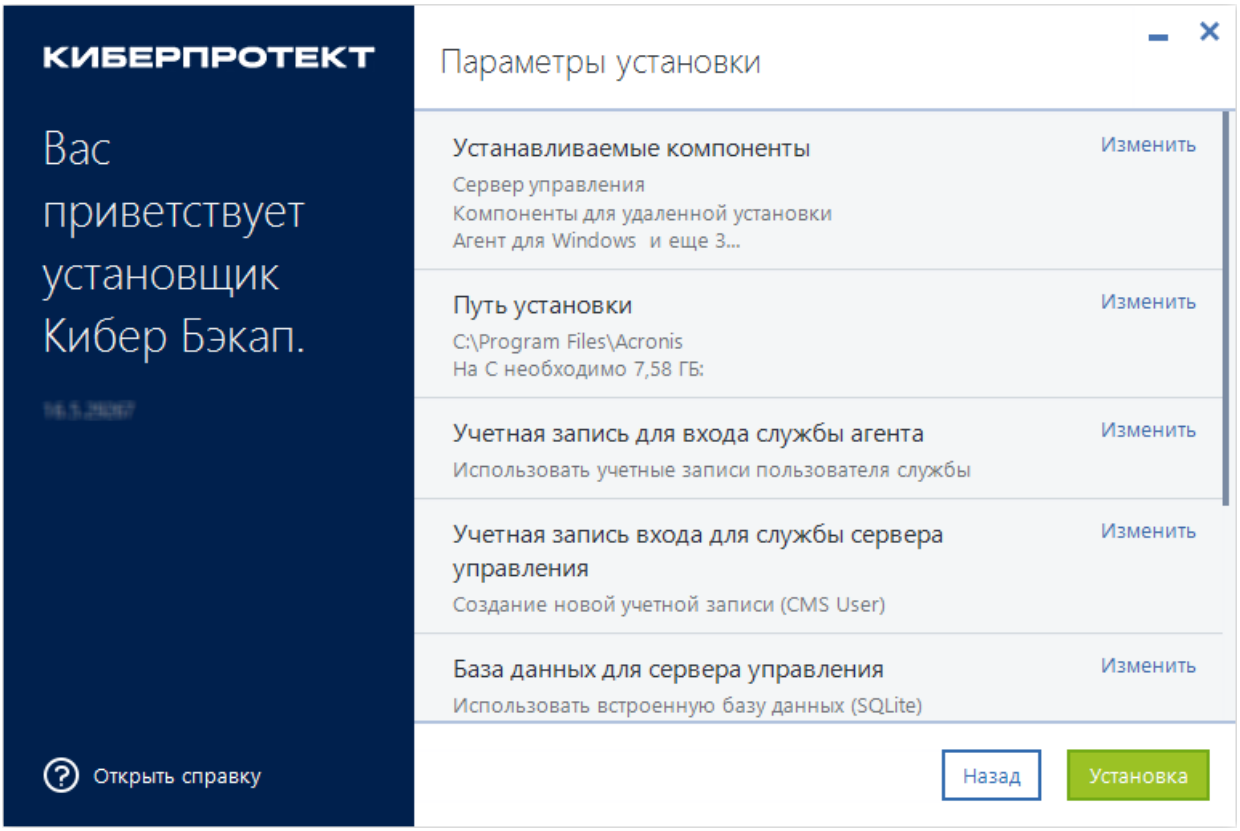
Установка агента для VK WorkMail

В этом разделе рассмотрена установка агента Кибер Бэкап для Windows. Для установки агента для Linux обратитесь к разделу *Установка в Linux*.

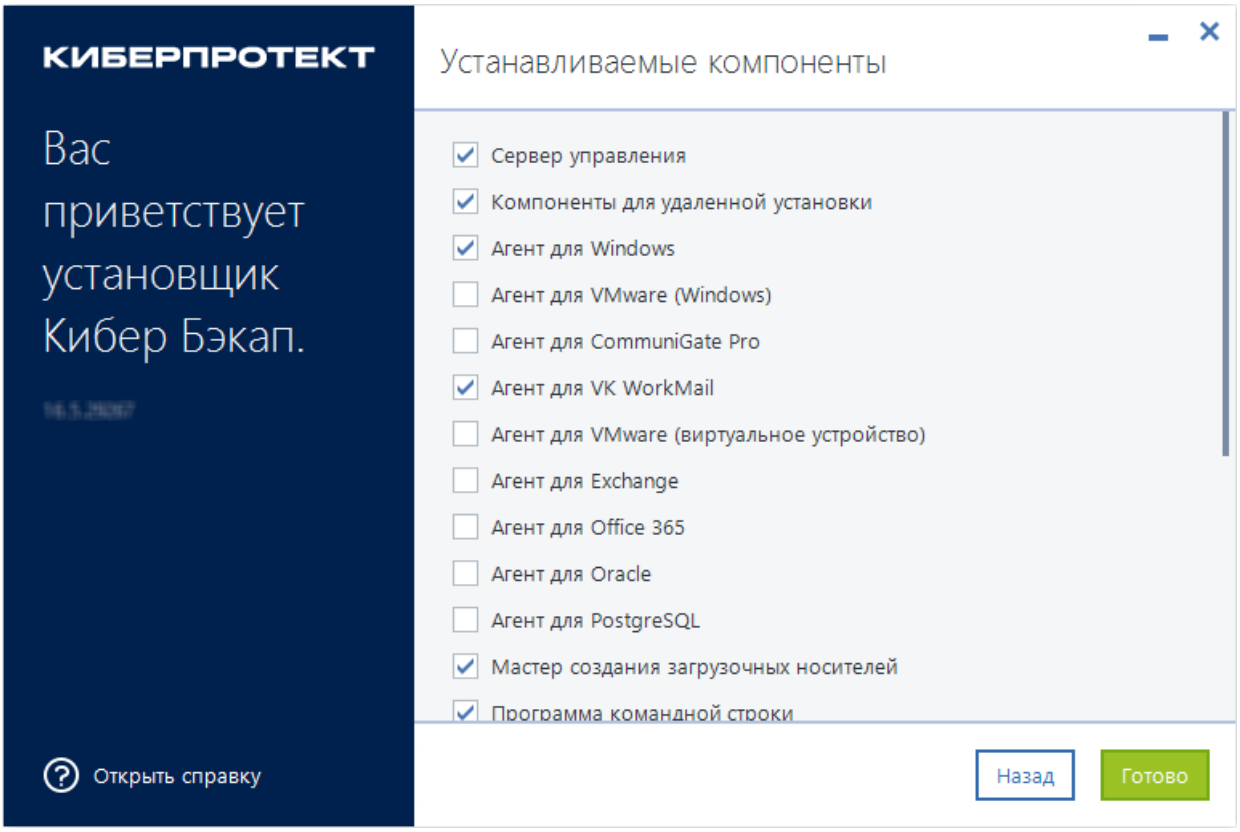
1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.



3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.



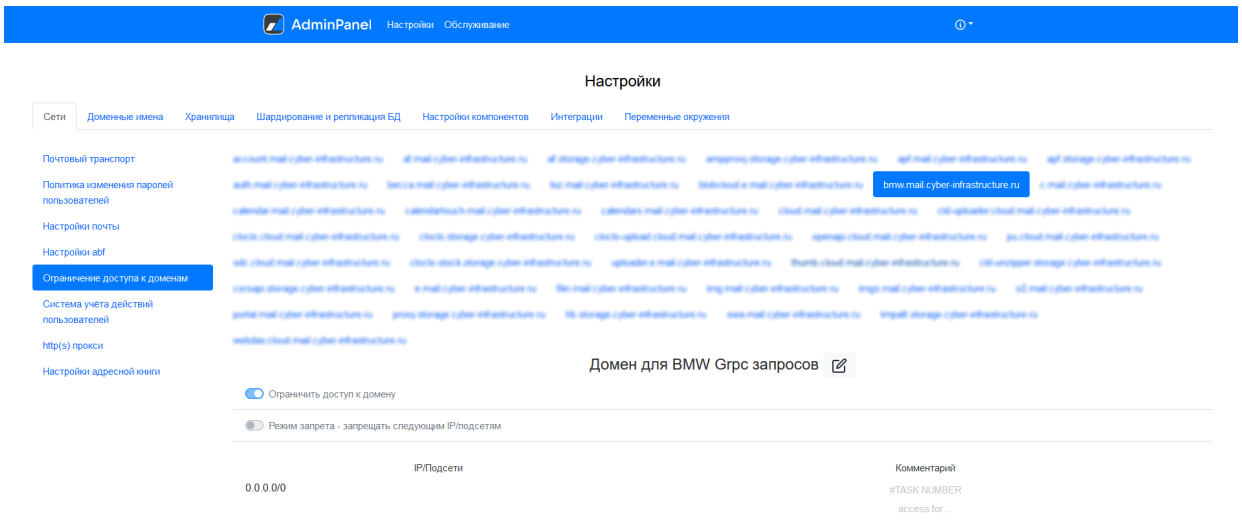
4. Отметьте в списке **Агент для VK WorkMail**.



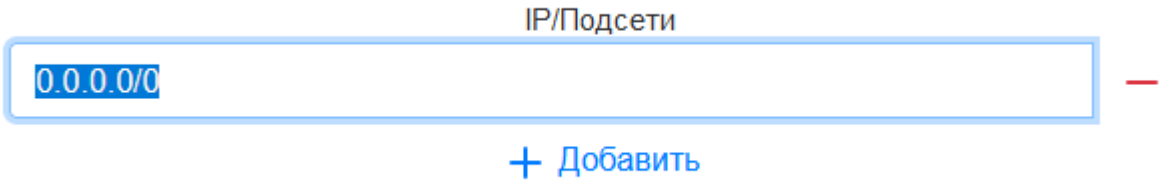
5. Щёлкните **Готово**.

Настройка в панели администрирования VK WorkMail

1. Укажите настройки в панели администрирования VK WorkMail аналогично следующему примеру:



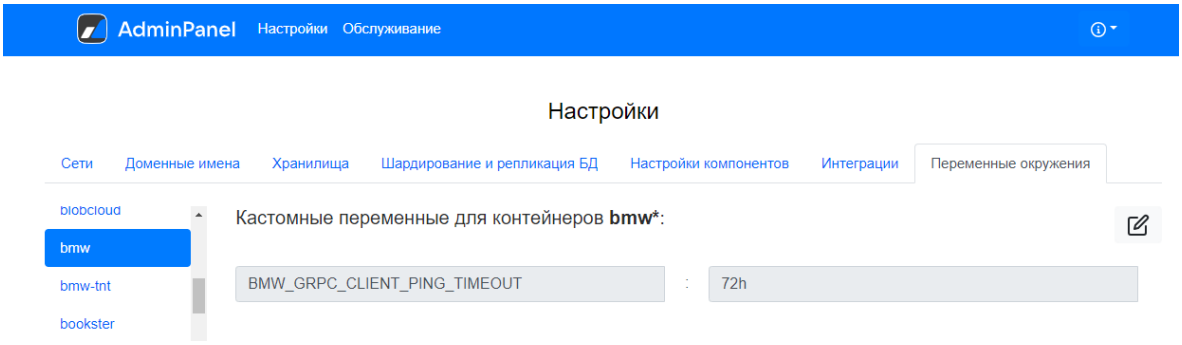
2. Для настройки IP-адреса нажмите значок редактирования  и введите IP-адрес компьютера, на который установлен агент для VK WorkMail.



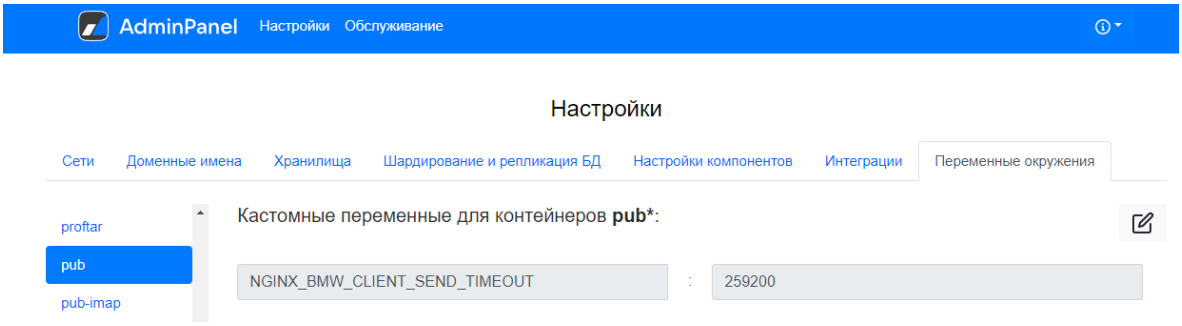
3. Нажмите **Сохранить**.
4. Добавьте переменные окружения:
    1. Перейдите в раздел **Настройки** и откройте вкладку **Переменные окружения**.
    2. В списке слева выберите контейнер **bmw** и создайте следующие переменные:
        - `BMW_GRPC_CLIENT_PING_TIMEOUT`, значение `72h`. Переменная устанавливает время ожидания новой ленты при заполнении предыдущей.
        - `BMW_GRPC_MAX_MESSAGE_SIZE_MB`, значение `256`. Переменная устанавливает максимальный размер писем для резервного копирования и восстановления.
        - `AMELI_WORKERS`, значение `10`. Переменная необходима для ускорения взаимодействия VK WorkMail и Кибер Бэкап.

            > **Примечание**
            >
            > Для VK WorkMail 26.2 и новее необходимо создавать переменную `AMELI_BACKUPER_THREADS`.

        - `BMW_MESCALITO_RESTORE_FIBERS`, значение зависит от конфигурации, его необходимо запросить у сотрудников технической поддержки платформы VK WorkSpace. Переменная необходима для восстановления почтовых ящиков, в которых есть письма с вложениями большого размера.
        - [VK WorkMail 26.1 и новее] `BMW_GRPC_DISABLE_DEPRECATED_METHODS`, значение `false`. Переменная используется для отключения проверок на использование устаревших методов удалённого вызова процедур.

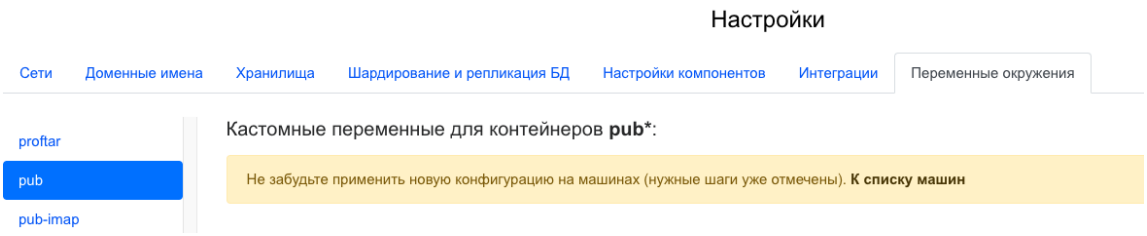


3. В списке слева выберите контейнер **pub**, создайте переменную `NGINX_BMW_CLIENT_SEND_TIMEOUT` и укажите для нее значение `259200`.

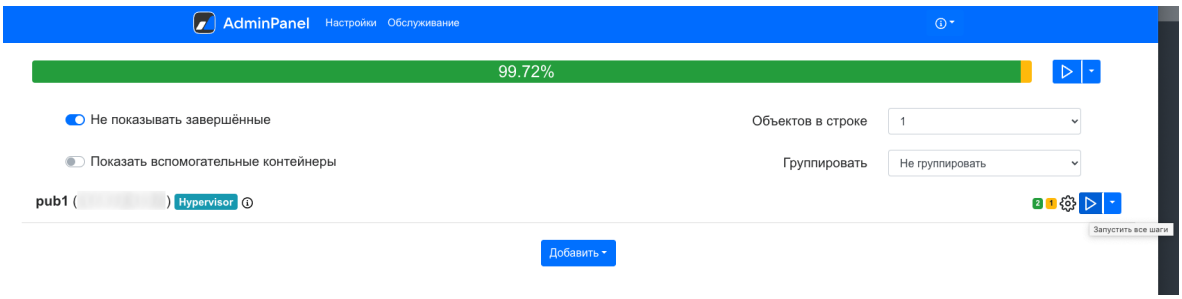


4. В списке слева выберите контейнер **stz-skel-ss**, создайте переменную `ZEPTO_WRITABLE_BUCKETS`. Значение зависит от конфигурации, его необходимо запросить у сотрудников технической поддержки платформы VK WorkSpace. Переменная необходима для восстановления почтовых ящиков, в которых есть письма с вложениями большого размера.

5. Откройте экран со списком машин, перейдя по ссылке **К списку машин**.

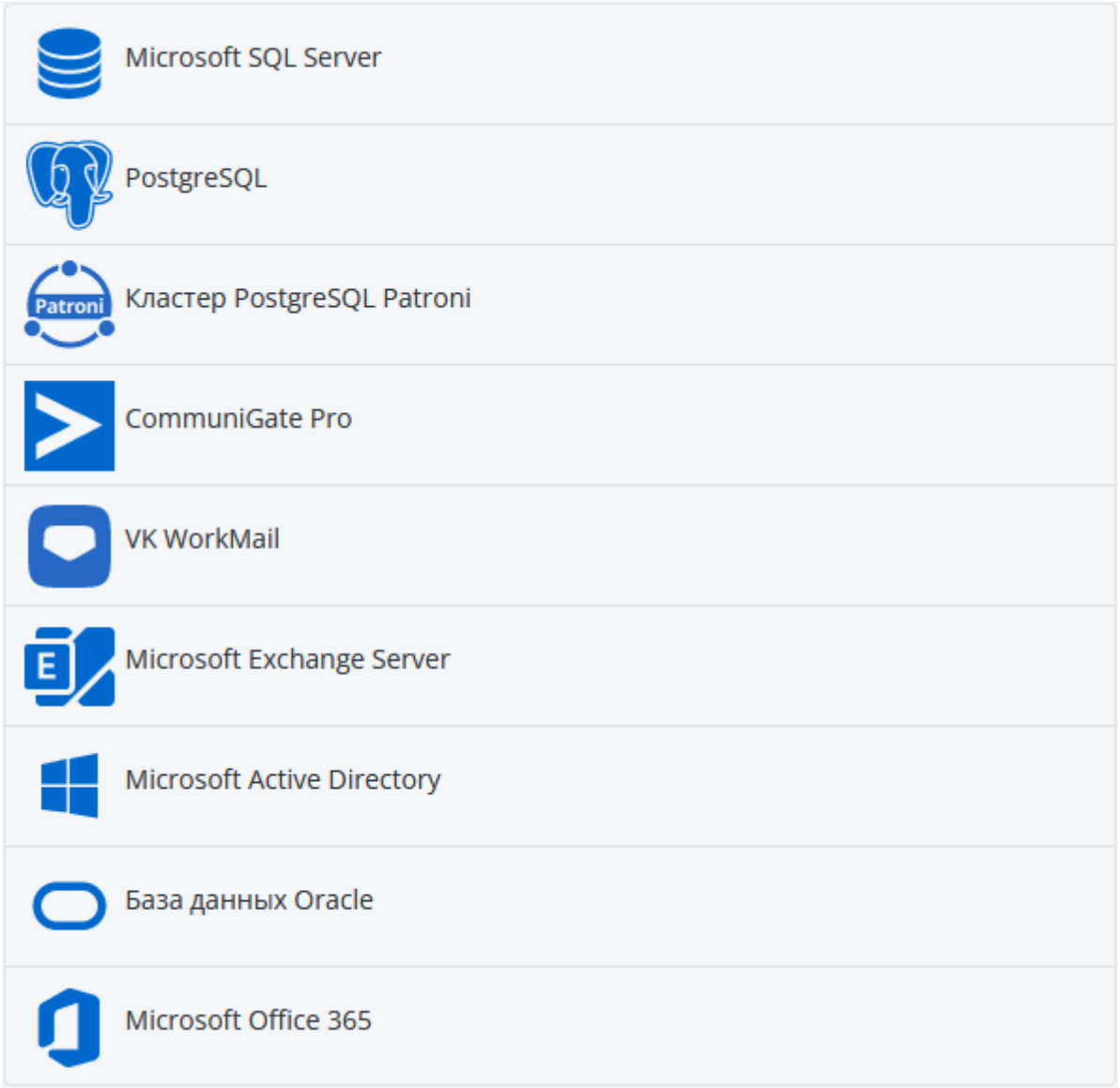


6. Примените изменения для обоих типов контейнеров, нажав на значок запуска .



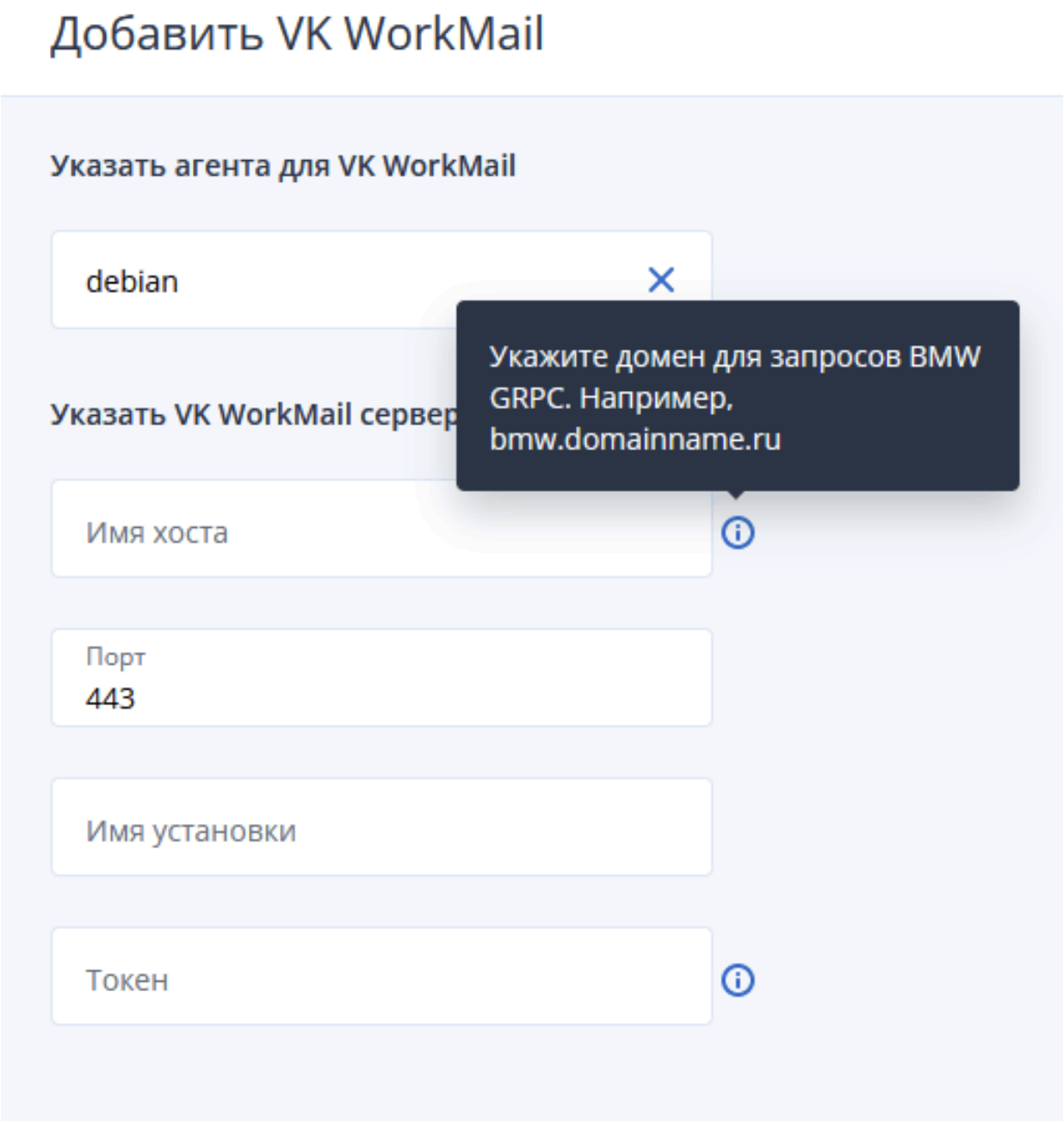
Добавление хоста VK WorkMail

1. В веб-консоли перейдите на вкладку **Устройства** главного меню слева и нажмите в правом верхнем углу **Добавить**.
2. В окне добавления нового устройства щёлкните **VK WorkMail**.



3. Заполните поля:
   - в поле **Указать агента для VK WorkMail** выберите из списка имя компьютера, на котором установлен агент или начните вводить имя для поиска;
   - в поле **Указать VK WorkMail сервер** укажите домен для запросов BMW GRPC, например, `bmw.domainname.ru`;
   - в поле **Порт** укажите номер порта;

- в поле **Имя установки** укажите имя текущей установки;
- в поле **Токен** укажите токен, выданный вам администратором. Получение токенов описано в документации VK WorkMail.



4. По окончании ввода данных нажмите **Добавить**.

Резервное копирование VK WorkMail и VK WorkDisk

Глобальная адресная книга VK WorkMail определяется в Кибер Бэкап как дополнительный пользователь с именем "`адресная книга name@domain`". Резервное копирование глобальных адресных книг VK WorkMail происходит аналогично резервному копированию данных пользователей VK WorkMail.

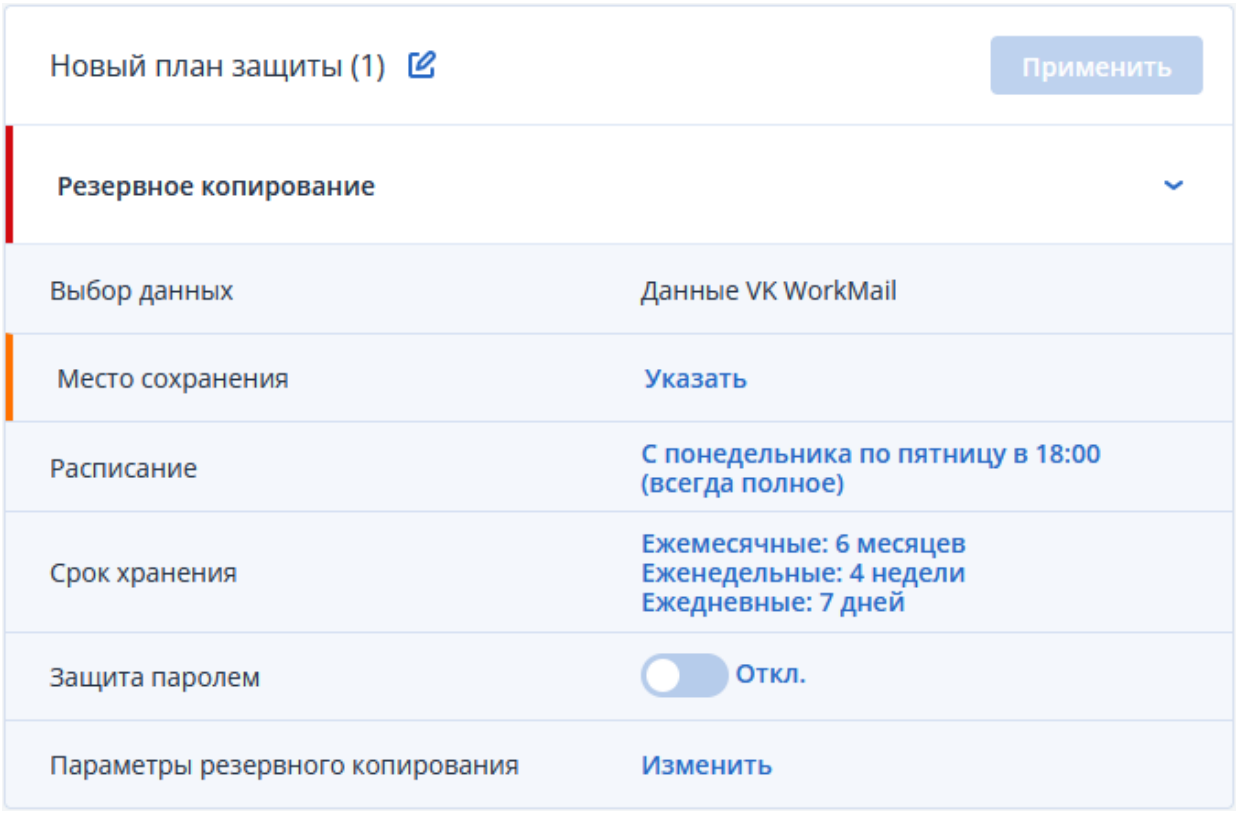
Резервное копирование данных пользователей VK WorkMail

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** → **VK WorkMail**.
2. Выберите из списка обнаруженных ресурсов VK WorkMail пользователя, для которого вы хотите создать защиту, и щёлкните по строке, в которой находится имя этого пользователя.

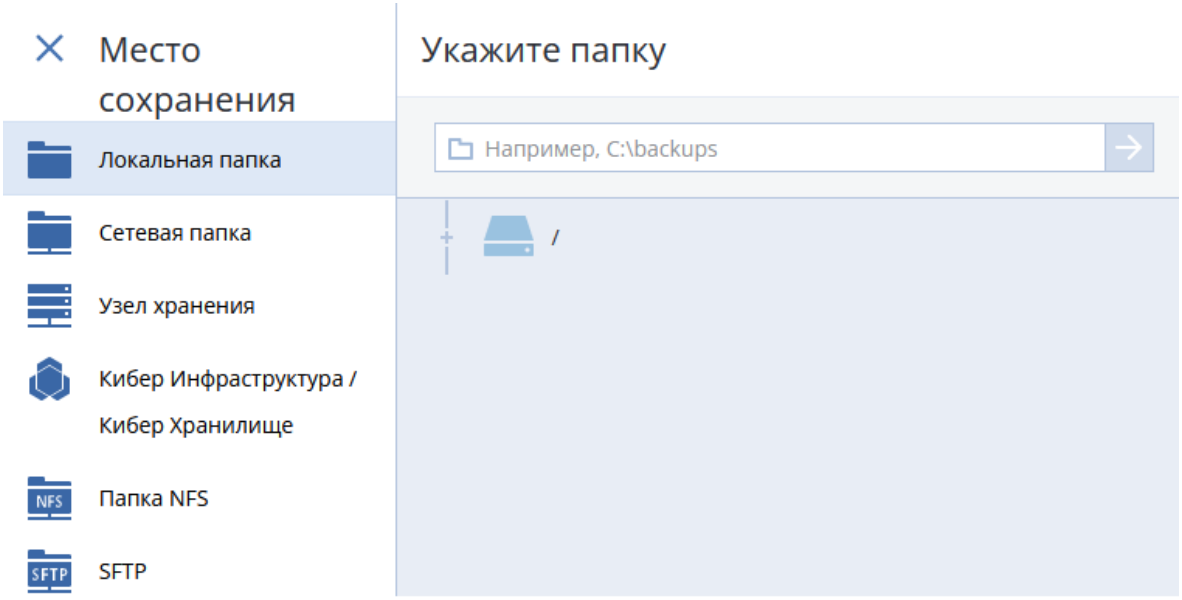
   > **Примечание**
   >
   > Для резервного копирования глобальной адресной книги VK WorkMail выберите пользователя с именем "`адресная книга name@domain`".

3. Перейдите на вкладку справа **Защитить** для защиты почтового ящика или группы почтовых ящиков (домена).



4. Заполните данные в окне создания плана защиты:

- В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения (в том числе на ленты), Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

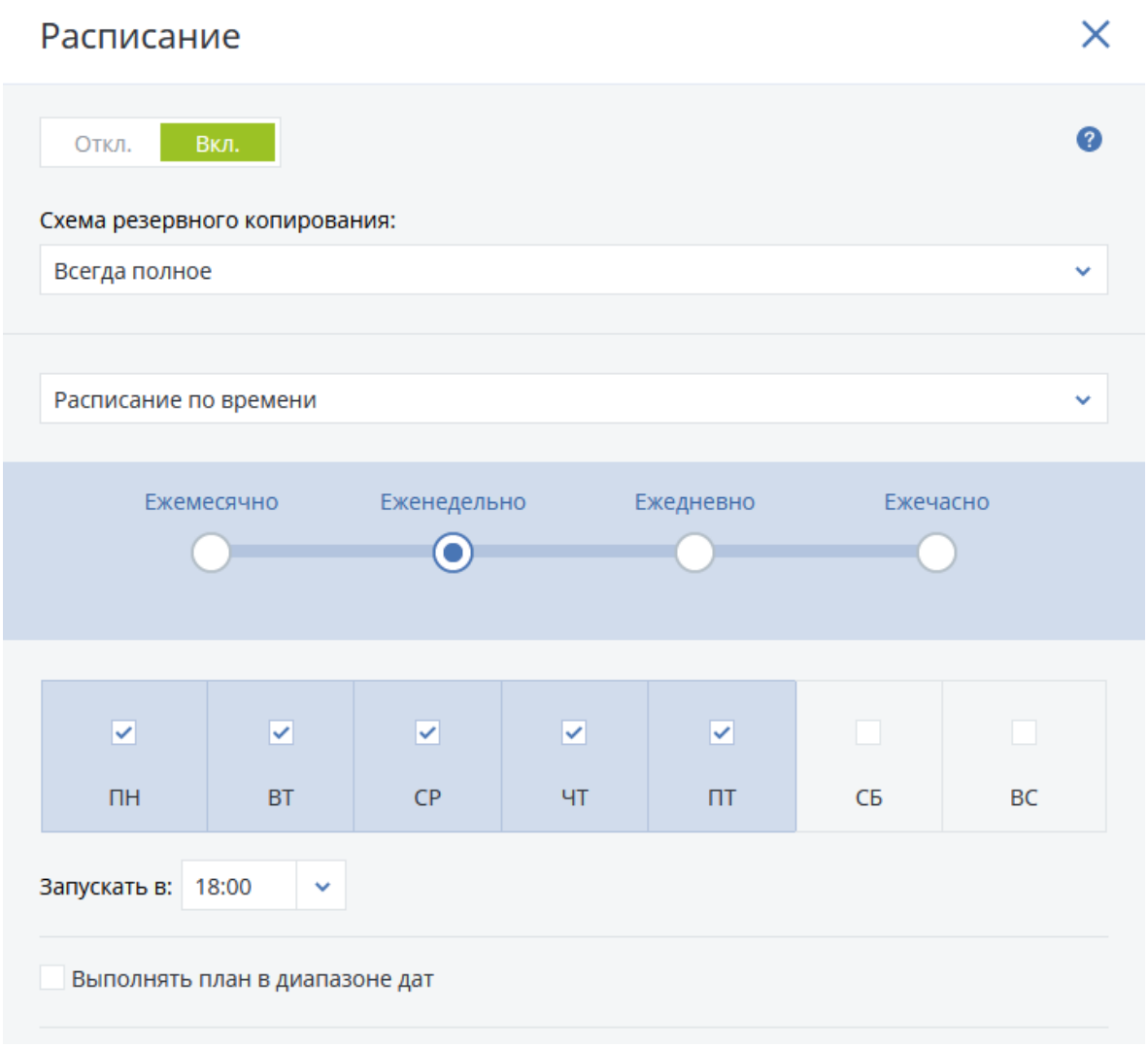


Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

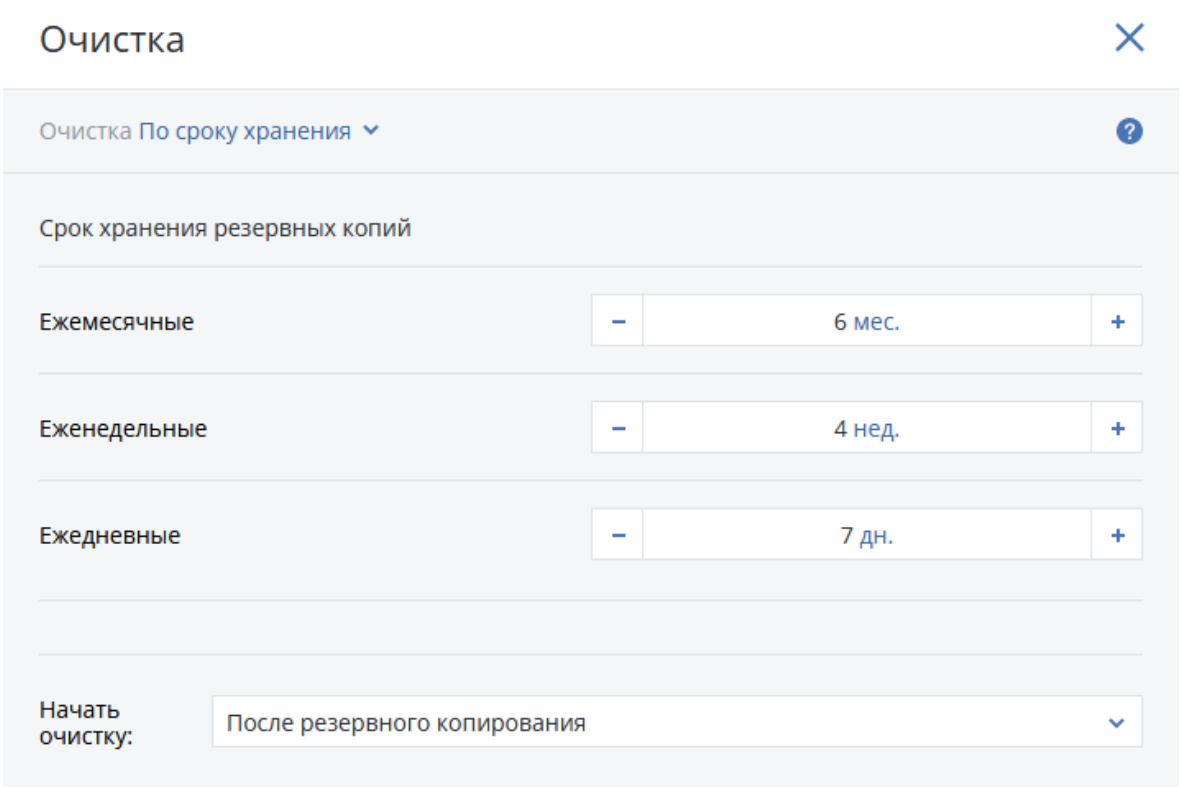
Важно

Для резервного копирования на ленты через узел хранения выполните шаги из раздела *Особенности резервного копирования на ленты*.

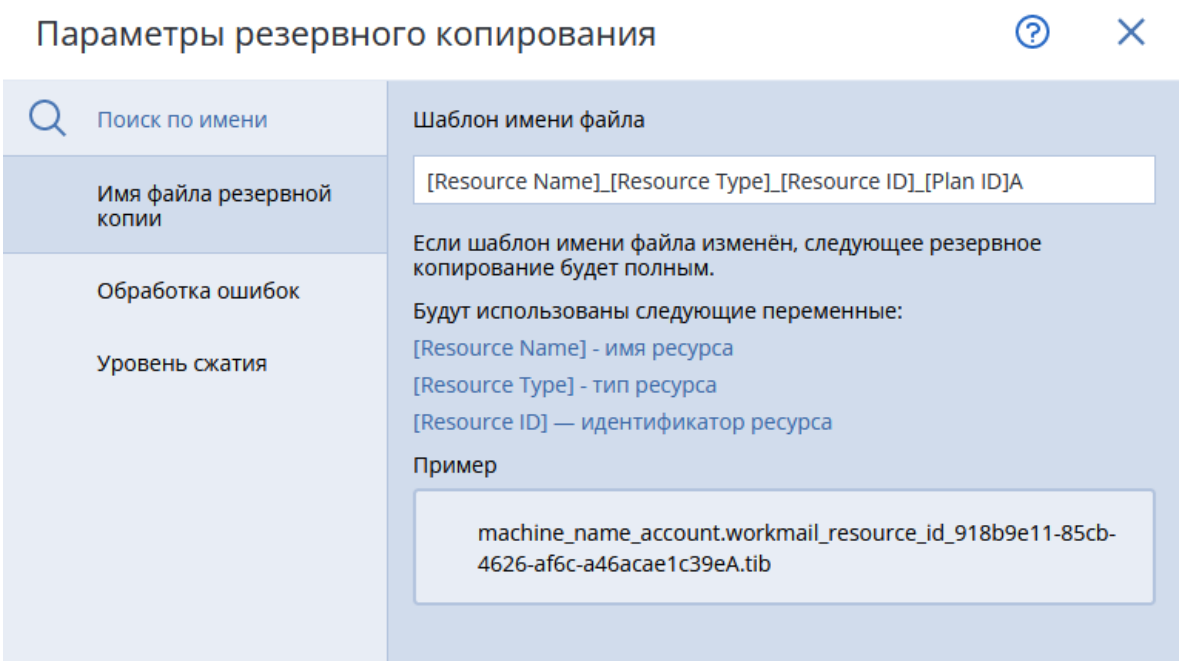
- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.



- [Необязательно] В поле **Параметры резервного копирования** укажите параметры обработки ошибок и уровень сжатия резервных копий.



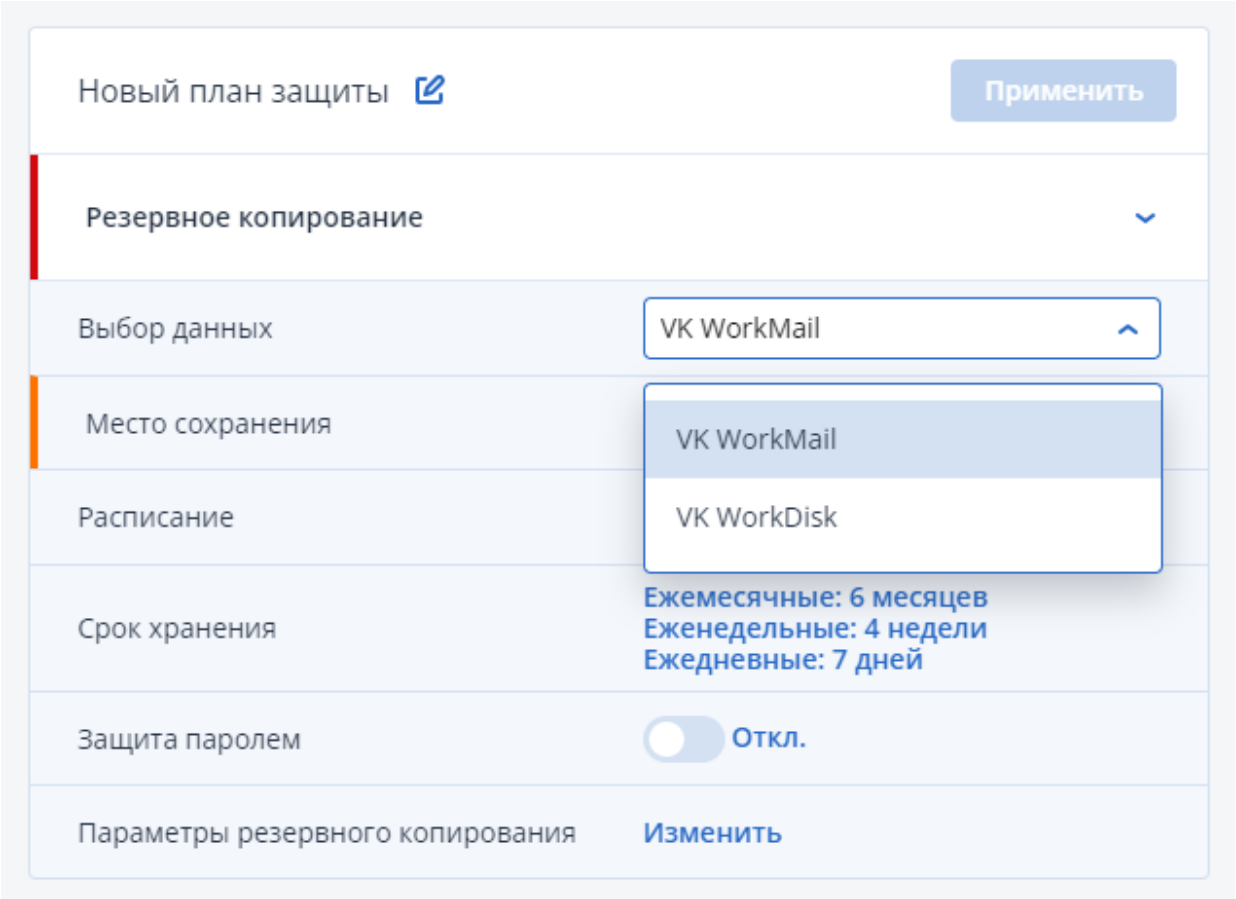
5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к выбранным доменам или почтовым ящикам.

См. также информацию в разделе *План защиты и модули*.

Резервное копирование данных пользователей VK WorkDisk

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** → **VK WorkMail**.
2. Выберите из списка пользователя, данные которого вы хотите защитить, и щёлкните по строке, в которой находится имя этого пользователя.
3. Перейдите на вкладку справа **Защитить** для защиты данных VK WorkDisk.



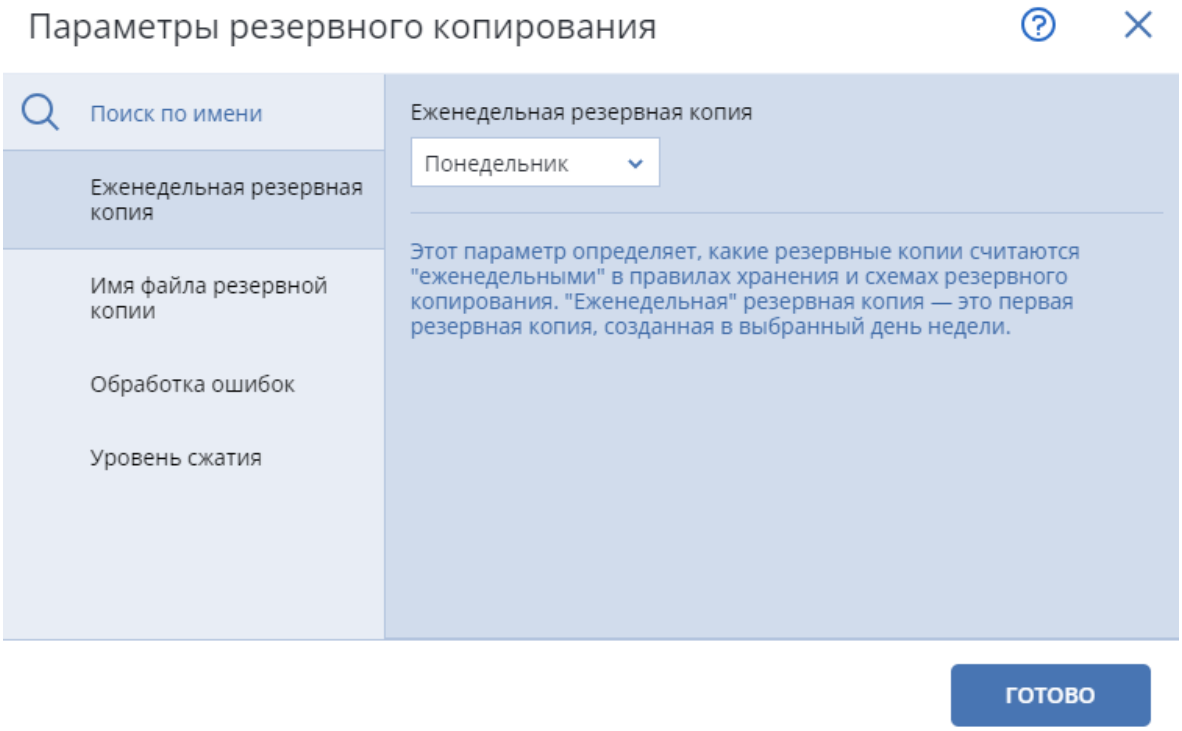
4. Заполните данные в окне создания плана защиты:
   - В поле **Выбор данных** выберите **VK WorkDisk**.
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения (в том числе на ленты), Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

     Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

Важно

Для резервного копирования на ленты через узел хранения выполните шаги из раздела *Особенности резервного копирования на ленты*.

- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.
- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
- [Необязательно] В поле **Параметры резервного копирования** укажите день недели для создания еженедельной копии, параметры обработки ошибок и уровень сжатия резервных копий.



5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к данным VK WorkMail выбранного пользователя.

См. также информацию в разделе *План защиты и модули*.

Резервное копирование больших объемов данных

При резервном копировании большого количества почтовых ящиков (до 60 000) рекомендуется соблюдать следующие условия:

- Иметь особую лицензию для резервного копирования больших объемов данных.
- Установить сервер управления на машину с ОС Linux, использующую СУБД PostgreSQL (см.

раздел *Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL*).

- Производить резервное копирование с помощью *Группы устройств*. В каждой группе должно быть не более 2 000 почтовых ящиков.
- Использовать для хранения резервных копий Кибер Инфраструктуру. Кроме того, при количестве резервных копий до 150 000, можно использовать сетевую папку.
- Использовать один агент VK WorkMail не более чем для 12 000 почтовых ящиков. Для увеличения производительности можно использовать до десяти агентов для каждого хоста VK WorkMail.

Использование нескольких агентов для одновременного резервного копирования данных

Для резервного копирования более 6 000 почтовых ящиков можно использовать сразу несколько агентов. Для этого выполните следующие действия:

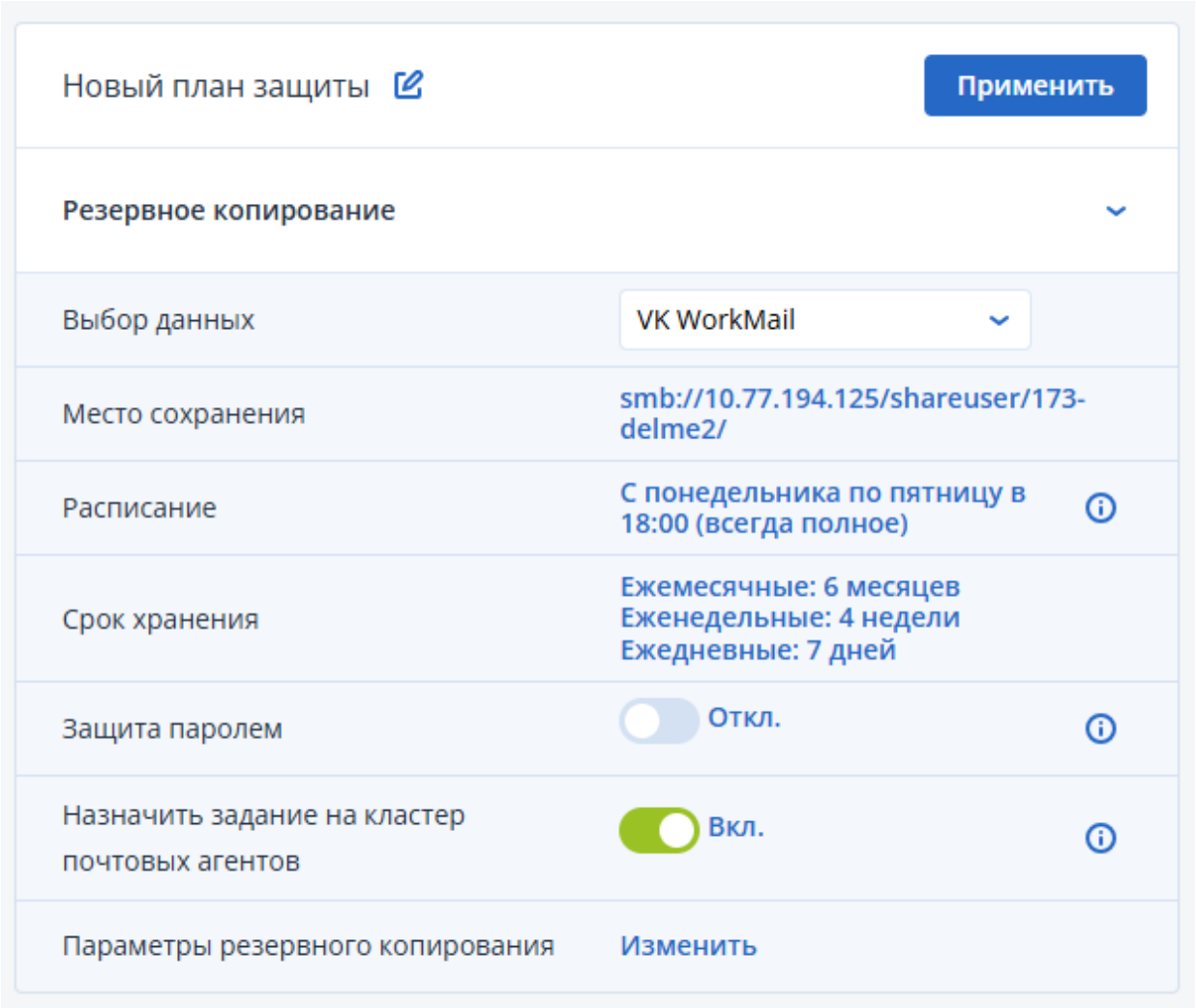
1. Зарегистрируйте необходимое количество агентов VK WorkMail (см. раздел *Установка VK WorkMail*). Агенты должны быть версии 17.3 или новее.

   Для задействования в резервном копировании всех агентов достаточно добавить хост VK WorkMail только для одного из агентов.

2. Создайте план резервного копирования для агентов. В резервном копировании будут участвовать все агенты VK WorkMail, зарегистрированные в Кибер Бэкап.

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** → **VK WorkMail**.
2. Выберите ресурсы VK WorkMail или VK WorkDisk, для которых вы хотите создать план защиты.
3. На вкладке справа нажмите **Защитить** или **Защитить группу**, если выбрана группа почтовых ресурсов.



4. Введите данные в окне создания плана защиты:

   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: сетевая папка, узел хранения (в том числе на ленты), Кибер Инфраструктура / Кибер Хранилище, SFTP, папка NFS (только для Linux).

     Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

   - В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.
   - В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
   - В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным агентам.
   - [Необязательно] В поле **Параметры резервного копирования** укажите метод разбиения резервных копий на меньшие по размеру фрагменты, параметры обработки ошибок и уровень

сжатия резервных копий.

5. По окончании настройки плана нажмите **Применить**.

При резервном копировании несколькими агентами балансировка нагрузки происходит в режиме циклического перебора (round robin).

Резервное копирование серверов VK WorkMail и VK WorkDisk

Резервное копирование сервера VK WorkDisk происходит автоматически при резервном копировании сервера VK WorkMail, к которому подключен сервер VK WorkDisk.

Для резервного копирования сервера VK WorkMail на нем должен быть установлен агент для Linux.

Для создания плана защиты сервера VK WorkMail выполните действия по аналогии со следующим примером.

Предварительные действия

1. Загрузите скрипт.
2. Загрузите файлы программы.
3. Прочитайте инструкцию.

> **Примечание**
>
> Компания Киберпротект предоставляет протестированную на совместимость версию программы VK WorkMail. Для установки последней версии программы обратитесь к официальному разработчику.

Резервное копирование

Настройте план резервного копирования в соответствии с инструкцией, как описано далее.

1. Скопируйте в директорию, например в `/tmp`, файлы программы: `mnt-backup` и `tars`.
2. Задайте права на выполнение:

   ```
   chmod +x /tmp/mnt-backup
   ```

3. В скрипте `pre-command.sh` укажите необходимые пути:

   ```
   script_dir=/tmp
   main_dir=/home/backup1
   ```

   здесь `script_dir` — путь к `mnt-backup`, `main_dir` — путь, куда будут сохраняться базы данных.

4. Запустите скрипт вручную до создания плана защиты, чтобы получить пути, которые нужно защитить и которые необходимо добавить в исключения (exclude) задачи резервного копирования:

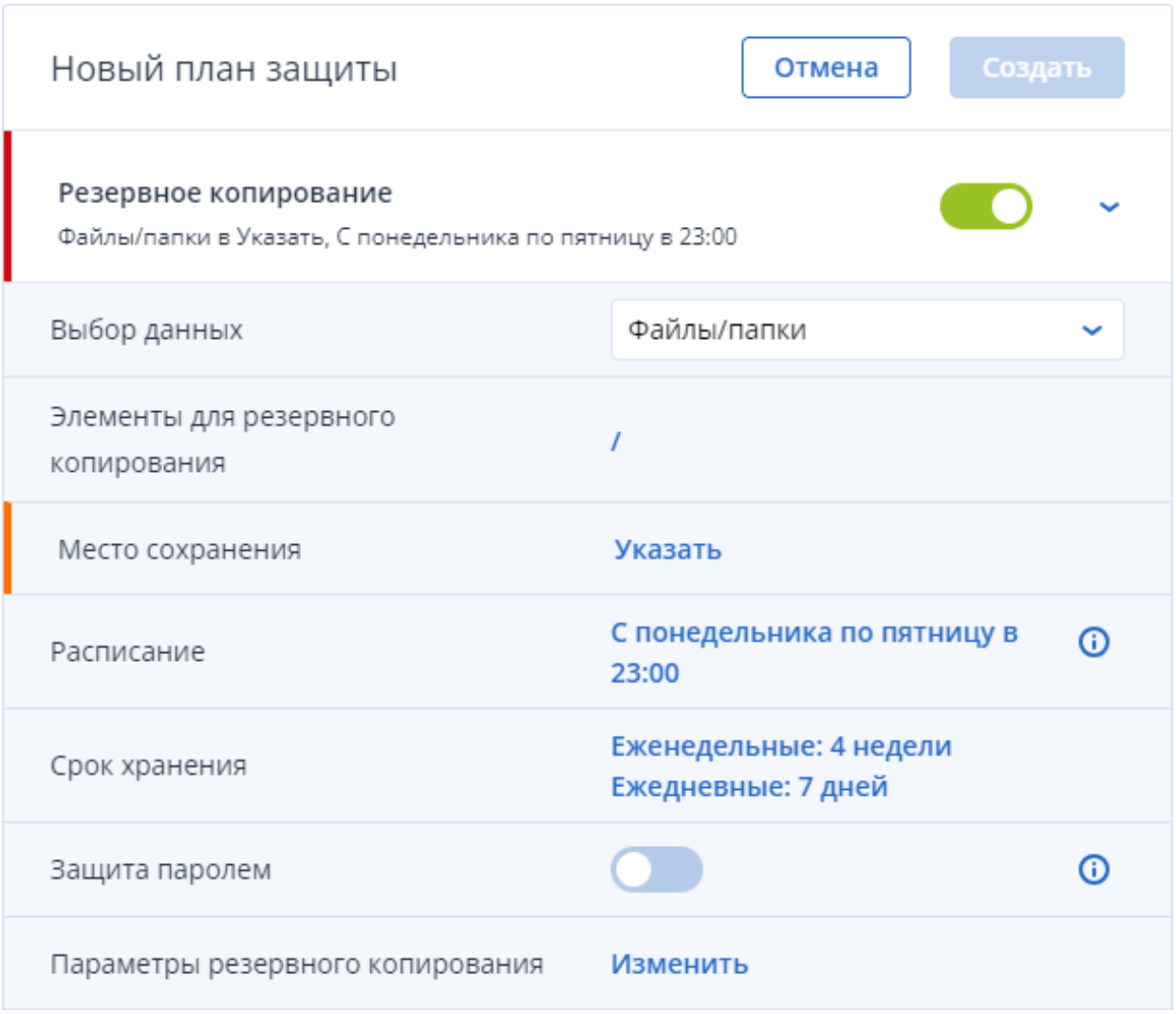
   ```
   chmod +x pre-command.sh
   ./pre-command.sh
   ```

   В результате в папке `/home/backup1/latest` появятся файлы:

   - `pathToStore.txt` — содержит пути, которые нужно защитить,
   - `pathToExclude.txt` — содержит абсолютные пути, которые нужно добавить в исключения задачи резервного копирования,
   - `README.txt` — содержит результат запуска скриптов.

   Для формирования пути используется `/opt/mailOnPremise`, а также те части, которые находятся в файле.

5. Перейдите в веб-консоли: **Устройства** → **Физические и виртуальные машины**.
6. Выберите из списка сервер VK WorkMail, который вы хотите защитить, и щёлкните по строке, в которой находится это устройство.
7. Перейдите на вкладку справа **Защитить**.



8. В поле **Выбор данных** выберите **Файлы/папки**.
9. В поле **Элементы для резервного копирования** выберите **С помощью правил политики**.
10. В поле **Добавить правило** поочередно укажите корневые директории тех путей, которые находятся в файле `pathToStore.txt`, например:

```
/var
/etc
/opt
/home
```

или просто поставьте знак корня

```
/
```

11. Нажмите **ОК**.

12. Перейдите в **Параметры резервного копирования → Фильтры файлов → Выполнять резервное копирование только файлов, соответствующих следующим критериям**.
13. Укажите пути по маске со звездочкой (*) из файла `pathToStore.txt`:

```
/var/lib/docker/*
/home/deployer/*
/opt/mailOnPremise/
/etc/systemd/system/onpremise-*
/etc/systemd/system/deployer.service
/home/backup1/latest/*
```

14. Перейдите в **Параметры резервного копирования → Фильтры файлов → Не выполнять резервное копирование файлов, соответствующих следующим критериям**.
15. Добавьте абсолютные пути из файла `pathToExclude.txt`:

```
/opt/mailOnPremise/dockerVolumes/ussug1/tarantool
/opt/mailOnPremise/dockerVolumes/evdokia-tar1/tarantool
/opt/mailOnPremise/dockerVolumes/filters-tar1/tarantool
/opt/mailOnPremise/dockerVolumes/abookpdd-tar1/tarantool
/opt/mailOnPremise/dockerVolumes/mstatqueue-tar1/tarantool
/opt/mailOnPremise/dockerVolumes/search-reindex-queue1/tarantool
/opt/mailOnPremise/dockerVolumes/cldudb-proxy1/tarantool
/opt/mailOnPremise/dockerVolumes/autoreplylimiter1/tarantool
/opt/mailOnPremise/dockerVolumes/stpath-tar1/tarantool
/opt/mailOnPremise/dockerVolumes/attfiledb1/tarantool
...
```

16. Перейдите в **Параметры резервного копирования → Команды до или после → Выполнение команды до резервного копирования** и включите переключатель: **Да**.
17. В поле **Команда или путь к файлу пакета на машине с агентом** вставьте:

```
./pre-command.sh
```

18. В поле **Рабочий каталог** вставьте путь, где лежит скрипт pre-command.sh, например:

```
/tmp
```

19. Нажмите **Готово**.

Важно

Поскольку вы используете команды ”до или после”, убедитесь, что код возврата скрипта от VK возвращает корректное значение. В противном случае, возможна неверная интерпретация результатов резервного копирования.

Особенности резервного копирования VK WorkMail и VK WorkDisk на ленты

Функциональность autoinventory

Перед резервным копированием на ленты через узел хранения необходимо отключить функционал `autoinventory` в файле `tape_devices.xml`:

```
<autoinventory>
  <enabled value=”0”/>
</autoinventory>
```

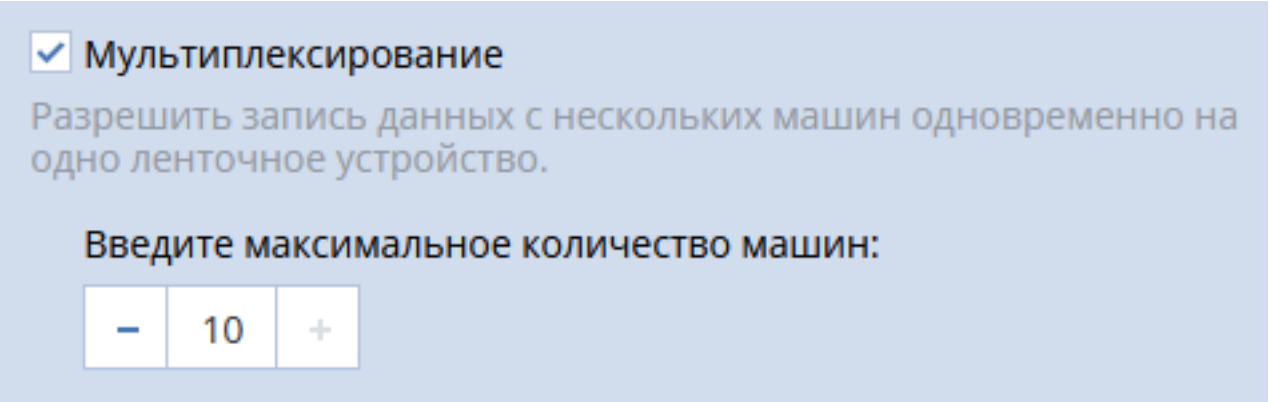
и перезапустить службу узла хранения.

- В ОС Windows отредактируйте файл `C:\ProgramData\Acronis\BackupAndRecovery\ARSM\Configuration\tape_devices.xml`. Затем перезапустите службу **Cyberprotect Storage Node Service** в приложении **Службы**.
- В ОС Linux отредактируйте файл `/var/lib/Acronis/BackupAndRecovery/ARSM/Configuration/tape_devices.xml`. Затем выполните команду

  ```
  systemctl restart acronis_storageserver
  ```

Мультиплексирование

Мультиплексирование должно быть включено. Максимальное количество машин должно быть не менее 10. Подробнее о мультиплексировании см. в разделе *Управление лентами*.



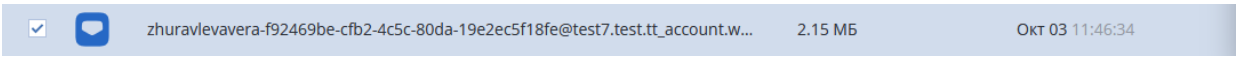
Восстановление VK WorkMail и VK WorkDisk

Восстановление глобальных адресных книг VK WorkMail происходит аналогично восстановлению данных пользователей VK WorkMail.

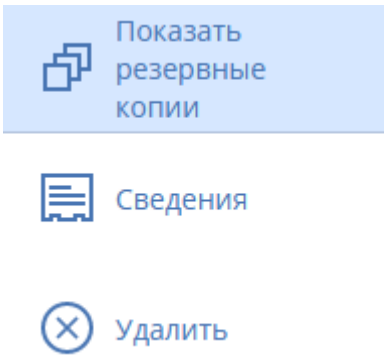
Восстановление данных пользователей VK WorkMail

Чтобы восстановить данные пользователей VK WorkMail, выполните следующие действия:

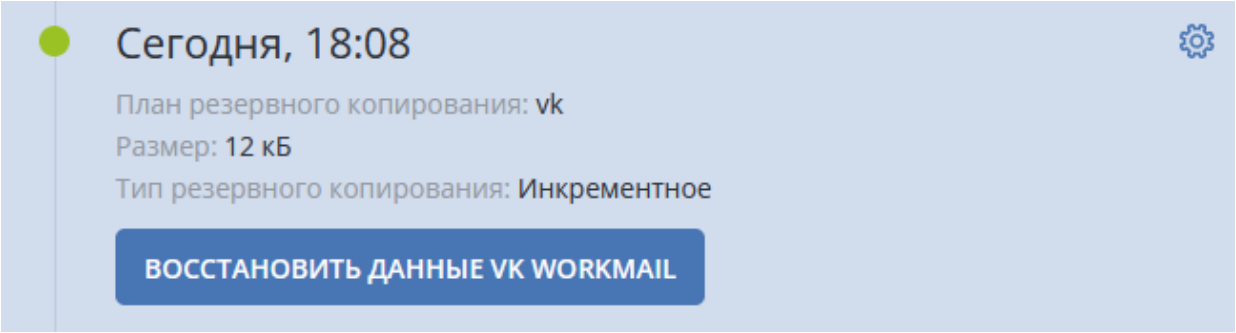
1. Перейдите в **Хранилища резервных копий** в главном меню слева.
2. Выберите в списке нужную резервную копию.



3. Выберите справа **Показать резервные копии**.

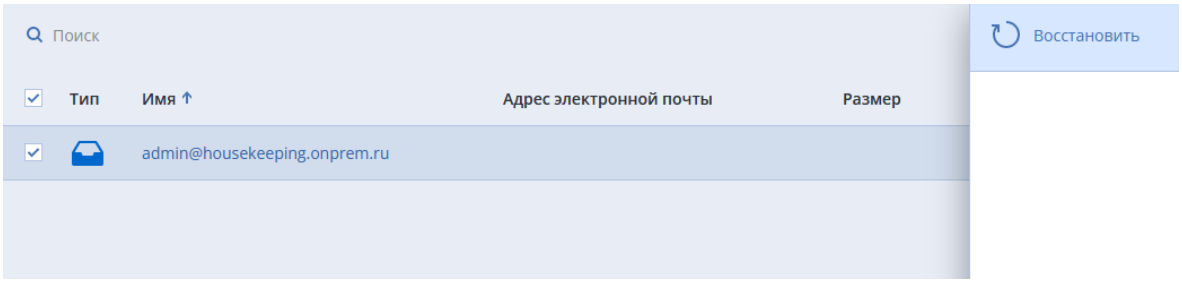


4. Нажмите **Восстановить данные VK WorkMail**.

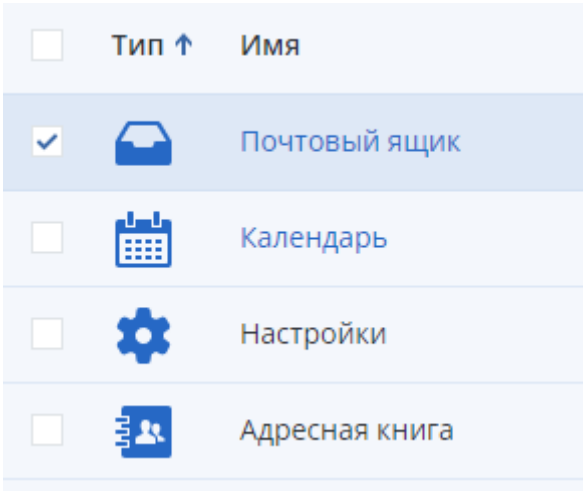


5. Выберите данные для восстановления:

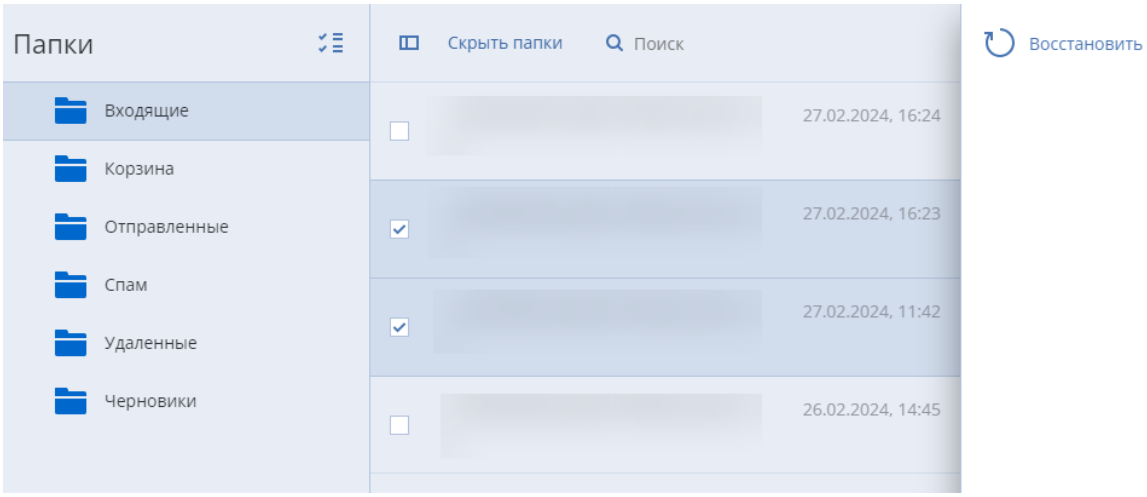
   - Если необходимо восстановить весь почтовый ящик, отметьте галочкой в списке имя почтового ящика, затем выберите справа **Восстановить**.



   - Если необходимо восстановить отдельные ресурсы пользователя, нажмите на имя резервной копии. Можно выбрать только один тип ресурса для восстановления. Выберите ресурс и нажмите справа **Восстановить**.



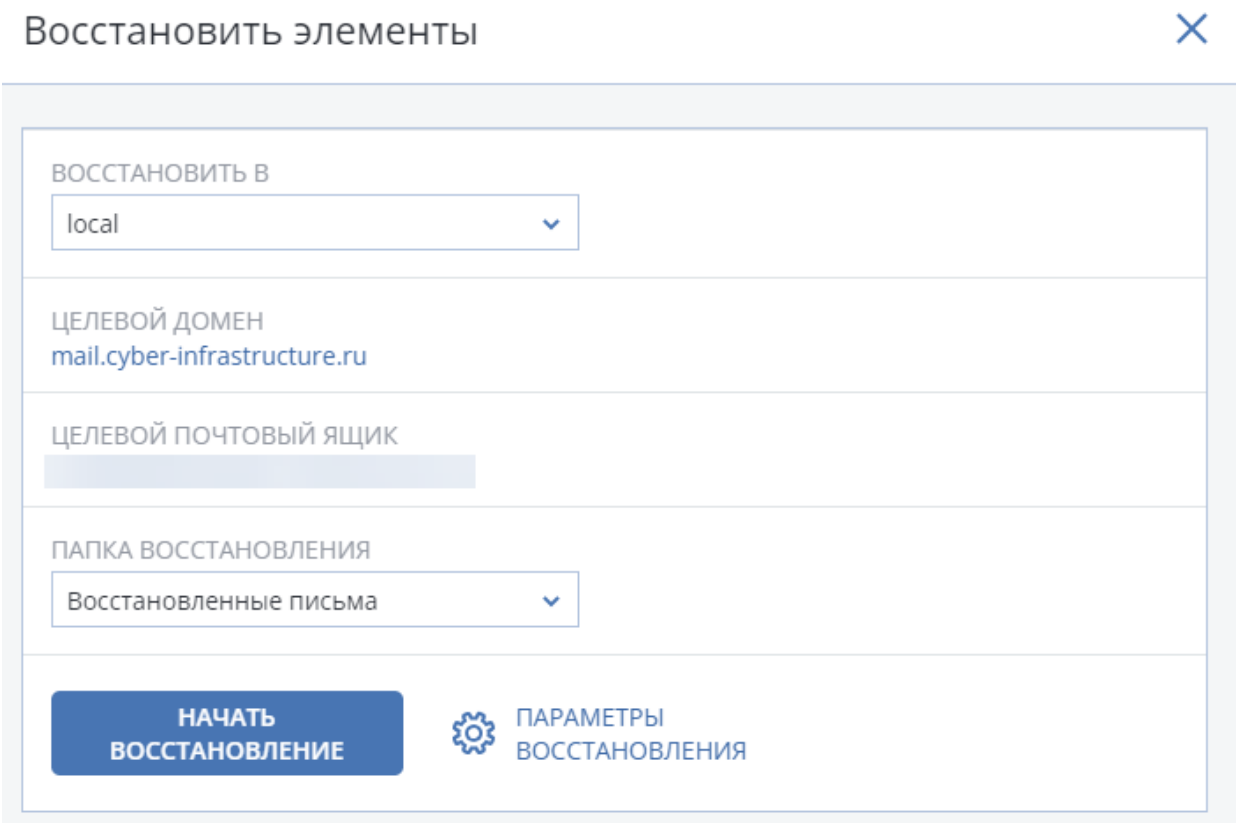
   - Если необходимо восстановить отдельные письма или события календаря, нажмите на **Почтовый ящик** или **Календарь** и выберите данные, затем нажмите справа **Восстановить**.



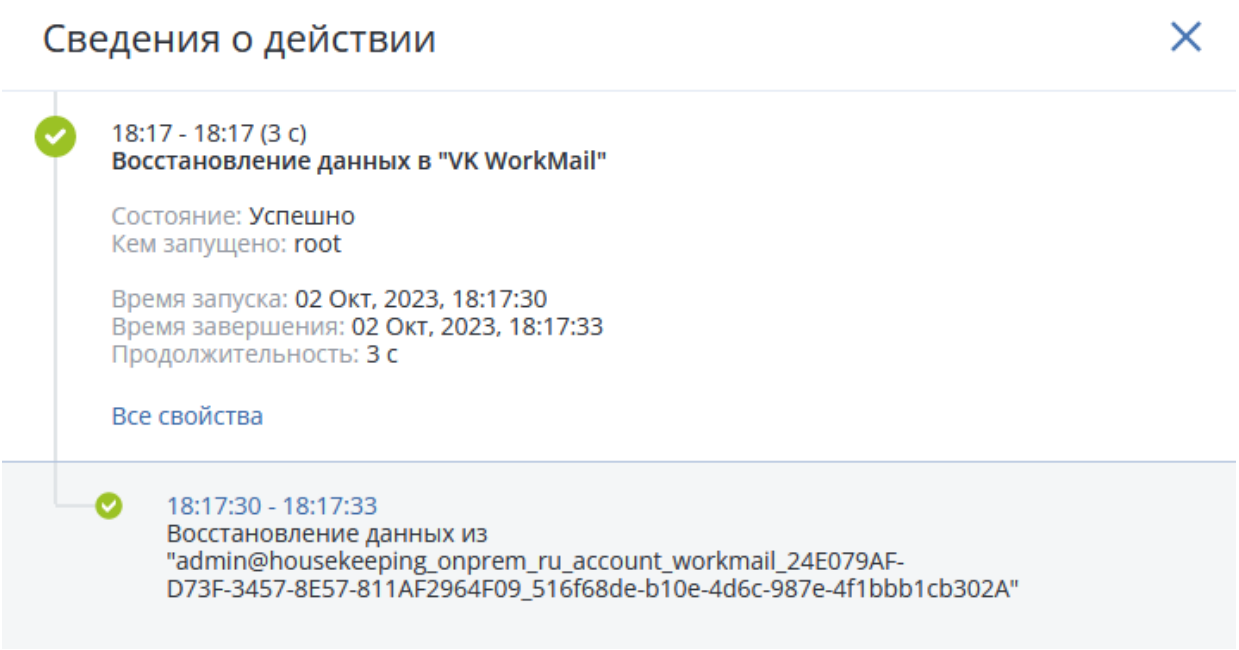
6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Укажите место восстановления.

> **Примечание**
>
> При восстановлении только профиля пользователя невозможно выбрать пользователя, отличного от оригинального.
>
> При восстановлении полного аккаунта пользователя в другого пользователя восстановление профиля будет пропускаться. Остальные данные будут восстановлены.

Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.



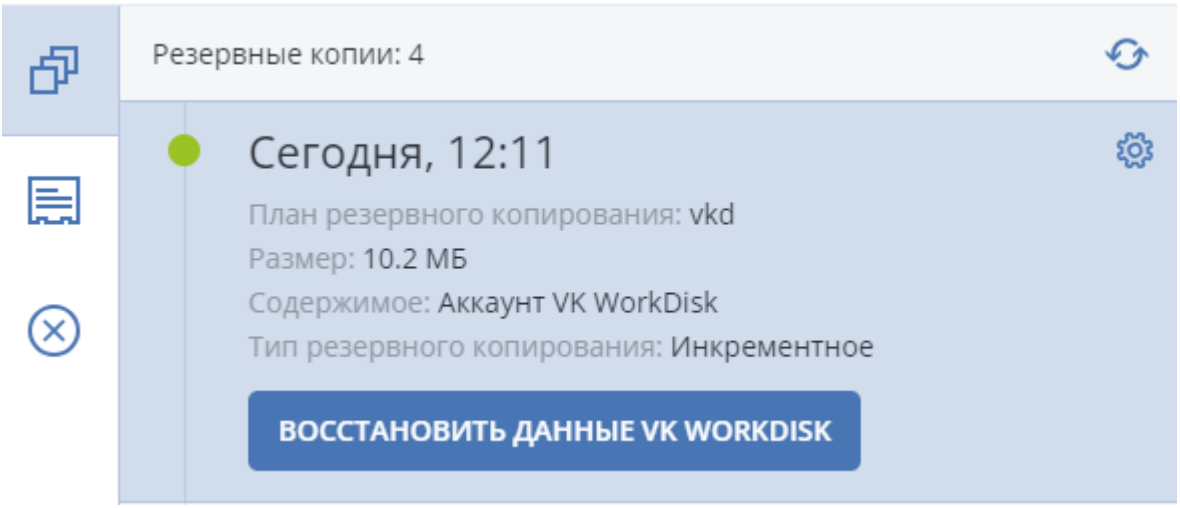
8. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.



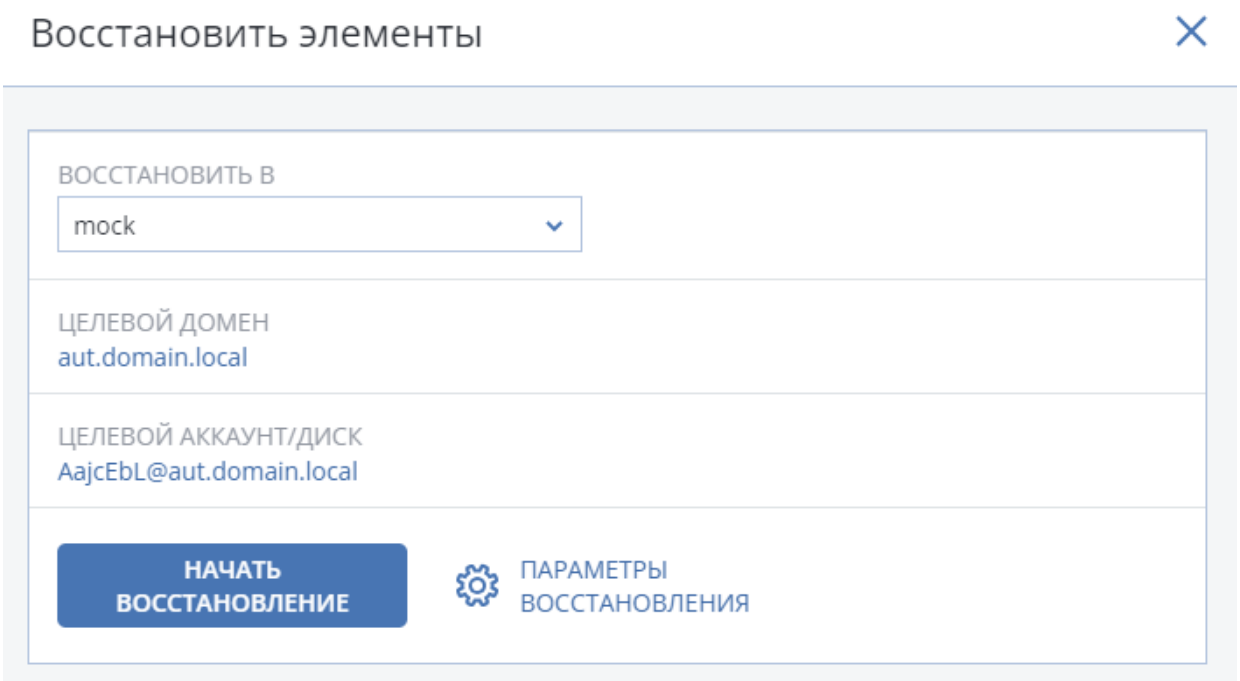
Восстановление данных пользователей VK WorkDisk

Чтобы восстановить данные пользователей VK WorkDisk, выполните следующие действия:

1. Перейдите в **Хранилища резервных копий** и выберите в списке нужную резервную копию.
2. Выберите справа **Показать резервные копии**.
3. Нажмите **Восстановить данные VK WorkDisk**.



4. Выберите данные для восстановления; затем выберите справа **Восстановить**.
5. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
6. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.

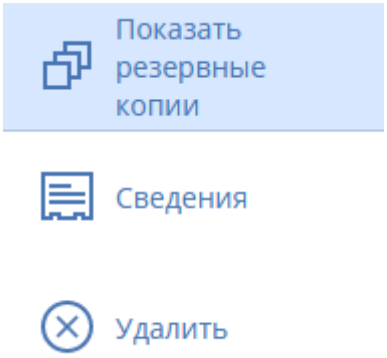


7. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

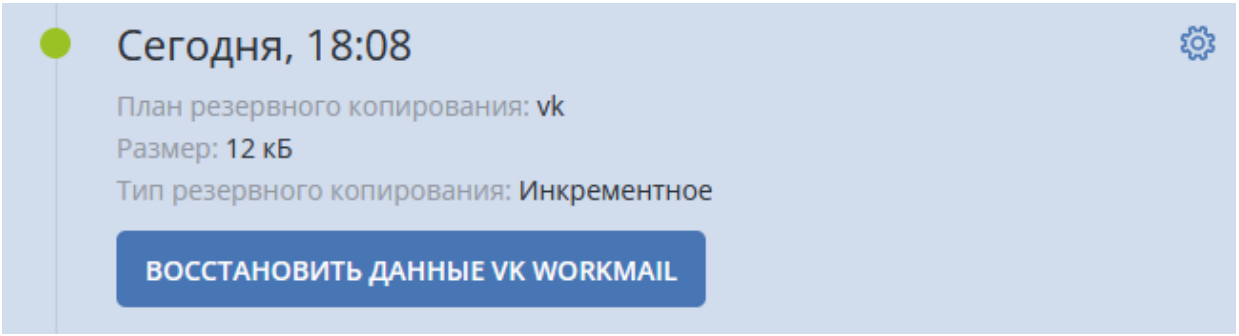
Просмотр писем VK WorkMail

Чтобы просмотреть письма пользователя VK WorkMail, выполните следующие действия:

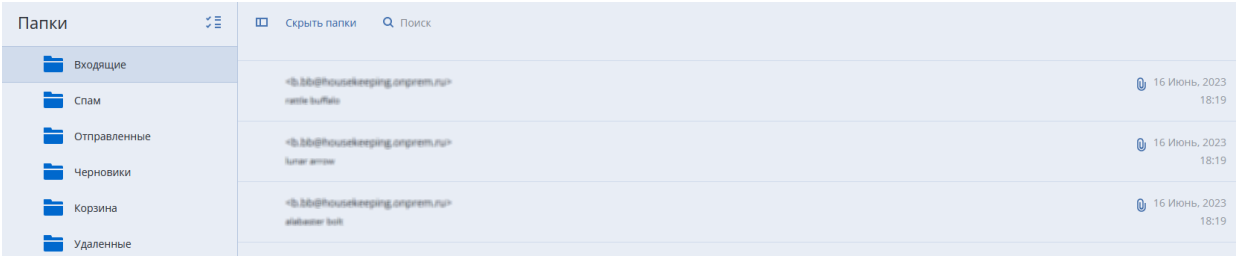
1. Перейдите в **Хранилища резервных копий** в главном меню слева.
2. Выберите нужное хранилище, щёлкните в списке нужную резервную копию.
3. Выберите справа **Показать резервные копии**.



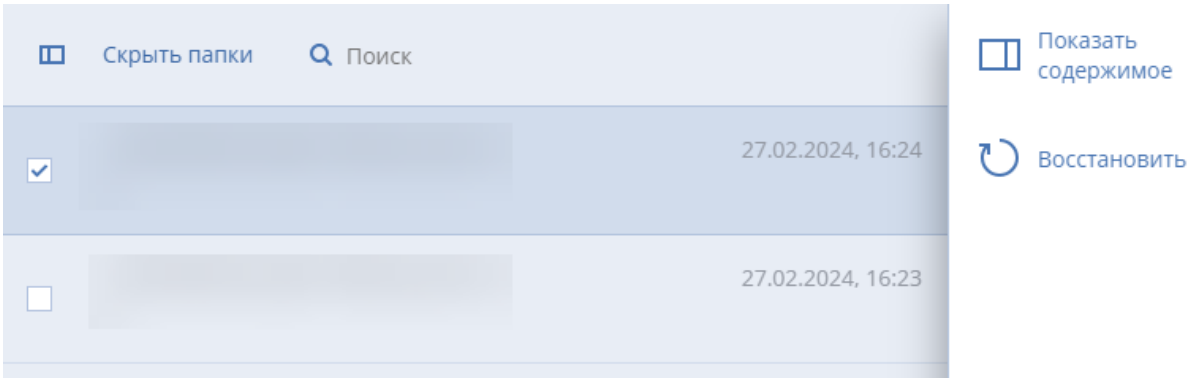
4. Щёлкните **Восстановить данные VK WorkMail**.



5. Нажмите имя пользователя в виде ссылки. Откроется список папок с письмами этого пользователя.



6. Выберите из списка нужное письмо, отметьте его галочкой.
7. Для просмотра содержимого письма нажмите справа **Показать содержимое**. Данная возможность недоступна для писем, хранящихся на лентах.



8. Для скачивания файла, приложенного к письму, щёлкните по нему.



Скачивание файлов из архива VK WorkDisk

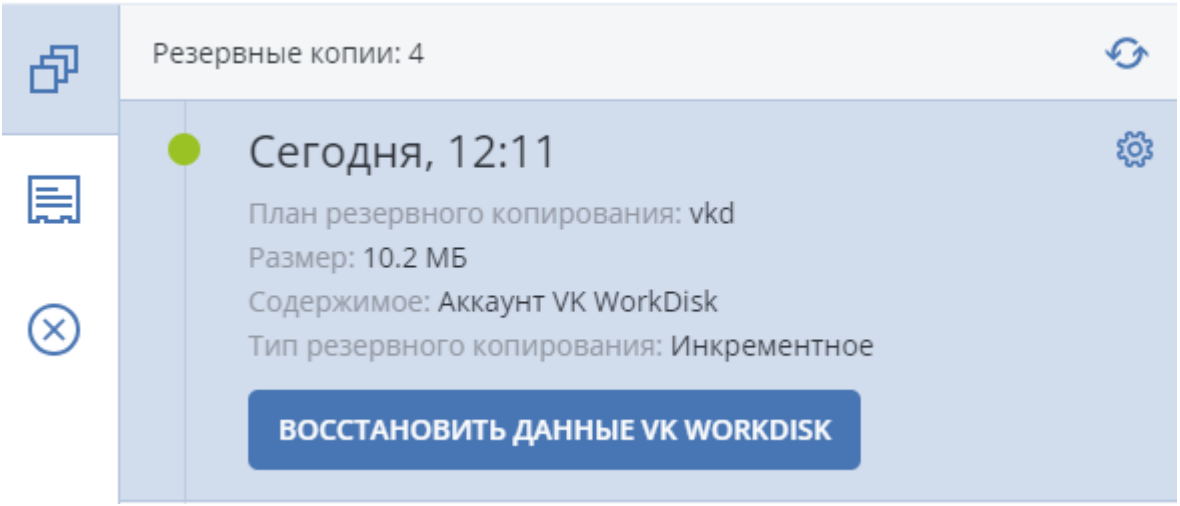
Перед скачиванием данных рекомендуется увеличить время ожидания до автоматического выхода по причине неактивности пользователя в настройках Кибер Бэкап. Для этого перейдите в **Настройки** → **Настройки системы** → **Безопасность** и либо уберите галочку **Завершить сеансы работы неактивных пользователей через**, либо установите время, которого точно хватит для скачивания данных.

Важно

Если во время скачивания файла произойдет автоматический выход пользователя из веб-консоли, файл придется скачивать заново.

Чтобы скачать файлы из архива VK WorkDisk, выполните следующие действия:

1. Перейдите в **Хранилища резервных копий**.
2. Выберите нужное хранилище, щёлкните в списке нужную резервную копию.
3. Выберите справа **Показать резервные копии**.
4. Нажмите **Восстановить данные VK WorkDisk**.



5. Нажмите имя пользователя в виде ссылки. Откроется список с данными пользователя.
6. Отметьте в списке нужные элементы галочкой. Количество выбранных элементов не должно превышать 150. Папка с файлами или диск целиком считаются за один элемент.
7. Для скачивания файлов нажмите **Загрузить**.

   Не выходите из окна просмотра архива и не переходите на другие точки восстановления до окончания скачивания данных. Чтобы воспользоваться другими функциями Кибер Бэкап, используйте новую вкладку браузера, иначе скачивание файла может быть прервано.

Примечание

Скачивание файлов из архива VK WorkDisk не поддерживается для резервных копий, расположенных на лентах.

Восстановление серверов VK WorkMail и VK WorkDisk

Восстановление данных на новую машину

Восстановление сервера VK WorkDisk происходит автоматически при восстановлении сервера VK WorkMail, к которому подключен сервер VK WorkDisk.

Для восстановления резервной копии сервера VK WorkMail, созданной по инструкции в разделе *Резервное копирование серверов VK WorkMail и VK WorkDisk*, выполните следующие действия:

1. Выключите исходную машину.
2. Для новой машины установите такой же IP-адрес, как для исходной.
3. Установите на новую машину агент Кибер Бэкап для Linux.
4. Восстановите данные в соответствующие директории, следуя шагам в разделе ”Восстановление

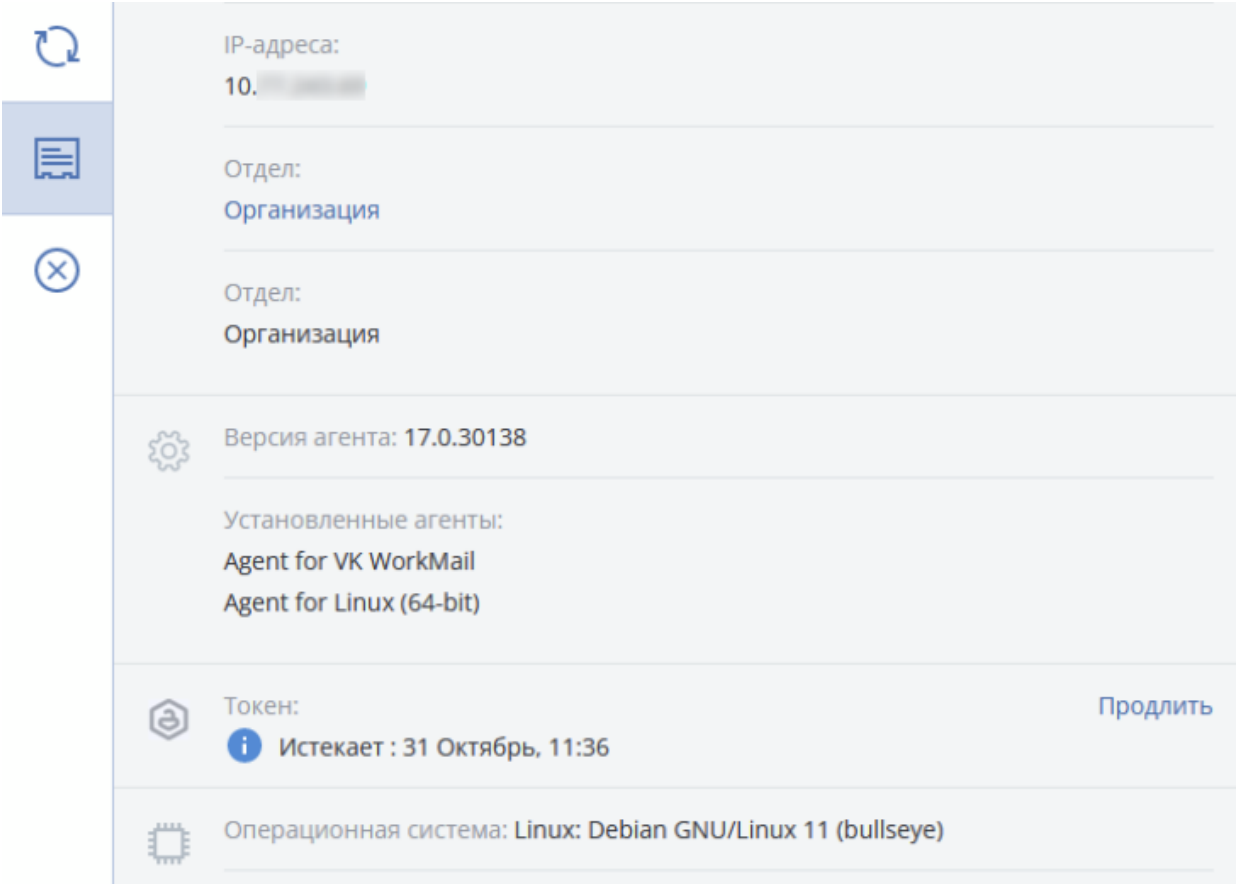
гипервизора” инструкции, предоставленной VK.

Обновление токена VK WorkMail

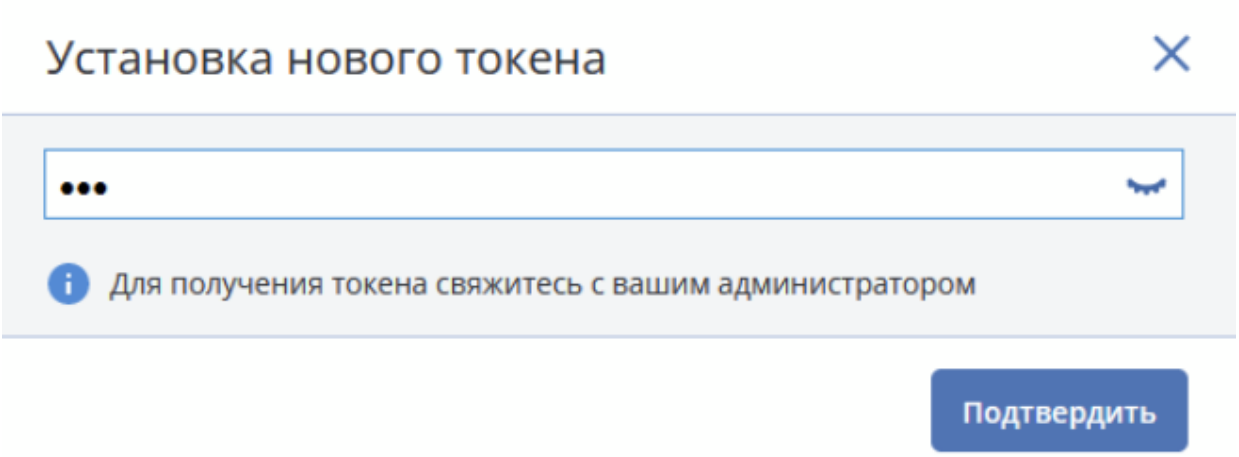
Для обнаружения, резервного копирования и восстановления данных устройства VK WorkMail Кибер Бэкап использует gRPC API, предоставляемый VK WorkMail, при обращениях к которому Кибер Бэкап передает токен для авторизации запросов. Токен обладает ограниченным сроком действия, поэтому его необходимо заблаговременно обновлять. Кибер Бэкап будет оповещать пользователей за месяц до истечения срока действия токена, а также при истечении этого срока.

Чтобы узнать дату окончания срока действия токена и обновить его при необходимости, выполните следующие шаги:

1. В веб-консоли перейдите на экран **Устройства** → **VK WorkMail** и выберите нужное устройство.
2. В правой панели перейдите на вкладку **Сведения**. В разделе **Токен** будет отображена дата окончания срока действия токена.



Если необходимо обновить токен, щёлкните **Продлить**, укажите новый токен и нажмите **Подтвердить**.



Защита Mailion

Mailion — почтовая система, ориентированная на крупные коммерческие и государственные организации.

Для резервного копирования данных Mailion понадобятся установленные и настроенные продукты:

- Кибер Бэкап 18.0 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе *Издания и лицензии Кибер Бэкап*).
- Почтовый сервис Mailion.

  Поддерживаемые версии Mailion указаны в разделе *Поддерживаемые почтовые сервисы*.

Для выполнения резервного копирования требуется установка агента Mailion.

Поддерживается установка агента для следующих операционных систем:

- Windows,
- Linux.

Полный список поддерживаемых операционных систем Windows и Linux см. в разделе *Поддерживаемые операционные системы*.

Возможности

Кибер Бэкап обеспечивает резервное копирование и восстановление:

- данных пользователя Mailion (электронные сообщения с форматированием и флагами, вложения, папки со структурой подпапок, настройки, календари и события календарей, контакты, задачи);
- тенанта Mailion (как группу пользователей);
- параметры общего доступа;

- почтовых ящиков ресурсов.

После выполнения резервного копирования в архиве можно посмотреть содержимое отдельных папок и писем, а также события и задачи в календаре.

Известные проблемы и ограничения

- Не поддерживается резервное копирование на ленты.
- Для восстановления структуры тенанта необходимо восстановить данные специального пользователя `Tenant Catalog`.
- Восстановить почтовый ящик пользователя можно только в пространство этого пользователя.
- Для восстановления данных пользователя на другой сервер Mailion надо предварительно восстановить на этот сервер тенант, в котором находится пользователь.

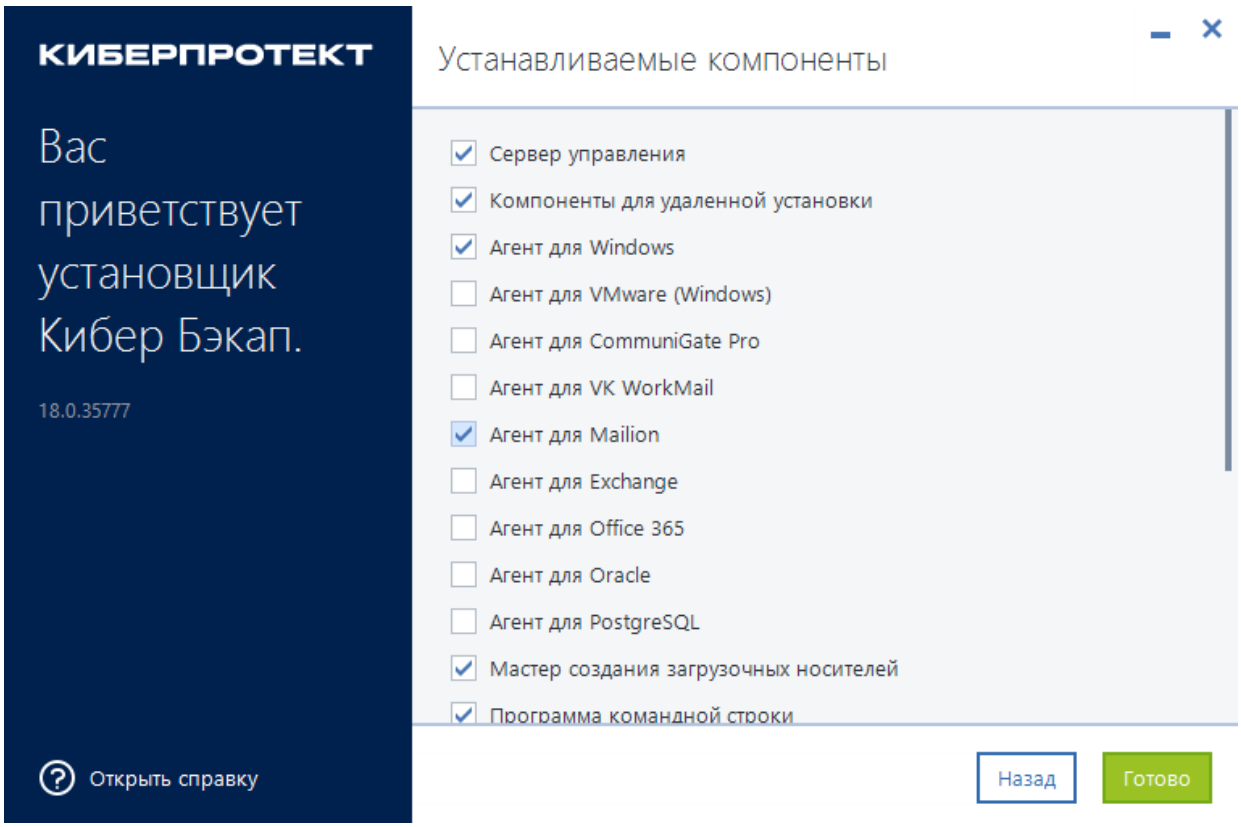
Установка Mailion

Установка Mailion включает в себя установку агента Кибер Бэкап и добавление хоста Mailion. Добавление хоста возможно лишь после установки агента.

Установка агента для Mailion

В этом разделе рассмотрена установка агента Кибер Бэкап для Windows. Для установки агента для Linux обратитесь к разделу *Установка в Linux*.

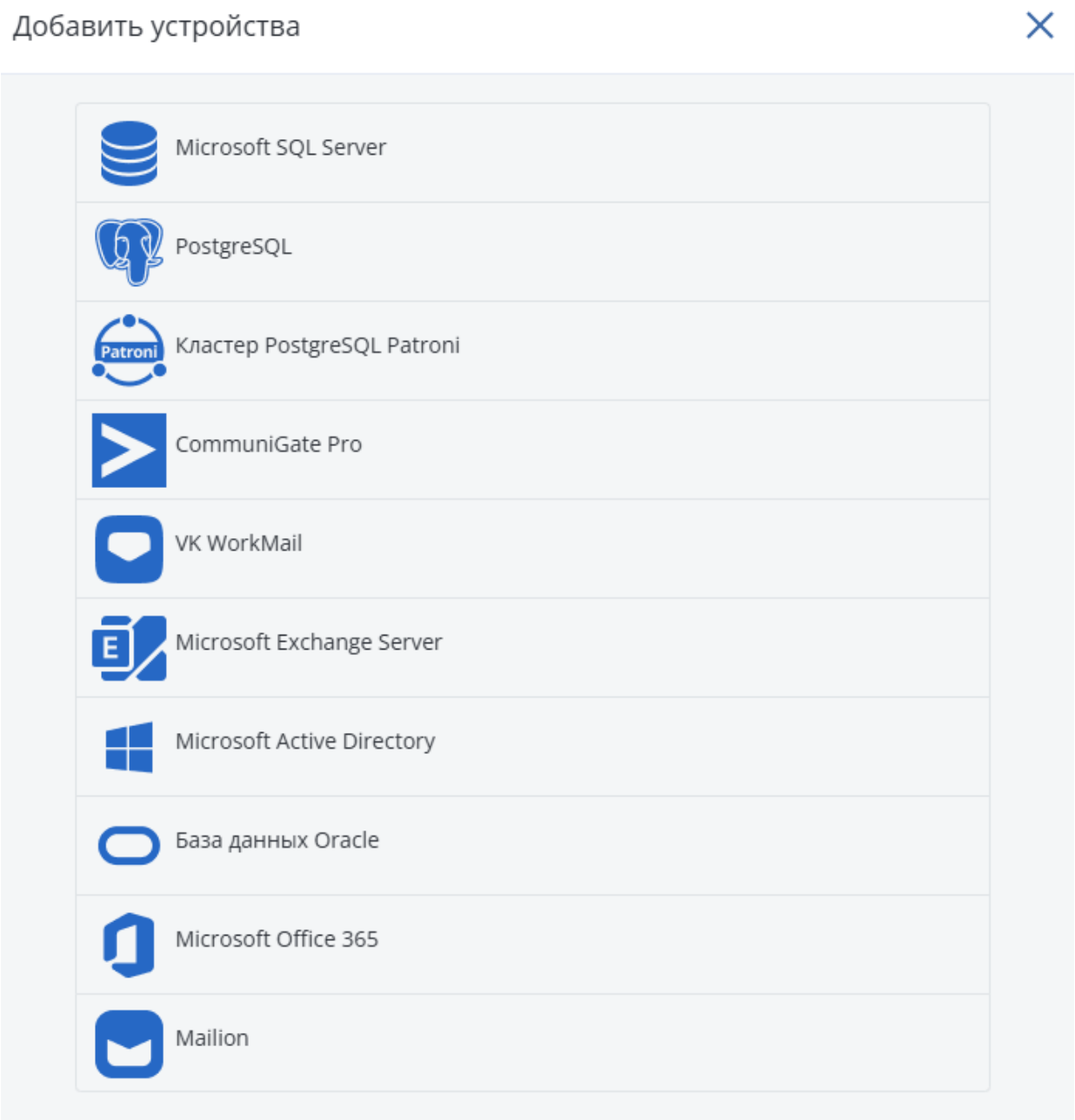
1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.
3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.
4. Отметьте в списке **Агент для Mailion**.



5. Нажмите **Готово**, затем нажмите **Установка**.

Добавление хоста Mailion

1. В веб-консоли перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.
2. В окне добавления нового устройства щёлкните **Mailion**.

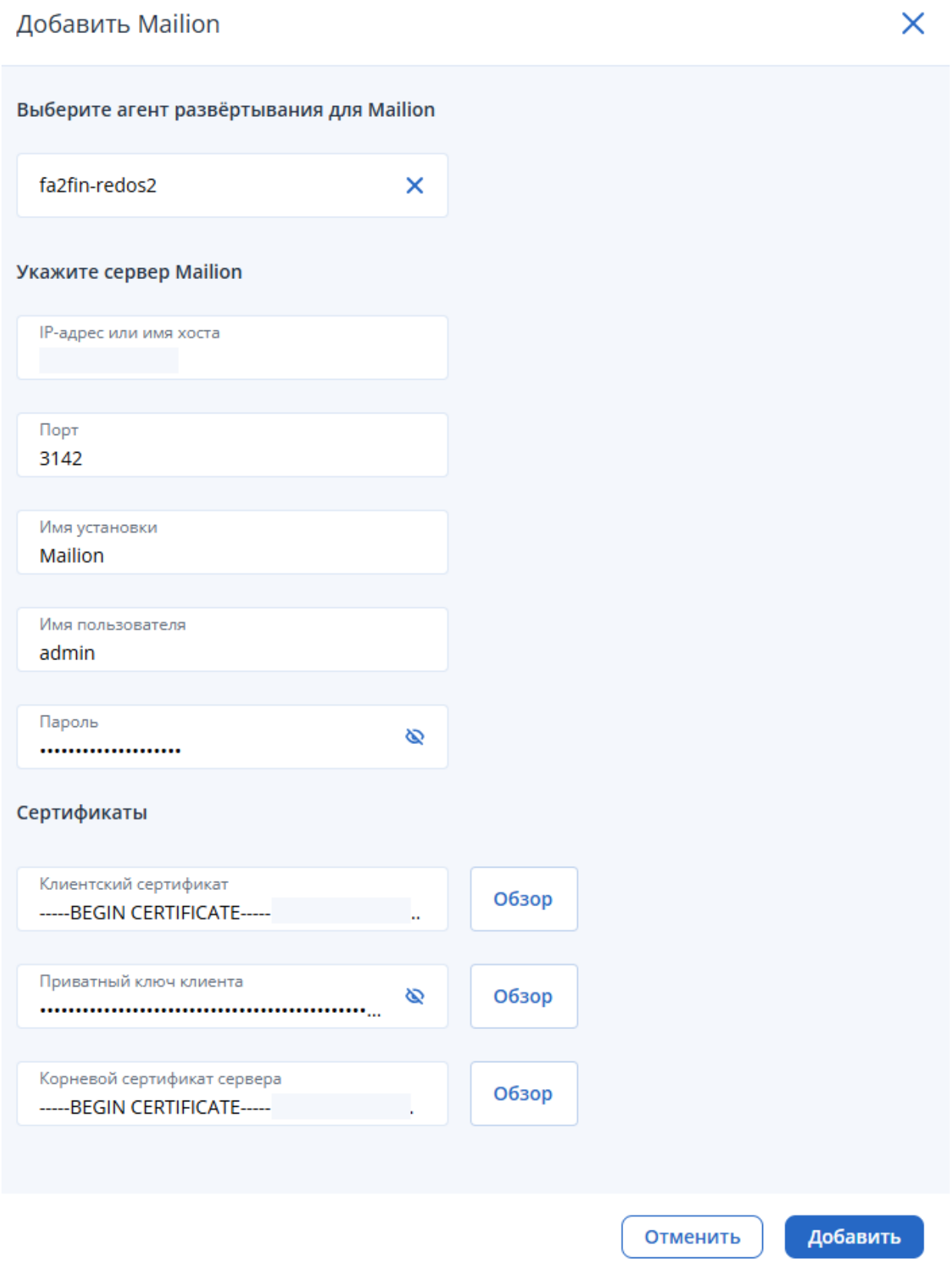


3. В поле **Выберите агент развертывания для Mailion** выберите из списка имя компьютера, на котором установлен агент или начните вводить имя для поиска.
4. В разделе **Укажите сервер Mailion**:
   - в поле **IP-адрес или имя хоста** укажите IP-адрес или имя сервера Mailion;
   - в поле **Порт** укажите порт для подключения к службам резервного копирования Mailion (порт по умолчанию, 3142);
   - в поле **Имя установки** укажите имя, под которым хост будет отображаться в системе;
   - в полях **Имя пользователя** и **Пароль** укажите данные специальной учетной записи `backuper` с

правами на резервное копирование в системе Mailion.

5. В разделе **Сертификаты** укажите файлы сертификатов в формате PEM, созданные при установке и настройке сервера Mailion (для получения сертификатов обратитесь к администратору почтовой системы Mailion):

   - **Клиентский сертификат** — нажмите **Обзор** и укажите личный сертификат пользователя, учетные данные которого используются для подключения к Mailion.
   - **Приватный ключ клиента** — нажмите **Обзор** и укажите закрытый ключ для клиентского сертификата.
   - **Корневой сертификат сервера** — нажмите **Обзор** и укажите Wildcard SSL-сертификат, выпущенный в аккредитованном центре сертификации для используемого экземпляра Mailion.

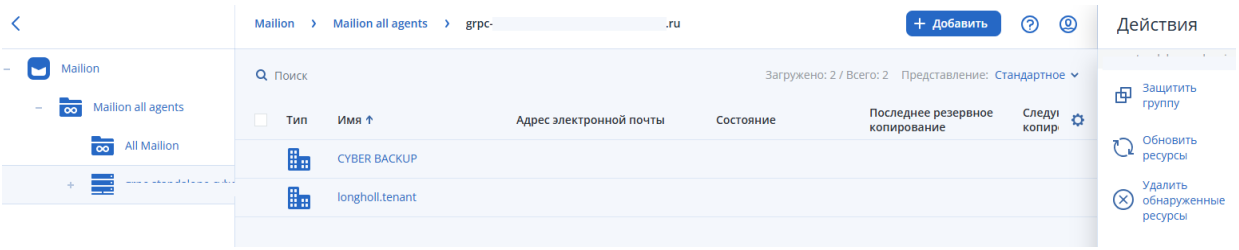


6. По окончании ввода данных нажмите **Добавить**.

Резервное копирование данных Mailion

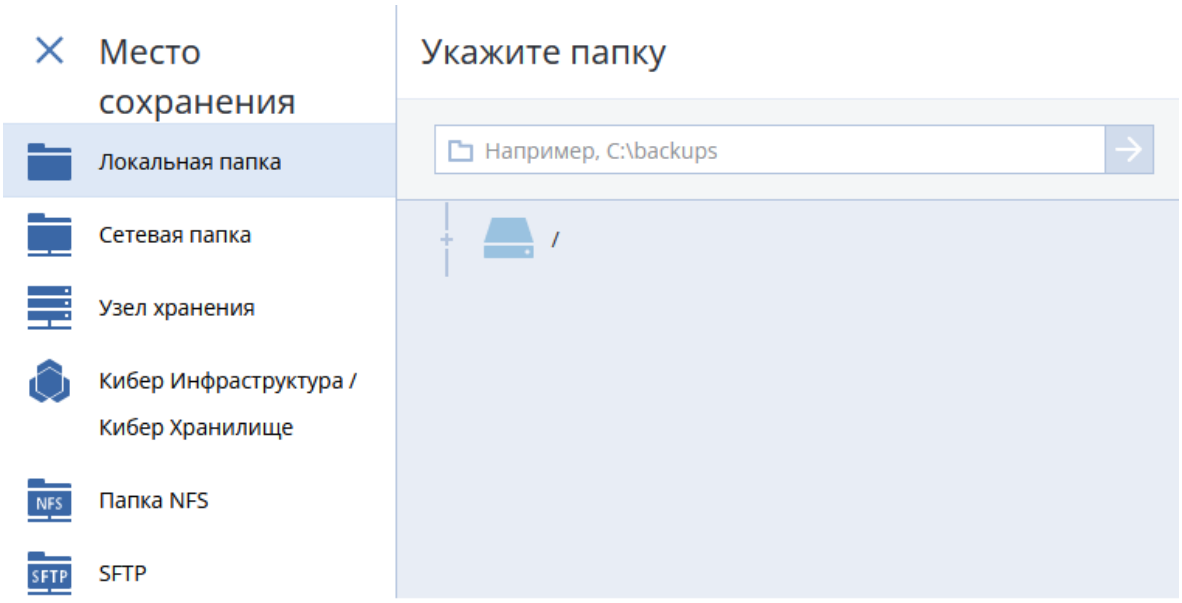
Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** → **Mailion**.
2. Выберите из списка данные Mailion, которые вы хотите защитить.
3. Перейдите на вкладку справа **Защитить** для защиты данных пользователя или **Защитить группу** для защиты тенанта и пользователей в нем.



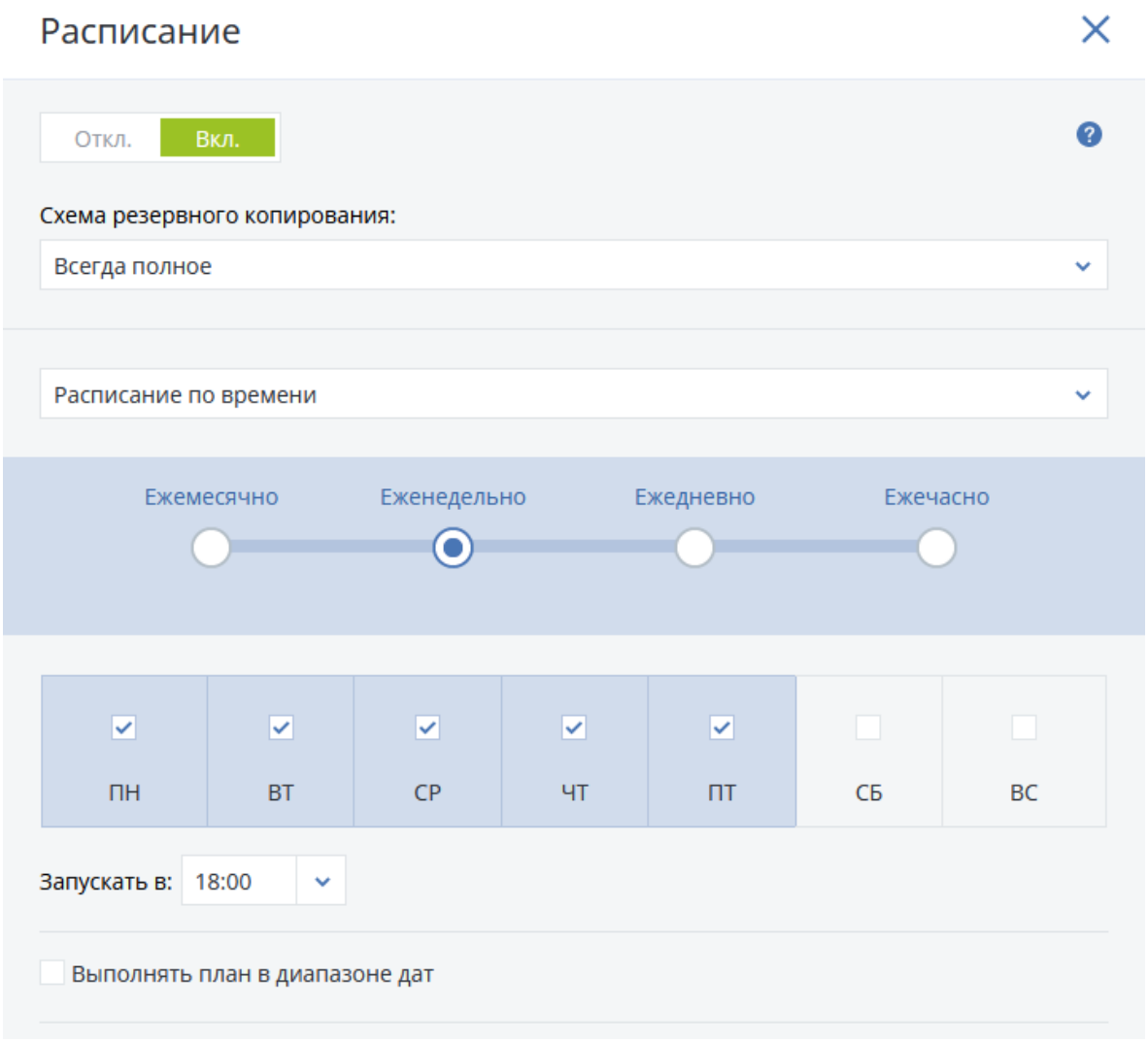
4. Заполните данные в окне создания плана защиты:

   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

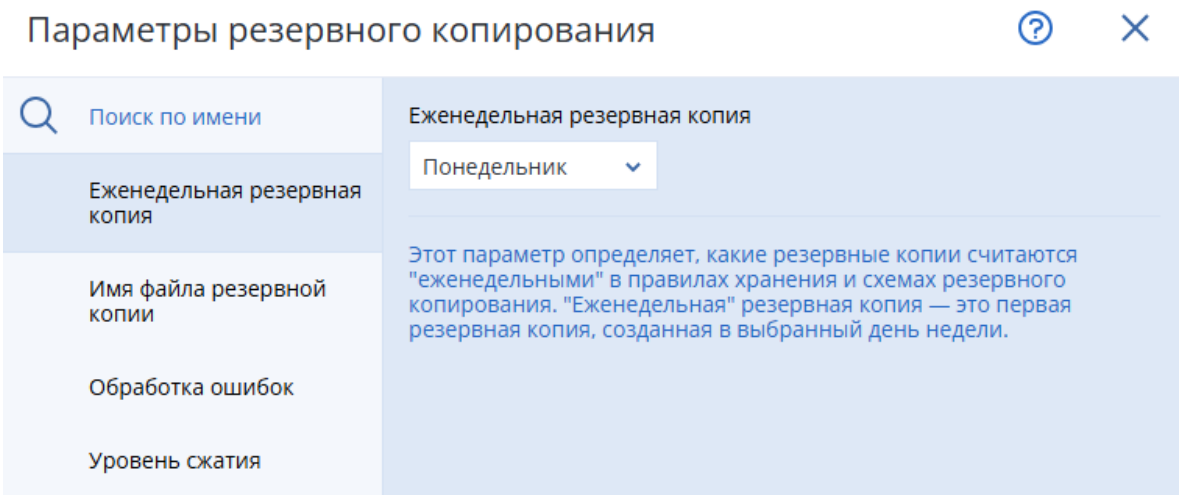


   Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

   - В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
- В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным агентам Mailion.
- [Необязательно] В поле **Параметры резервного копирования** укажите параметры обработки ошибок и уровень сжатия резервных копий.



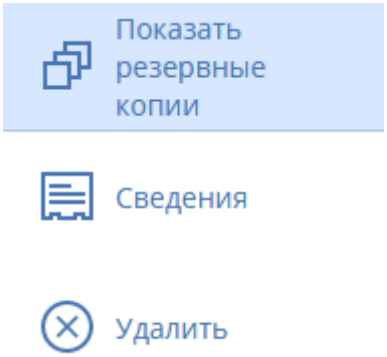
5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к выбранным данным.

См. также информацию в разделе *План защиты и модули*.

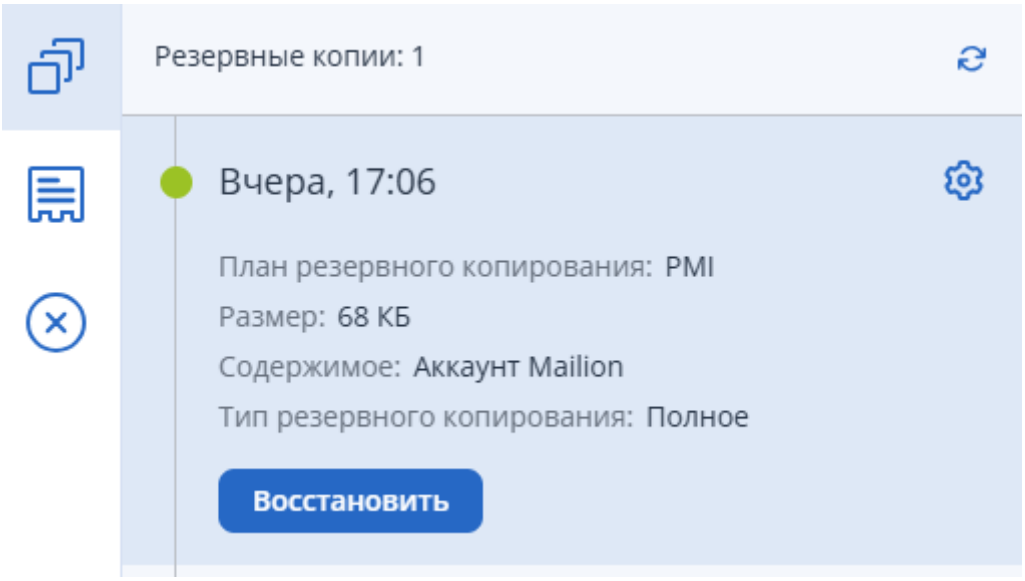
Восстановление данных Mailion

Чтобы восстановить данные Mailion, выполните следующие действия:

1. Перейдите в **Хранилище резервных копий** и выберите в списке нужные данные.
2. Выберите справа **Показать резервные копии**.

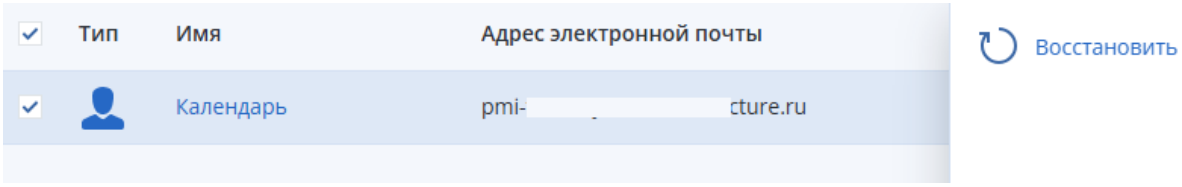


3. Нажмите **Восстановить**.

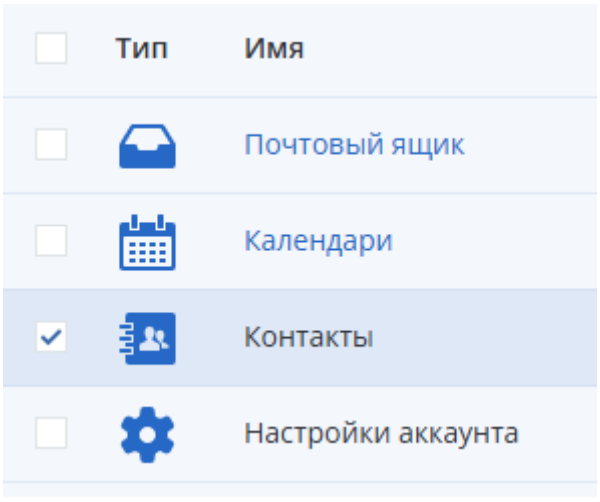


4. Выберите данные для восстановления:

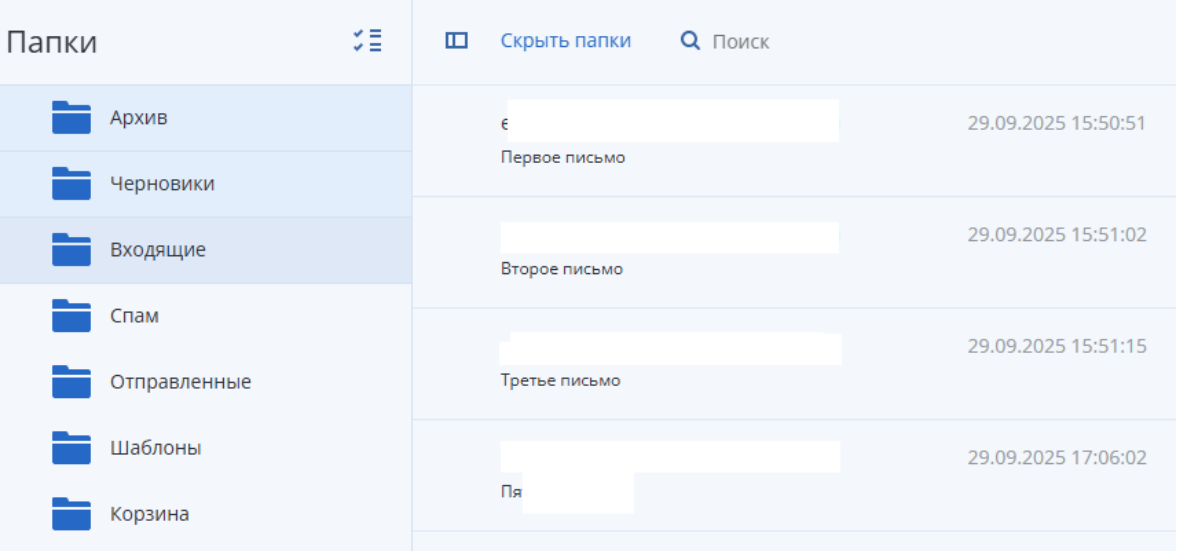
   - Если необходимо восстановить весь почтовый ящик, отметьте галочкой в списке имя почтового ящика, затем выберите справа **Восстановить**.



   - Если необходимо восстановить отдельные ресурсы пользователя, нажмите на имя резервной копии. Можно выбрать только один тип ресурса для восстановления. Выберите ресурс и нажмите справа **Восстановить**.

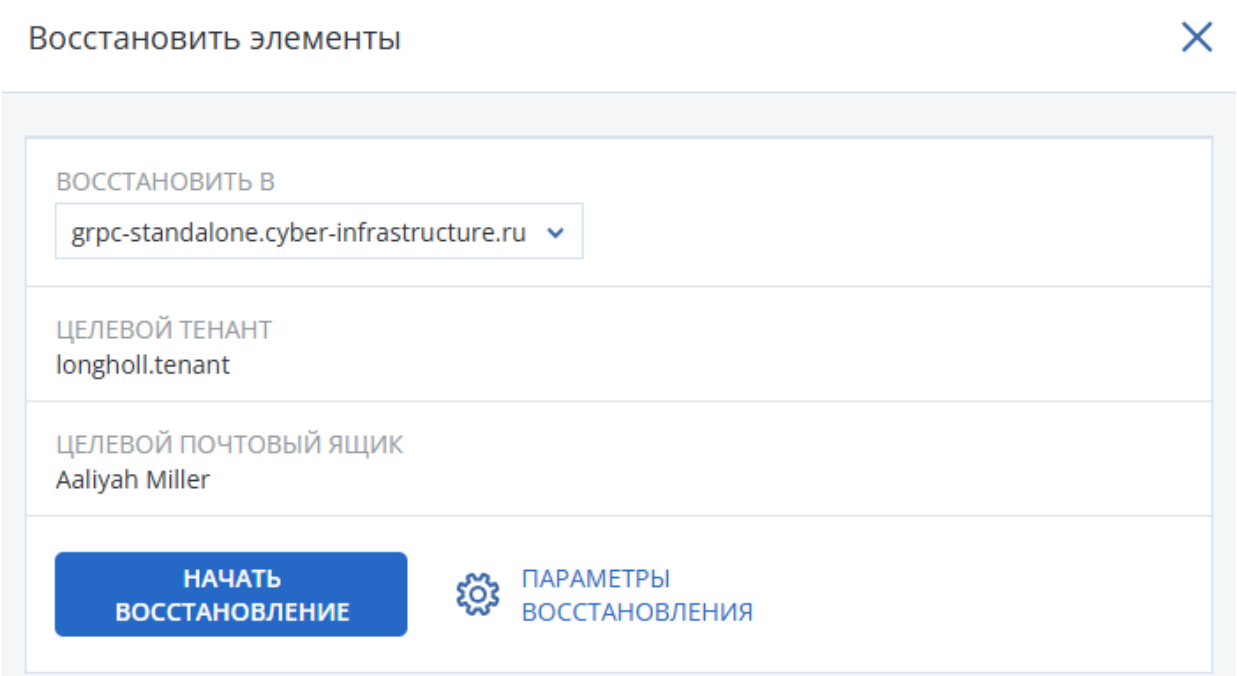


   - Если необходимо восстановить отдельные письма, нажмите на **Почтовый ящик** и выберите данные, затем нажмите справа **Восстановить**.

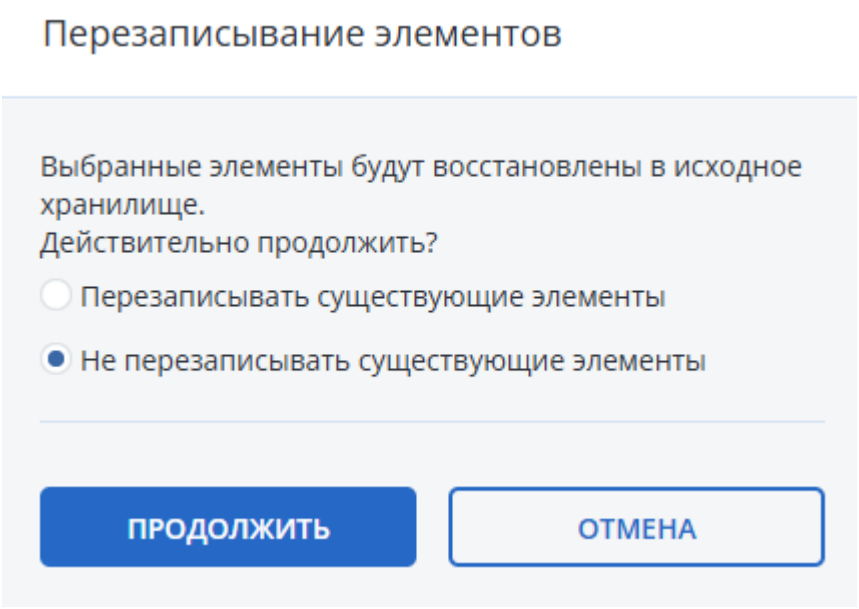


5. Укажите место восстановления. Возможные варианты:

   - Текущий сервер.
   - Новый сервер. Если сервер еще не зарегистрирован в Кибер Бэкап, укажите данные нового сервера как при установке (см. раздел *Установка Mailion*).



6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.
8. При восстановлении на текущий сервер укажите признак перезаписывания данных и нажмите **Продолжить**.



9. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

Защита RuPost

С помощью Кибер Бэкап можно выполнять резервное копирование данных почтовой системы RuPost. При использовании Кибер Бэкап регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователей и различных сбоев. Удаленные элементы можно восстановить из резервной копии.

Для резервного копирования данных RuPost понадобятся установленные и настроенные продукты:

- Кибер Бэкап 19.0 или новее с лицензией Кибер Бэкап для почтового ящика (список лицензий см. в разделе *Издания и лицензии Кибер Бэкап*).
- Почтовый сервис RuPost.

  Поддерживаемые версии RuPost указаны в разделе *Поддерживаемые почтовые сервисы*.

Для выполнения резервного копирования требуется установка агента для RuPost.

Поддерживается установка агента для операционных систем на основе Linux.

Полный список поддерживаемых операционных систем Linux см. в разделе *Поддерживаемые операционные системы*.

Возможности

Кибер Бэкап обеспечивает следующие возможности:

- резервное копирование и восстановление пользователей, почтовых ящиков и календарей;
- резервное копирование и восстановление групп пользователей;
- полное и инкрементное резервное копирование;
- гранулярное восстановление;
- возможность назначения резервного копирования на кластер почтовых агентов;
- возможность запуска планов резервного копирования вручную;
- восстановление на исходное или новое месторасположение.

После выполнения резервного копирования в архиве можно посмотреть содержимое отдельных папок и писем.

Известные проблемы и ограничения

- Не поддерживается просмотр содержимого письма на лентах.
- Не поддерживается скачивание приложения к письму (attachment) на лентах.
- Не поддерживается восстановление календаря в месторасположение, отличное от исходного.

Установка RuPost

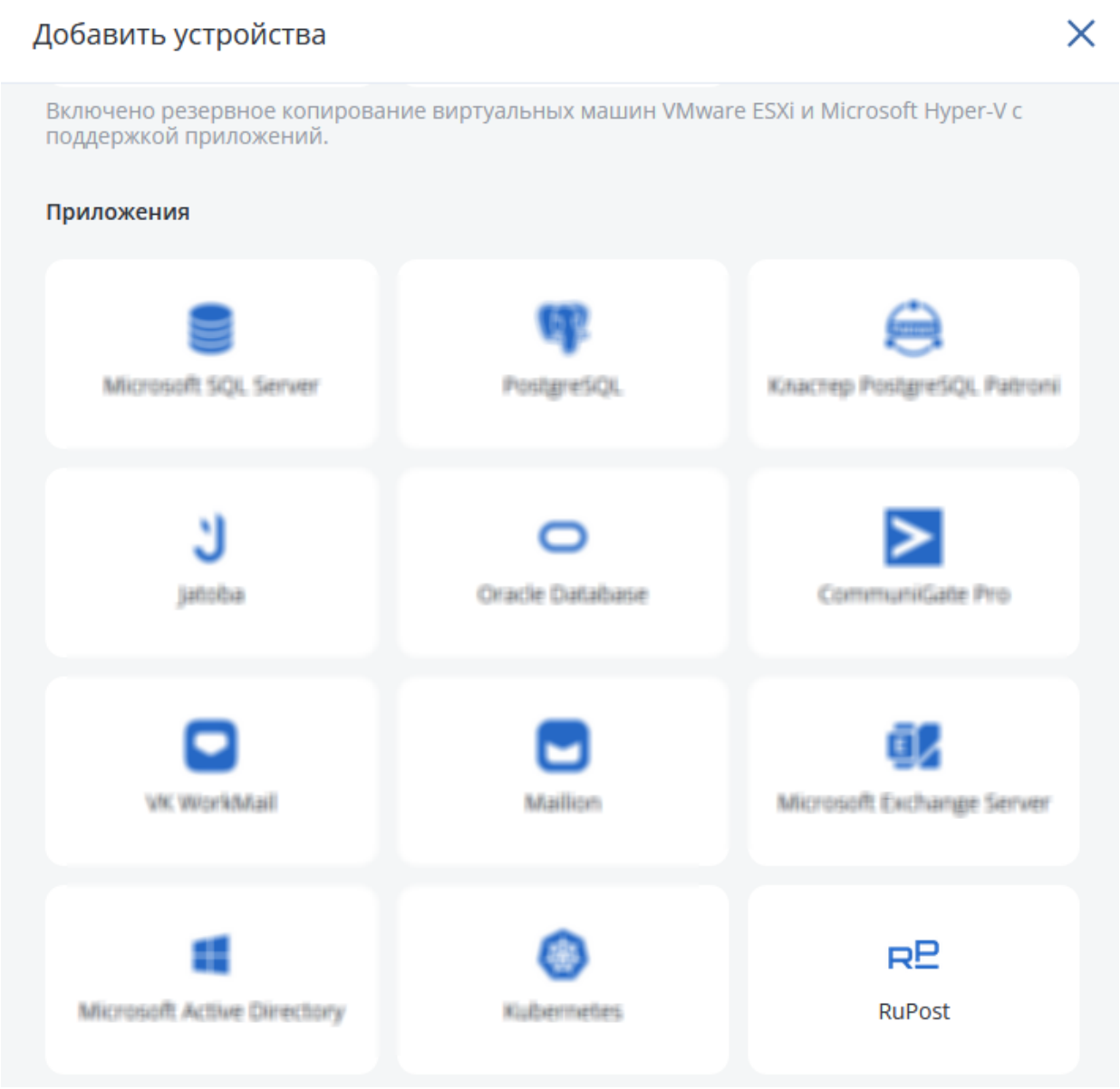
Установка RuPost включает в себя установку агента Кибер Бэкап и добавление хоста RuPost. Добавление хоста возможно лишь после установки агента.

Установка агента для RuPost

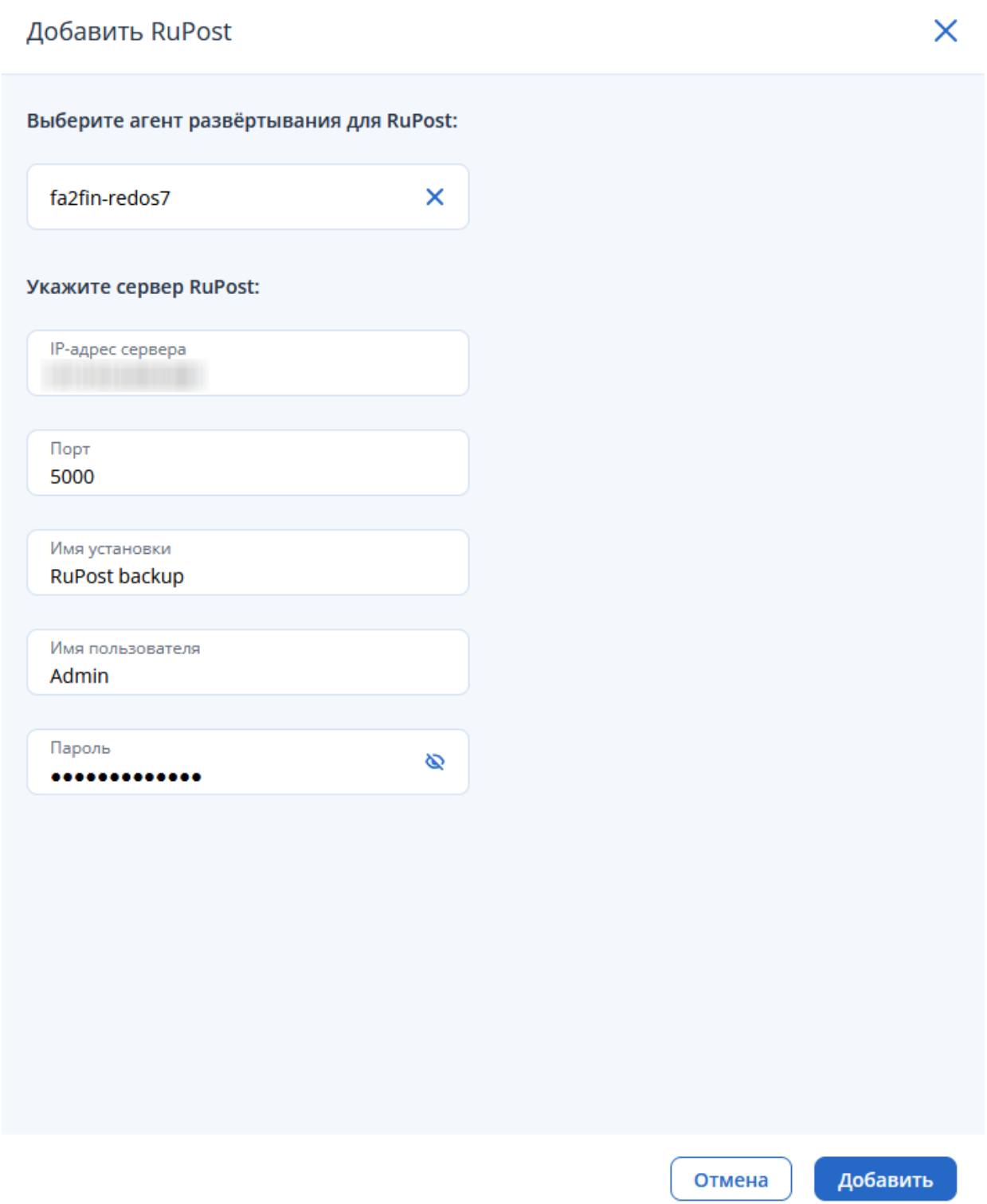
Для установки агента для RuPost для Linux обратитесь к разделу *Установка агентов в ОС Linux вручную*.

Добавление хоста RuPost

1. В веб-консоли перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.
2. В блоке **Приложения** щёлкните **RuPost**.



3. В поле **Выберите агент развертывания для RuPost** выберите из списка имя компьютера, на котором установлен агент или начните вводить имя для поиска.



4. В разделе **Укажите сервер RuPost**:

   - в поле **IP-адрес сервера** укажите IP-адрес или имя сервера RuPost;
   - в поле **Порт** укажите порт для подключения к службам резервного копирования RuPost (порт по умолчанию: 5000);

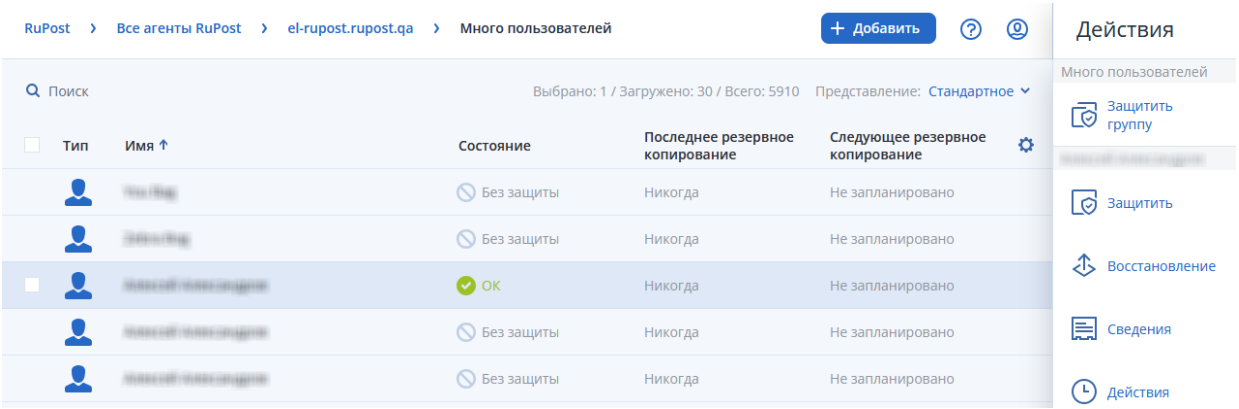
- в поле **Имя установки** укажите имя, под которым хост будет отображаться в веб-консоли;
- в полях **Имя пользователя** и **Пароль** укажите данные пользователя с правом доступа к панели администрирования RuPost.

5. По окончании ввода данных нажмите **Добавить**.

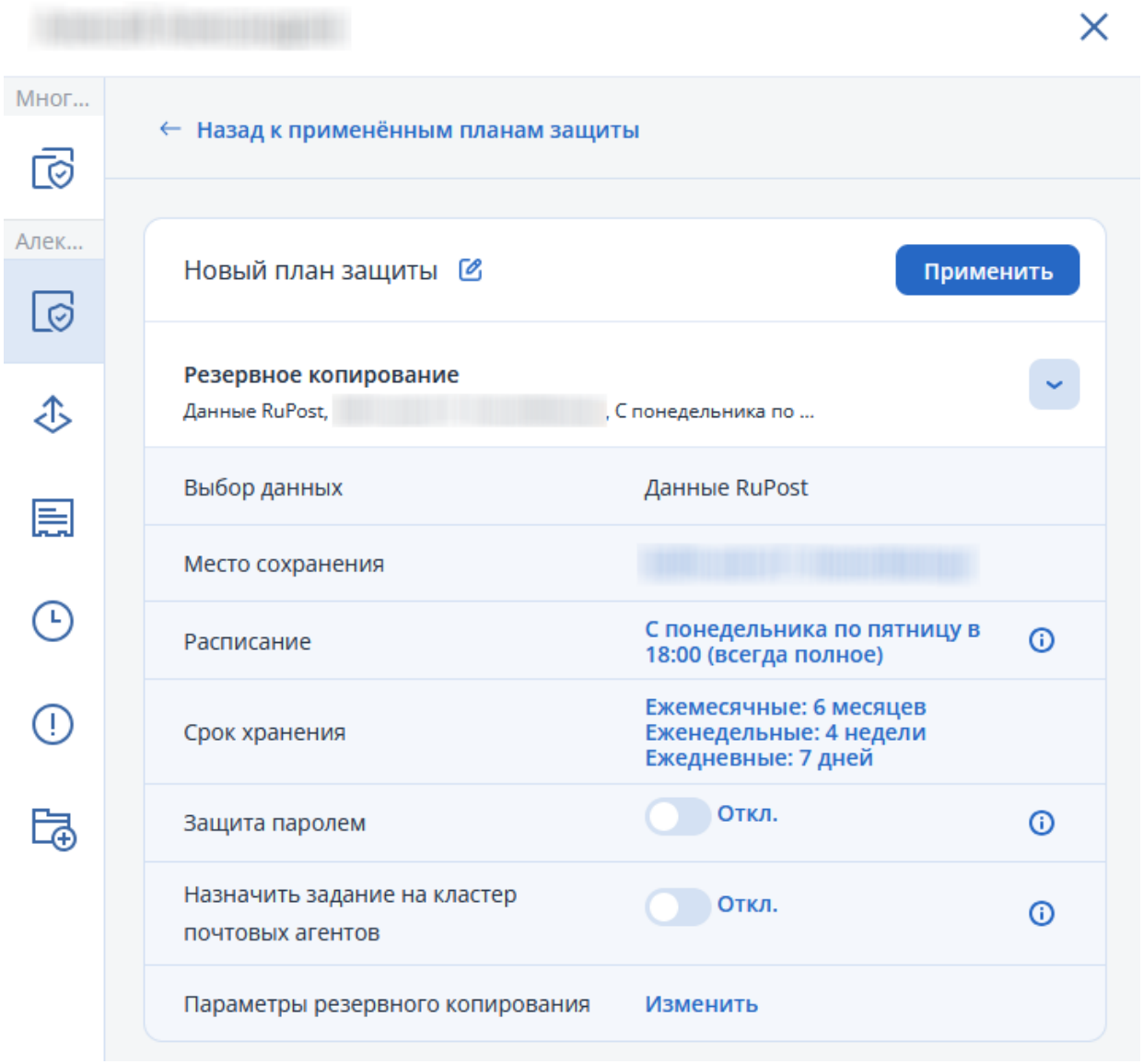
Резервное копирование данных RuPost

Для создания плана защиты выполните следующие действия:

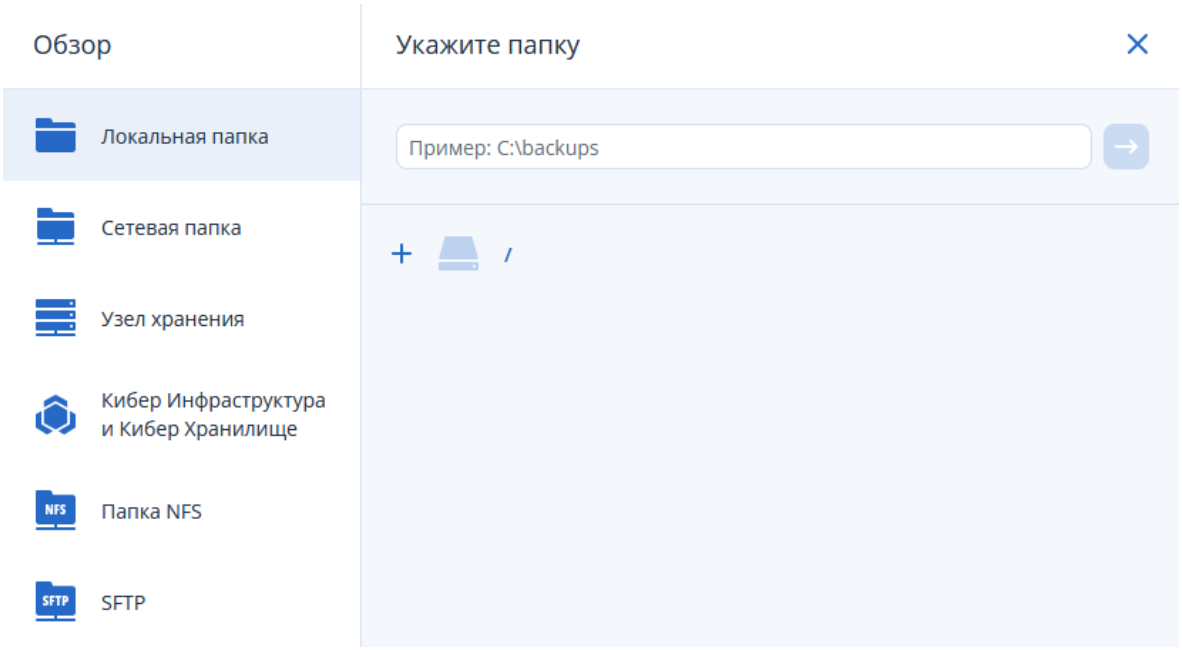
1. В веб-консоли перейдите в **Устройства** → **RuPost**.
2. Выберите из списка ресурсы RuPost, которые вы хотите защитить.
3. Перейдите на вкладку справа **Защитить** для защиты данных пользователя или **Защитить группу** для защиты группы пользователей.



4. Заполните данные в окне создания плана защиты:



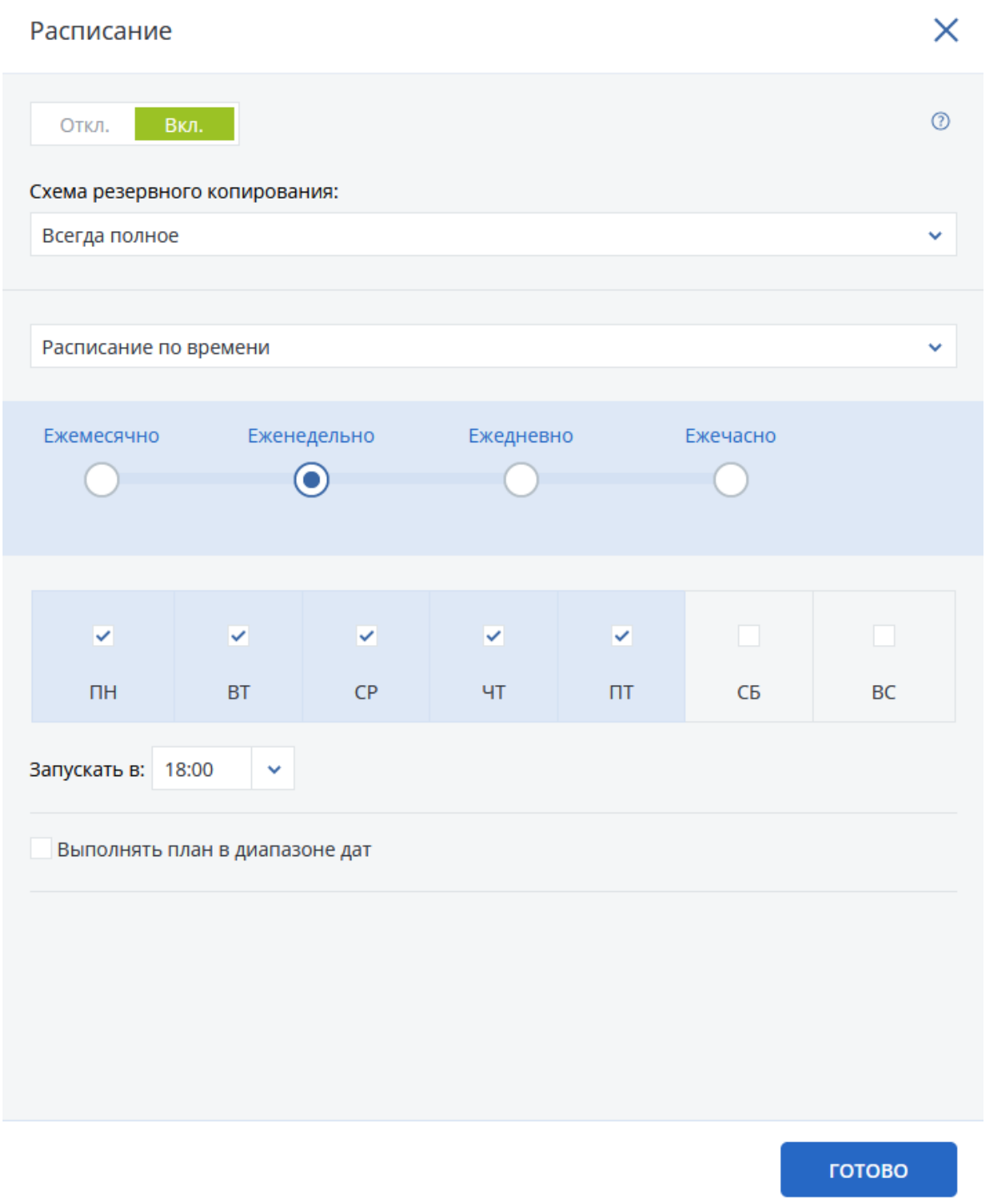
- В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP, ленты.



Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.

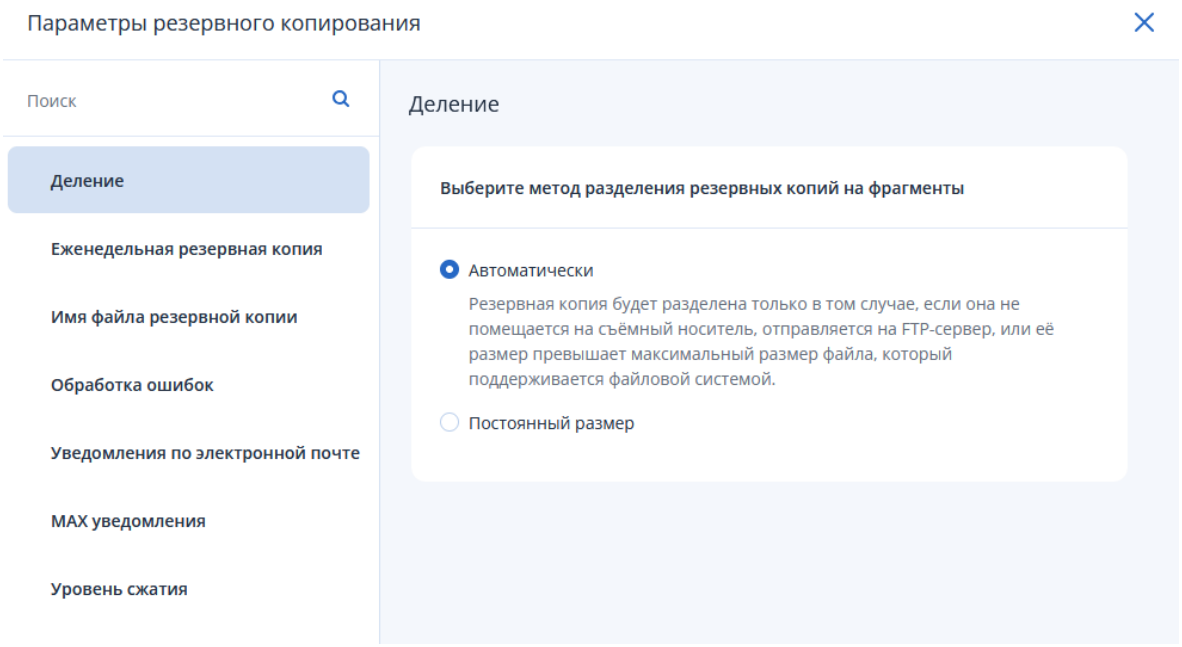
> **Примечание**
>
> Время выполнения резервного копирования в плане защиты должно умещаться в окно резервного копирования, иначе оно завершится с ошибкой. При необходимости настройте границы окна резервного копирования в панели администрирования RuPost.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища. Подробнее об этом см. раздел *Правила хранения*.
- В поле **Назначить задание на кластер почтовых агентов** включите переключатель, чтобы назначить план защиты всем зарегистрированным в Кибер Бэкап агентам для RuPost.

> **Примечание**
>
> При выборе локального места хранения резервных копий назначение на кластер не поддерживается.

- [Необязательно] В поле **Параметры резервного копирования** настройте дополнительные параметры, такие как уведомления, обработка ошибок, уровень сжатия резервных копий и другие.



5. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к выбранным данным.

См. также информацию в разделе *План защиты и модули*.

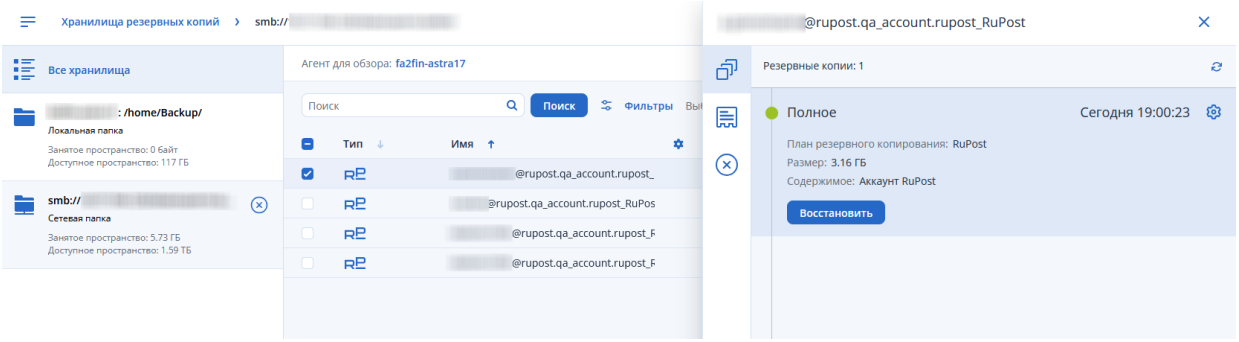
При необходимости запуск резервного копирования можно осуществить вручную (см. раздел *Запуск резервного копирования вручную*).

> **Примечание**
>
> Время выполнения резервного копирования при его запуске вручную должно умещаться в окно резервного копирования, иначе оно завершится с ошибкой. При необходимости настройте границы окна резервного копирования в панели администрирования RuPost.

Восстановление данных RuPost

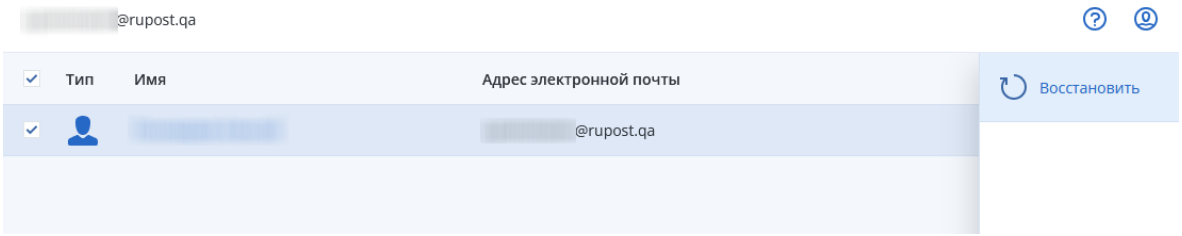
Чтобы восстановить данные RuPost, выполните следующие действия:

1. Перейдите в **Хранилище резервных копий**.
2. В колонке **Все хранилища** щелкните нужное хранилище.
3. В списке резервных копий отметьте нужную и щелкните справа **Восстановить**.



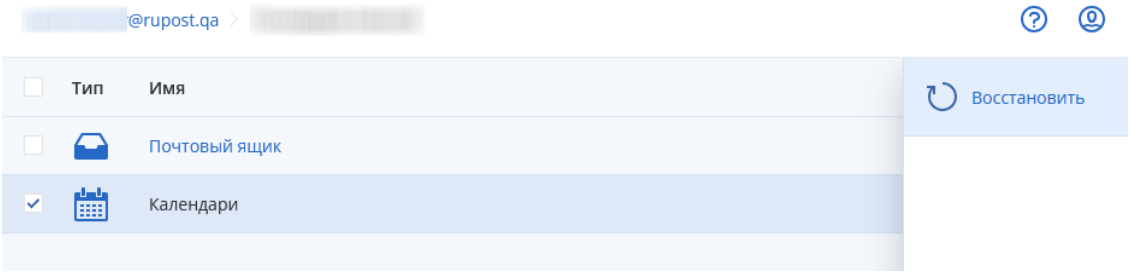
4. Выберите данные для восстановления:

   - Если необходимо восстановить все ресурсы пользователя, отметьте в списке имя почтового ящика и затем нажмите справа **Восстановить**.

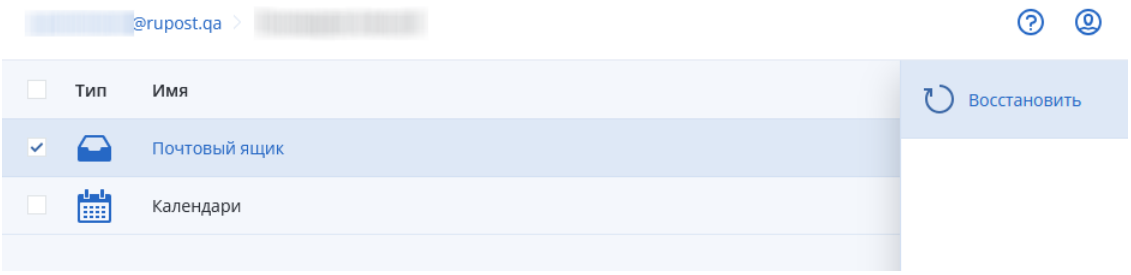


   - Если необходимо восстановить отдельные ресурсы пользователя, нажмите на имя пользователя. Выберите один тип ресурса для восстановления:

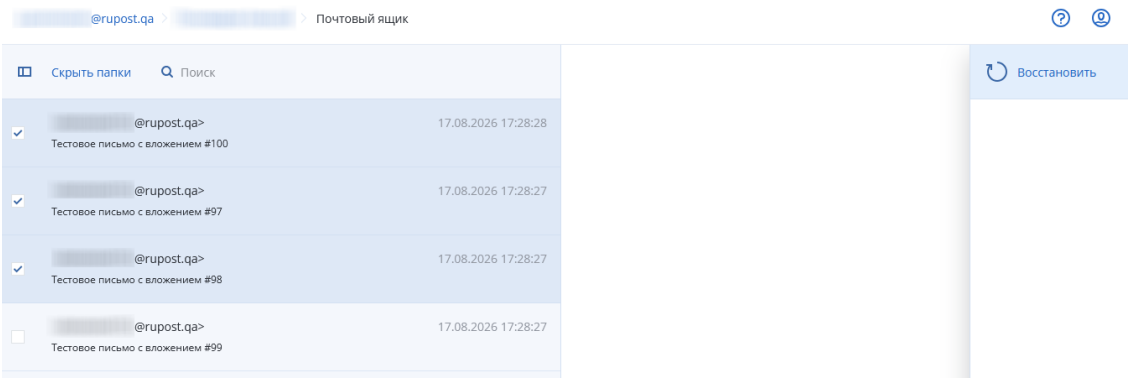
     - Если необходимо восстановить календари, нажмите **Календари** и щелкните справа **Восстановить**.



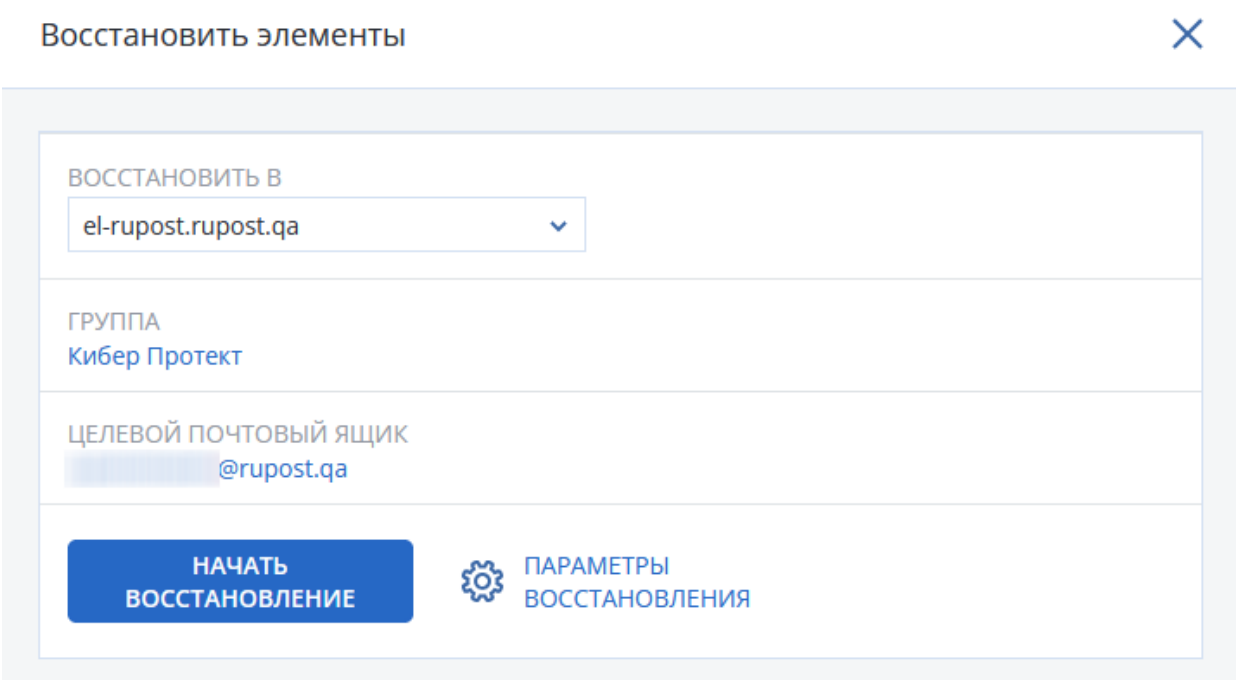
     - Если необходимо восстановить почтовый ящик, отметьте **Почтовый ящик** и нажмите справа **Восстановить**.



- Если необходимо восстановить отдельные письма, нажмите **Почтовый ящик**, далее щелкните пользователя, отметьте в списке нужные письма и нажмите **Восстановить**.



5. [Для почтового ящика и писем] Укажите место восстановления (по умолчанию предлагается исходное месторасположение):



- Выберите сервер для восстановления.

Примечание

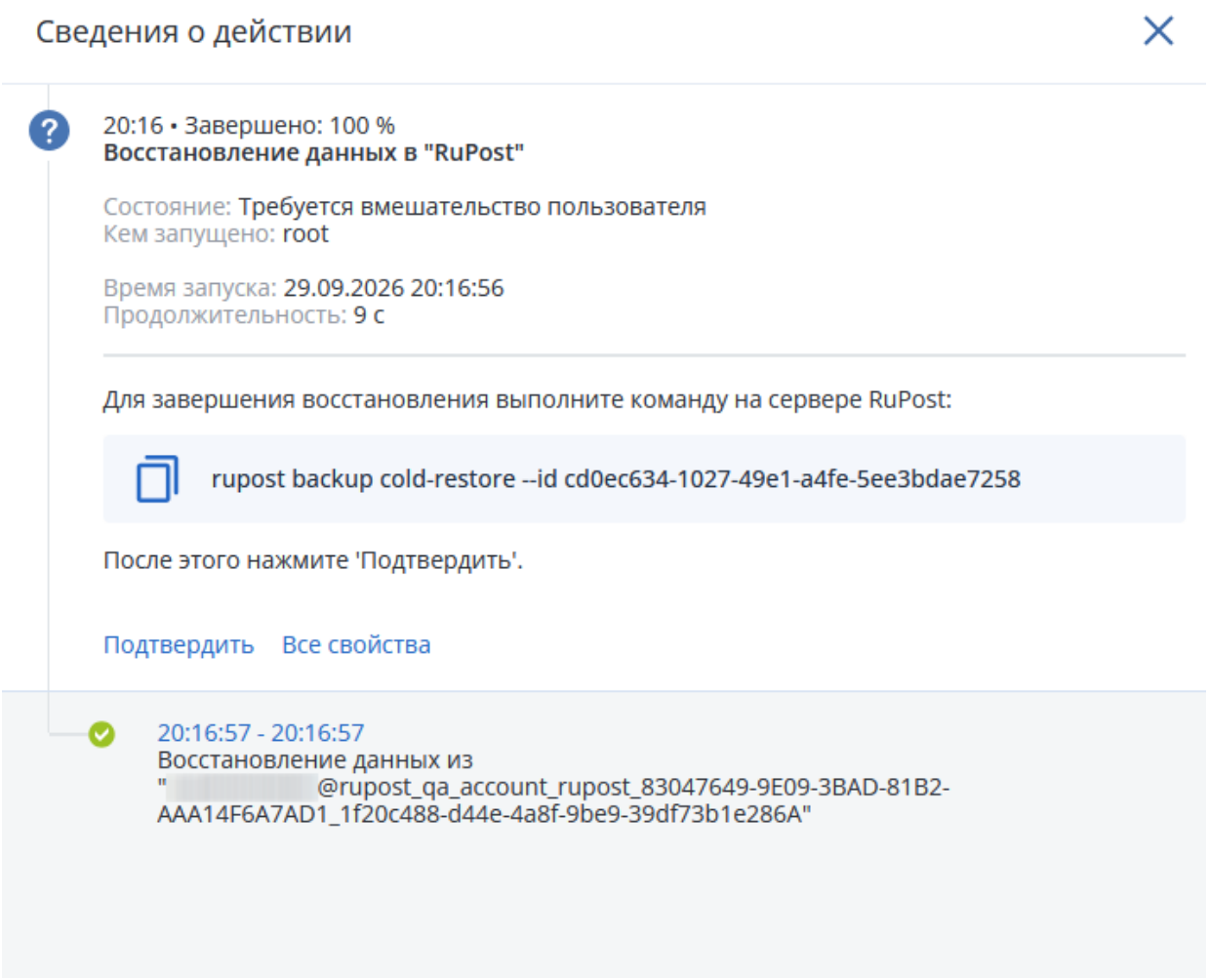
Сервер должен быть зарегистрирован в Кибер Бэкап.

- Укажите группу для восстановления.
- Укажите почтовый ящик для восстановления.

Примечание

При восстановлении всех ресурсов пользователя на новое месторасположение восстановления календаря не произойдет.

6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Нажмите **Начать восстановление**.
8. Прочитайте появившуюся на экране информацию.



Выполните необходимые действия в панели администрирования RuPost.

9. Нажмите **Подтвердить**.

> **Примечание**
>
> Для завершения восстановления необходимо выполнить команду в панели управления RuPost. В противном случае восстановление не будет выполнено, а следующее резервное копирование данных того же пользователя завершится с ошибкой.

10. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

Защита Oracle Database

С помощью Кибер Бэкап можно выполнять резервное копирование данных Oracle Database.

Поддерживаемые версии СУБД Oracle указаны в разделе *Поддерживаемые СУБД*.

Поддержка резервного копирования осуществляется с помощью команд, выполняемых до и после резервного копирования, в связке с ПО RMAN. Команды позволяют использовать ПО RMAN для создания первичных резервных копий БД Oracle через интерфейс Кибер Бэкап в рамках планов резервного копирования. При этом сохраняется вся функциональность Кибер Бэкап, доступная для файлового резервного копирования: расписание запуска заданий, настройка для размещения резервных копий в поддерживаемое хранилище, политики хранения резервных копий (включая их ротацию), уровень сжатия, защита резервных копий паролем для безопасного хранения, тип резервной копии (полная, инкрементная) и т. д.

Восстановление резервных копий в режиме Point-in-time Recovery (PITR) обеспечивается в виде связки операции восстановления резервной копии из хранилища, распаковки из сжатого защищенного архива и последующего применения ряда команд, в соответствии с доступными механизмами работы СУБД.

В качестве команд до и после резервного копирования можно использовать скрипты ОС и RMAN. Примеры приведены в статье базы знаний.

Примечание

Для работы с Oracle Database версий старше 12 не требуется устанавливать агент для Oracle, как описано в разделе *Защита Oracle Database предыдущих версий*. Для таких версий необходим только агент для Linux (см. раздел *Установка агентов в ОС Linux вручную*).

Это позволит использовать все преимущества RMAN, включая:

- Различные типы резервного копирования:
  - Full Backup,
  - Incremental Backup,
  - Differential Backup,
  - Cumulative Backup,
  - Archivelog Backup.
- Выполнение резервного копирования как промышленных БД, так и копий горячего резерва (Standby).

- Выполнение резервного копирования БД в конфигурации кластера Oracle RAC.
- Восстановление на заданные точки во времени (Point-in-Time Recovery, PITR):
  - с указанием времени в различных вариантах,
  - с указанием номера изменения БД (SCN).

Защита Oracle Database предыдущих версий

В данном разделе описано, как настроить резервное копирование баз данных Oracle следующих версий:

- Oracle Database 11g, все выпуски;
- Oracle Database 12c, все выпуски.

Поддерживаются только конфигурации с одним экземпляром.

Условия для резервного копирования

Для резервного копирования баз данных Oracle понадобится Кибер Бэкап 15 или новее с лицензией ”Кибер Бэкап для физического сервера” на каждый экземпляр Oracle Database, резервное копирование которого вы планируете выполнять (список лицензий см. в разделе *Издания и лицензии Кибер Бэкап*).

Для выполнения резервного копирования нужно установить агент Кибер Бэкап для операционной системы, которую вы используете (Windows или Linux), а также агент для Oracle. Список поддерживаемых операционных систем см. в разделе *Поддерживаемые операционные системы*.

Предварительные требования для резервных копий машин Windows с поддержкой приложений описаны в разделе *Предварительные требования*.

Методы резервного копирования

Решение Кибер Бэкап предоставляет два метода защиты данных Oracle. Оба метода позволяют использовать функциональность управления резервными копиями: централизованное управление, репликация, хранение, уведомления электронной почты и другие возможности.

Резервное копирование сервера

Создайте резервную копию всего сервера Oracle, используя резервное копирование с поддержкой приложений для согласованности состояния базы данных Oracle с приложениями.

Преимущества:

- Меньшее директивное время восстановления при сбое всего сервера.
- Резервное копирование полностью настраивается в графическом интерфейсе пользователя. Не

обязательно иметь навыки работы с Oracle Recovery Manager (RMAN).

- Имея резервную копию всего сервера, можно легко создать виртуальную машину, которая развертывается за считанные секунды и заменяет исходный сервер.

Ограничения:

- База данных должна храниться в обычной файловой системе, поддерживаемой программой резервного копирования. Разделы без форматирования и тома Oracle Automatic Storage Management (ASM) не поддерживаются.

Резервное копирование базы данных

Создайте резервную копию базы данных Oracle с помощью Oracle Recovery Manager (RMAN) в локальной папке, затем создайте резервную копию полученных файлов в другом хранилище, сохранив в локальной папке только последние резервные копии RMAN. Решение предоставляет сценарии RMAN, которые могут автоматически запускаться до резервного копирования файлов. Поэтому всю процедуру можно настроить и выполнить в одном рабочем процессе. При этом не требуется навыков создания сценариев RMAN.

Преимущества:

- Поддержка баз данных, которые хранятся на необработанных разделах или томах Oracle Automatic Storage Management (ASM).

Ограничения:

- Большее директивное время восстановления при сбое всего сервера.

Сравнительная характеристика

Показатель	**Резервное копирование сервера**	**Резервное копрование базы данных**
Директивное время восстановления при сбое всего сервера	Меньше	Больше
Возможность запускать виртуальный сервер Oracle	Да, ESX или Hyper-V	Нет
Поддержка разделов без форматирования/ASM	Нет	Да
Поддержка распространения базы данных на несколько томов	Да	Да

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Показатель	Резервное копирование сервера	Резервное копрование базы данных
Простота использования	Резервное копирование полностью настраивается в графическом интерфейсе пользователя. Нет необходимости знать RMAN.	Необходимо настроить отдельные планы резервного копирования для полных резервных копий архивированного журнала.

Методы восстановления

Восстановление сервера

Восстановление всего сервера на момент времени создания резервной копии. При восстановлении сервера на ”голое железо” Oracle Database восстанавливается среди других данных и будет в согласованном состоянии.

Преимущества:

- Самый быстрый и простой способ аварийного восстановления.
- Позволяет выполнить миграцию физической машины на виртуальную (P2V), а также воспользоваться другими методами репликации или миграции сервера Oracle.
- Не обязательно иметь навыки работы с Oracle Recovery Manager (RMAN).

Восстановление с использованием Oracle Explorer

Восстанавливайте файлы данных по состоянию на определенный момент времени, используя инструмент Oracle Explorer, который входит в состав решения. Данный инструмент использует RMAN и включает в себя целый ряд полезных параметров RMAN в удобном пользовательском интерфейсе. Этот инструмент позволяет выполнить восстановление как с резервных копий с поддержкой приложений, так и с резервных копий баз данных.

Преимущества:

- Позволяет выполнить фрагментарное восстановление данных Oracle на определенный момент времени непосредственно с резервных копий с поддержкой приложений.
- Не обязательно иметь навыки работы с Oracle Recovery Manager (RMAN).

Ограничения:

- При восстановлении с резервных копий баз данных может потребоваться двухэтапный процесс.

Восстановление с использованием сценариев

Восстанавливайте базу данных по состоянию на время создания последней резервной копии с локально сохраненных резервных копий RMAN. Для такого восстановления решение предоставляет сценарий RMAN. Чтобы восстановить базу данных по состоянию на время создания предыдущей резервной копии RMAN, сначала восстановите эту резервную копию RMAN из резервной копии на уровне файлов, а затем используйте сценарии для восстановления базы данных.

Те же самые операции восстановления можно выполнить с файлами данных и файлом управления. Это решение предоставляет отдельные сценарии для этих операций восстановления.

Кроме того, это решение предоставляет отдельные сценарии для восстановления по состоянию на настраиваемый момент времени. Этот момент времени можно задать, указав точную дату и время или номер системного изменения (SCN).

Преимущества:

- Можно настроить восстановление в расширенных сценариях.

Ограничения:

- Для выполнения настройки требуется знание RMAN.
- Может потребоваться двухэтапный процесс восстановления.

Общие ограничения

- Кластеры Oracle Real Application (RAC) не поддерживаются.
- Поддерживаются только конфигурации базы данных с одним экземпляром.
- Невозможно создать резервную копию отдельных подключаемых баз данных (pluggable database, PDB). Для них резервные копии создаются как часть контейнерной базы данных (container database, CDB).
- База данных должна быть в режиме ARCHIVELOG (флаг `NOARCHIVELOG` отключен).

  Базу данных в режиме NOARCHIVELOG можно скопировать только в закрытом состоянии, а решение для резервного копирования рассчитано на то, чтобы создавать резервные копии баз данных без простоя. Если включенная база данных работает в этом режиме, а RMAN больше невозможно использовать, при попытке создать резервную копию на уровне дисков будет возвращена ошибка VSS.

  Чтобы избежать этой ошибки, остановите и закройте базу данных командой до захвата данных и перезапустите базу данных командой после захвата данных. Можно будет восстановить весь сервер, но восстановление через Oracle Explorer будет недоступно.

Установка

Компоненты программного обеспечения для резервного копирования

Чтобы защитить данные Oracle, необходимы следующие компоненты:

- **Сервер управления** позволяет централизованно управлять несколькими машинами: создавать планы резервного копирования, отслеживать их выполнение, развертывать агенты и выполнять другие действия. Его можно установить на машине с Windows или Linux, которая имеет сетевой доступ ко всем управляемым машинам.

  Чтобы установить сервер управления, выполните действия, описанные в разделе *Установка сервера управления*.

- **Агенты** необходимы для резервного копирования серверов и баз данных.

  - Чтобы защитить физический или виртуальный сервер, на котором работает Oracle Database, установите на этот компьютер **Агент для Oracle**. **Агент для Windows** или **Агент для Linux** (в зависимости от операционной системы сервера) и **агент для Oracle** должны быть установлены на физической машине с Oracle Database. В Linux **Агент для Oracle** использует тот же установщик, что и **Агент для Linux**.
  - **Oracle Explorer** предназначен для фрагментарного восстановления данных Oracle. Этот компонент входит в состав агента для Oracle.

  Чтобы установить агенты, выполните действия, описанные в разделе *Локальная установка агентов*.

- **Python 3** на машине с агентом для Oracle необходим для резервного копирования и восстановления Oracle Database. Путь к интерпретатору Python (`python` для Linux или `python.exe` для Windows) должен быть добавлен в переменную окружения `PATH`.

Сценарии интеграции с Oracle RMAN

Эти сценарии автоматически устанавливаются вместе с агентом для Oracle.

Эти сценарии устанавливаются в следующую папку:

- В Windows: `%ProgramFiles%\Acronis\Oracle`.
- В Linux: `/usr/lib/Acronis/Oracle`.

Далее эта папка называется `<папка расположения сценариев>`.

Список сценариев

В таблице ниже перечислены предоставляемые сценарии.

Имя сценария	ОС	Описание
main.py	Windows, Linux	Основной сценарий, который выполняет все операции, связанные с резервным копированием и восстановлением Oracle. Не предназначен для независимого использования.
main.cfg	Windows, Linux	Конфигурационный файл содержит параметры доступа к базе данных и другие параметры, которые являются общими для других сценариев. Это — единственный файл, в который может потребоваться внести изменения. Этот файл расположен в следующей папке: • В Windows: `%ProgramData%\Acronis\Oracle\Config` • В Linux: `/var/lib/Acronis/Oracle/Config`
backup_full_pre.bat	Windows	Вызывает основной сценарий для создания полной резервной копии базы данных утилитой RMAN.
backup_full_pre.sh	Linux	
backup_incr_pre.bat	Windows	Вызывает основной сценарий для создания резервной копии архивированных журналов утилитой RMAN.
backup_incr_pre.sh	Linux	
restore_disaster.bat	Windows	Вызывает основной сценарий для восстановления всей базы данных до последнего доступного состояния.
restore_disaster.sh	Linux	
restore_datafiles.bat	Windows	Вызывает основной сценарий для восстановления файлов данных до последнего доступного состояния (полное восстановление).
restore_datafiles.sh	Linux	
restore_controlfile.bat	Windows	Вызывает основной сценарий для восстановления файла управления до последнего доступного состояния.
restore_controlfile.sh	Linux	

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Имя сценария	ОС	Описание
restore_to-point-in-time.bat	Windows	Вызывает основной сценарий для восстановления базы данных до состояния на определенный момент времени в прошлом (неполное восстановление). Такой момент времени указывается датой и временем в следующем формате: гггг-мм-дд:чч24:мм:сс.
restore_to-point-in-time.sh	Linux	
restore_to-scn.bat	Windows	Вызывает основной сценарий для восстановления базы данных до состояния на определенный момент времени в прошлом (неполное восстановление). Такой момент времени задается номером системного изменения (SCN).
restore_to-scn.sh	Linux	
last_log.bat	Windows	Вызывает основной сценарий, чтобы показать его последний журнал.
last_log.sh	Linux	
*.rman	Windows, Linux	Сценарии RMAN для различных операций. Не предназначен для независимого использования.
*.sql	Windows, Linux	Сценарии SQL*Plus для различных операций. Не предназначен для независимого использования.
Other	Windows, Linux	Вспомогательные сценарии. Не предназначен для независимого использования.

Параметры конфигурации

В этом разделе перечислены параметры, которые можно изменить в файле `main.cfg`. Эти параметры влияют только на резервное копирование базы данных. Резервное копирование сервера не использует эти параметры.

- `BACKUP_DIR`: локальная папка, в которой будут храниться резервные копии RMAN.

  На диске, на котором вы хотите хранить резервные копии RMAN, должно быть достаточно свободного места для двух копий базы данных.

  Путь по умолчанию: `C:\local_rman_backups\` в Windows и `tmp/local_rman_backups` в Linux.

> **Примечание**
>
> В Windows используйте две обратные косые черты вместо одной. Например, путь по умолчанию: `C:\\local_rman_backups\\`.

- TARGET: строка подключения для базы данных.

  Значение по умолчанию: /. Если задано это значение, сценарий выполняет вход в Oracle с использованием аутентификации операционной системы.

  > **Примечание**
  >
  > Поддерживается только аутентификация операционной системы. В Windows данный сценарий использует учетную запись, с которой запускается служба агента. В Linux данный сценарий использует значение переменной ORACLE_USER (см. далее в этом разделе). Как в Windows, так и в Linux учетная запись, которую вы указываете, должна иметь системную привилегию SYSDBA в Oracle. Чтобы предоставить эту привилегию, добавьте пользователя в группу ORA_DBA.

  Чтобы использовать проверку подлинности базы данных, укажите строку подключения в следующем формате:

  ```
  <имя_пользователя>/<пароль>[@<идентификатор подключения>]
  ```

  В этом выражении:

  - <имя_пользователя>/<пароль> — это учетные данные сценария, который будет использоваться для входа в Oracle. Эта учетная запись должна иметь системную привилегию SYSDBA в Oracle.
  - <идентификатор подключения> — это идентификатор подключения Oracle Net. Это может быть имя сетевой службы, имя службы базы данных или имя сетевой службы. Идентификатор подключения требуется в Oracle Database Engine 12 для того, чтобы строка подключения указывала на контейнерную базу данных (CDB), а не на подключаемую базу данных (PDB).

  Пример: чтобы для подключения к базе данных, которая имеет псевдоним Oracle Net FLEETDB, сценарий использовал имя пользователя, для параметра TARGET введите значение HR/password@FLEETDB.

В Linux может потребоваться дополнительно изменить указанные ниже переменные среды Oracle, чтобы они соответствовали фактическим настройкам Oracle Database:

- ORACLE_BASE: корень дерева каталогов Oracle Database. Значение по умолчанию: /u01/app/oracle. Чтобы узнать фактическое значение, выполните команду env | grep ORACLE_BASE под учетной записью, которая имеет системную привилегию SYSDBA в Oracle.
- ORACLE_HOME: расположение конкретной установки Oracle Database. Значение по умолчанию: /u01/app/oracle/product/12.1.0.2/db_1/. Чтобы узнать фактическое значение, выполните команду env | grep ORACLE_HOME под учетной записью, которая имеет системную привилегию SYSDBA в

Oracle.

- `ORACLE_SID`: системный идентификатор базы данных. Значение по умолчанию `orcl`. Чтобы узнать фактическое значение, выполните команду `env | grep ORACLE_SID` под учетной записью, которая имеет системную привилегию SYSDBA в Oracle.
- `ORACLE_USER`: учетная запись, которую RMAN и SQL*Plus используют для входа в Oracle, когда параметр `TARGET` имеет значение `/` (см. описание параметра TARGET выше). Значение по умолчанию: `oracle`. Учетная запись, которую вы указываете, должна иметь системную привилегию SYSDBA в Oracle. Кроме того, эта учетная запись должна входить в группу **acronis** . Эта группа автоматически создается во время установки агента для Oracle и определяется в файле `/etc/passwd`. Если учетная запись `ORACLE_USER` не входит в группу **acronis**, используйте команду `groupadd`, чтобы добавить ее.
- `RMAN_PATH`: каталог с утилитой RMAN.

  Значение по умолчанию: `$ORACLE_HOME/bin`. Чтобы узнать фактическое значение, выполните команду `which rman` под учетной записью, которая имеет системную привилегию SYSDBA в Oracle. Например, если команда возвращает строку `/u01/app/oracle/product/12.1.0.2/db_1/lib/rman`, задайте переменной `RMAN_PATH` значение `$ORACLE_HOME/lib`.

Резервное копирование базы данных Oracle

Подготовка

Выберите локальную папку, в которой будут храниться резервные копии RMAN. На диске, выделенном для хранения резервных копий RMAN, должно быть достаточно свободного пространства для двух копий базы данных. Не выбирайте тот же диск, на котором хранится база данных.

Путь по умолчанию: `C:\local_rman_backups\` в Windows и `/tmp/local_rman_backups` в Linux. Чтобы изменить этот путь, измените значение параметра `BACKUP_DIR` в файле `main.cfg` как описано в разделе *Параметры конфигурации*.

Если папка не существует, создайте ее вручную заранее. Указанные ниже пользователи должны иметь разрешение на чтение в отношении этой папки:

1. Учетная запись, с которой выполняется служба агента.
2. Учетная запись, с которой выполняется служба экземпляра (`OracleService<Идентификатор базы данных>`).
3. [Только в Linux] Суперпользователь.

При необходимости измените другие параметры конфигурации сценария.

Создание планов резервного копирования

Чтобы создать резервную копию базы данных Oracle, создайте один или несколько планов резервного копирования. Один из них является обязательным: сначала создается полная резервная копия RMAN, затем создается полная резервная копия полученных файлов в другое хранилище. Другой план является дополнительным: сначала создается резервная копия архивированных журналов RMAN, затем создается инкрементная резервная копия полученных файлов в том же самом хранилище и с таким же именем файла, как и у полной резервной копии. Используйте второй план для резервного копирования архивированных журналов чаще, чем для создания резервной копии базы данных.

Прежде чем приступить к созданию резервных копий архивированных журналов, сначала необходимо создать полную резервную копию RMAN. Пока не будет создана полная резервная копия, невозможно будет восстановить базу данных. Если по расписанию первым запускается инкрементное резервное копирование, запустите перед ним создание полной резервной копии вручную.

Порядок создания плана резервного копирования для полных резервных копий

Следуйте указанным ниже инструкциям:

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**. Выберите папку для хранения резервных копий RMAN.
2. В разделе **Расписание** → **Схема резервного копирования** выберите **Всегда полное** или **Пользовательская**.
3. Укажите расписание резервного копирования. Если выбрана схема резервного копирования **Пользовательская**, укажите в этом разделе только расписание полного резервного копирования.

   Рекомендуем создавать полные резервные копии один раз в неделю.
4. В разделе параметров резервного копирования выполните следующие действия:

   1. Щёлкните **Имя файла резервной копии** и измените шаблон измени файла. Не используйте переменные `[Plan ID]` и `[Plan name]`.

      Запомните или запишите указанный шаблон, поскольку вам нужно будет задать то же самое значение во втором плане резервного копирования.
   2. Щёлкните **Pre/post-команды**.
   3. Включите переключатель **Выполнение команды до резервного копирования**.
   4. Укажите следующие настройки.

      [В Windows]

      - В поле **Команда** введите `<папка со сценариями>\backup_full_pre.bat`.

- В поле **Рабочая директория** введите `<папка со сценариями>`.

[В Linux]

- В поле **Команда** введите `/<папка со сценариями>/backup_full_pre.sh`.
- В поле **Рабочая директория** введите `/<папка со сценариями>/`.

Порядок создания плана резервного копирования для резервных копий архивированного журнала

Следуйте указанным ниже инструкциям:

1. В области **Элементы для резервного копирования** выберите **Файлы/папки**. Выберите папку для хранения резервных копий RMAN.
2. В области **Место сохранения** выберите то же самое хранилище резервных копий, в котором хранятся полные резервные копии.
3. В разделе **Расписание** → **Схема резервного копирования** выберите **Пользовательская**.
4. Измените расписание резервного копирования для полных резервных копий. Поскольку в этом случае нет необходимости создавать полные резервные копии, они должны быть полностью исключены из расписания.

   Рекомендуем изменить расписание на **По событию в журнале событий Windows** и оставить другие параметры без изменений.
5. Укажите расписание резервного копирования для инкрементных резервных копий.

   Мы рекомендуем создавать инкрементные резервные копии каждый день недели, кроме дня, выбранного для полных резервных копий.
6. В разделе параметров резервного копирования выполните следующие действия:
   1. Щёлкните **Имя файла резервной копии** и укажите такой же шаблон имени файла, который используется для полных резервных копий.
   2. Щёлкните **Pre/post-команды**.
   3. Включите переключатель **Выполнение команды до резервного копирования**.
   4. Укажите следующие настройки.

      #### Windows

      - В поле **Команда** введите `<папка со сценариями>\backup_incr_pre.bat`.
      - В поле **Рабочая директория** введите `<папка со сценариями>`.

Linux

- В поле **Команда** введите `/<папка со сценариями>/backup_incr_pre.sh`.
- В поле **Рабочая директория** введите `/<папка со сценариями>/`.

Резервное копирование сервера

При создании плана защиты сервера с базой данных Oracle следуйте инструкции:

1. Выберите всю машину. В противном случае невозможно будет создать резервную копию с поддержкой приложений.
2. Щёлкните **Резервное копирование приложения** и включите переключатель **Oracle Database**.
3. В разделе параметров резервного копирования выполните следующие действия:
   1. Убедитесь, что параметр **Многотомные моментальные снимки** включен.
   2. [Только для Windows] Убедитесь, что для физических машин включен параметр резервного копирования **Служба теневого копирования томов (VSS)**. Рекомендуем не менять установленное по умолчанию **Автоматически выбирать поставщика моментальных снимков**, если на то нет причин.

   Эти настройки обеспечивают правильную фиксацию и запись базы данных при создании моментального снимка. В результате резервная копия приложения будет полностью согласованной.

Дополнительную информацию о резервном копировании см. в разделе *Резервное копирование*.

Восстановление всего сервера

1. Выполните действия, как описано в разделе *Восстановление машины*.
2. Если за период времени, прошедшего с момента создания резервной копии, с которой выполнено восстановление, есть доступные журналы (например, они могут храниться на отдельном неуправляемом томе или по отдельности в разных местах), после восстановления сервера восстановите их к последнему актуальному состоянию с помощью RMAN.

Восстановление баз данных Oracle с использованием Oracle Explorer

Oracle Explorer может взаимодействовать только с агентом для Oracle, который установлен на том же сервере.

- В Windows Oracle Explorer расположен в папке `%ProgramFiles%\Acronis\OracleExplorer`. Чтобы запустить этот инструмент, можно использовать ярлык, созданный на рабочем столе после установки агента для Oracle.

- В Linux запустите `/usr/lib/Acronis/OracleExplorer/oracle_explorer.sh`.

Oracle Explorer восстанавливает данные Oracle в два этапа. На первом этапе восстанавливаются требуемые файлы Oracle (файлы данных, файл параметров сервера, контрольный файл и архивированные журналы) из резервной копии с поддержкой приложений или из резервной копии базы данных. Если эти файлы не нужно восстанавливать, этот шаг можно пропустить. Затем инструмент вызывает команду восстановления RMAN, которая применяет журналы отката и выполняет другие операции, чтобы привести базу данных в нужное состояние.

Порядок восстановления данных Oracle

1. Запустите Oracle Explorer.
2. Выберите хранилище резервных копий. Если потребуется, укажите имя пользователя и пароль для доступа к хранилищу.
3. Выберите резервную копию. Если потребуется, укажите пароль для зашифрованной резервной копии.
4. Выберите точку восстановления и базу данных для восстановления.
5. Выберите файлы Oracle для восстановления из резервной копии. Если эти файлы не нужно восстанавливать, пропустите этот шаг.

   Рекомендуется выбрать табличные пространства и архивированные журналы. При восстановлении контрольного файла необходимо будет создать новое олицетворение базы данных. При восстановлении файла параметров сервера будут утрачены изменения, внесенные в параметры экземпляра после создания резервной копии.

   Если выбран вариант восстановления журналов архива, выберите журналы для восстановления.

   Файлы Oracle всегда будут восстанавливаться в исходное хранилище и перезаписываться.
6. [Необязательно] Выберите параметры восстановления:
   - Момент времени, по состоянию на который будет восстанавливаться база данных.

     Это может быть восстановление до последнего доступного состояния (полное восстановление) или восстановление до момента времени в прошлом (неполное восстановление). Такой момент времени указывается через дату и время из интервала между точкой восстановления, выбранной раньше, и текущим моментом или через номер системного изменения (SCN).
   - Определяет, открывать ли базу данных после восстановления.

     Не открывайте базу данных, если вы планируете выполнять ручные операции восстановления, используя RMAN.

- Определяет, сбрасывать ли журналы.

  Этот параметр необходимо использовать с осторожностью, поскольку при сбросе журналов отката создается новое олицетворения базы данных. Это может обусловить ограничения для отката базы данных к предыдущему олицетворению.

- Учетная запись, с которой выполняется восстановление.
- Файлы базы данных также можно восстановить без запуска операции восстановления RMAN, если вы планируете выполнить восстановление позже.

Далее в этом разделе описан ряд основных сценариев восстановления с рекомендуемыми параметрами, которые можно выбрать в каждом случае.

Восстановление до последнего состояния

Используйте эту процедуру, если файлы данных потеряны или повреждены, а также при сбоях базы данных, относящихся к другим типам. Предполагается, что контрольный файл и файл параметров сервера рабочие.

Этот сценарий также можно использовать, чтобы привести базу данных в актуальное состояние после восстановления всего сервера с более старой резервной копии на уровне диска.

В этом сценарии при необходимости выберите **Табличные пространства** и **Журналы архива**. В параметрах восстановления выберите **Восстановить к последнему доступному состоянию**, не снимайте флажок **Открыть базу данных после восстановления** и не устанавливайте флажок **Сбросить журналы**.

Восстановление по состоянию на более ранний момент времени

Используйте эту процедуру, когда база данных функционирует должным образом, но вам нужно откатить ее к предыдущему состоянию.

В этом сценарии при необходимости выберите **Табличные пространства** и **Журналы архива**. В параметрах восстановления выберите **Восстановить на момент времени** или **Восстановить до номера системного изменения (SCN)**; укажите дату и время или SCN, по состоянию на которые необходимо восстановить базу данных; не снимайте флажок **Открыть базу данных после восстановления** и установите флажок **Сбросить журналы**.

Восстановление данных Oracle с помощью сценариев

Восстановление резервной копии RMAN из резервной копии на уровне файлов

Выполните эту операцию в следующих ситуациях:

- Последняя резервная копия RMAN потеряна или повреждена.
- Необходимо восстановить базу данных до состояния на предыдущий момент времени.

Порядок восстановления:

Выполните действия, как описано в разделе *Восстановление файлов с помощью веб-интерфейса*.

Восстановление данных Oracle с резервной копии RMAN

Аварийное восстановление базы данных Oracle

Этот метод применяется для восстановления всего сервера или диска, на котором установлена Oracle Database при отсутствии ее резервной копии на уровне дисков. Этот метод делает базу данных согласованной с состоянием резервной копии RMAN.

Порядок восстановления:

1. Переустановите операционную систему или перейдите на другой сервер, который работает надлежащим образом. Если операционная система работает нормально, пропустите этот шаг.
2. Переустановите Oracle Database.
3. Создайте новую базу данных с тем же именем и в том же месте, как и та, которую необходимо восстановить.
4. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.
5. [В Windows] В командной строке введите `cd <папка расположения сценариев>`.

   [В Linux] В терминале введите `cd /<папка расположения сценариев>`.
6. Запустите файл `restore_disaster.bat` (в Windows) или `restore_disaster.sh` (в Linux).

Полное восстановление базы данных

Используйте этот метод, если база данных не работает или повреждена после создания последней резервной копии. Чтобы воспользоваться этим методом, контрольный файл и файл параметров сервера должны быть неповрежденными.

Порядок восстановления:

1. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе.

При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.

2. [В Windows] В командной строке введите `cd <папка расположения сценариев>`.

   [В Linux] В терминале введите `cd /<папка расположения сценариев>`.

3. Запустите файл `restore_datafiles.bat` (в Windows) или `restore_datafiles.sh` (в Linux).

Восстановление контрольного файла

Используйте этот метод, если контрольный файл потерян или поврежден после создания последней резервной копии.

Порядок восстановления:

1. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.

2. [В Windows] В командной строке введите `cd <папка расположения сценариев>`.

   [В Linux] В терминале введите `cd /<папка расположения сценариев>`.

3. Запустите файл `restore_controlfile.bat` (в Windows) или `restore_controlfile.sh` (в Linux).

4. Создайте полную резервную копию.

   При восстановлении контрольного файла журналы сбрасываются, поэтому следующая резервная копия должна быть полной.

Восстановление по состоянию на настраиваемый момент времени (неполное восстановление)

Этот метод позволяет восстановить базу данных на настраиваемый момент времени (Point-in-Time Recovery, PITR). Этот момент времени можно указать следующими способами:

- Точная дата и время. Доступный диапазон от момента создания резервной копии RMAN до текущего момента.
- Номер системного изменения (SCN). Доступный диапазон от времени, записанного в файле `scn.in` до последнего значения времени, доступного в архивированных журналах.

  Файл `scn.in` хранится в папке с резервными копиями RMAN. Как правило, SCN в этом файле несет информацию о моменте времени последней резервной копии.

Чтобы узнать последнее значение SCN из архивированных журналов, выполните следующие действия:

1. В командной строке (в Windows) или в терминале (в Linux) введите `sqlplus / as sysdba`, чтобы войти в Oracle.
2. Введите `select max(next_change#)-1 from v$archived_log;`

Порядок восстановления:

1. Восстановите нужную резервную копию RMAN из резервной копии на уровне файлов, как описано ранее в этом разделе. Это приведет к перезаписи файла `scn.in`.

   При выполнении восстановления с самой последней резервной копии RMAN, которая не повреждена, пропустите этот шаг.

2. [В Windows] В командной строке введите `cd <папка расположения сценариев>`.

   [В Linux] В терминале введите `cd /<папка расположения сценариев>`.

3. Выполните любое из следующих действий:

   - Чтобы выполнить восстановление на определенный момент времени, запустите `restore_to-point-in-time.bat <момент времени>` (в Windows) или `restore_to-point-in-time.sh<момент времени>` (в Linux).

     Переменная `<момент времени>` должна быть указана в следующем формате: `yyyy-mm-dd:hh24:mi:ss`.

   - Чтобы выполнить восстановление по состоянию на определенный SCN, запустите `restore_to-scn.bat <SCN>` (в Windows) или `restore_to-scn.sh <SCN>` (в Linux).

   Если дата и время (SCN) не указаны, восстановление выполняется на момент времени, который определен номером SCN, указанным в файле `scn.in`.

4. Создайте полную резервную копию.

   При неполном восстановлении журналы сбрасываются, поэтому следующая резервная копия должна быть полной.

Защита баз данных PostgreSQL

Кибер Бэкап поддерживает резервное копирование экземпляров (instances) PostgreSQL, Postgres Pro, кластеров СУБД Jatoba (JaDog) и баз данных PostgreSQL на основе Patroni.

Вы можете выполнять резервное копирование следующих баз данных и кластеров PostgreSQL (перечень поддерживаемых версий см. в разделе *Поддерживаемые СУБД*):

- PostgreSQL;
- PostgreSQL для 1C;
- Postgres Pro Standard;
- Postgres Pro Enterprise;
- Patroni;
- Platform V Pangolin SE (требуются дополнительные настройки на машине с агентом, подробнее см. статью базы знаний);
- Proxima DB;
- СУБД Jatoba;
- JaDog (Jatoba);
- СУБД Tantor;
- Arenadata Prosperity.

Условия для резервного копирования

- Для резервного копирования баз данных PostgreSQL понадобятся установленные и настроенные продукты:
  - Кибер Бэкап 15 или новее с лицензией ”Кибер Бэкап для СУБД PostgreSQL” на каждый экземпляр PostgreSQL, резервное копирование которого вы планируете выполнять (список лицензий см. в разделе *Издания и лицензии Кибер Бэкап*). Одна лицензия для PostgreSQL распространяется на один экземпляр или на один кластер (Jatoba (JaDog), Patroni).
  - PostgreSQL.
- Для выполнения резервного копирования нужно установить агент Кибер Бэкап для операционной системы, которую вы используете (агент для Windows или агент для Linux), а также агент для PostgreSQL. Перечень версий поддерживаемых ОС приведён в разделе *Поддерживаемые операционные системы*.
- Резервное копирование кластеров СУБД Jatoba (JaDog) поддерживается в Кибер Бэкап начиная с версии 19.0.
- Резервное копирование кластеров Jatoba (JaDog) поддерживается только для агента для Linux.
- Объем ОЗУ машины, на которую будет установлен агент для PostgreSQL, должен составлять не менее 4 ГБ.

Возможности

1. Кибер Бэкап поддерживает следующие виды резервного копирования:
   - полное резервное копирование;
   - инкрементное резервное копирование;
   - резервное копирование журнала транзакций.

   Примечание

   До версии 18.5 в Кибер Бэкап под инкрементным резервным копированием понималось резервное копирование журнала транзакций. Начиная с версии 18.5 инкрементное резервное копирование основано на отслеживании фактических изменений в файлах баз данных. Резервное копирование журнала транзакций выделено в отдельную схему.

   Полное резервное копирование означает резервное копирование кластеров с базами данных. На одном сервере может быть несколько кластеров.

   Примечание

   При резервном копировании данные сразу записываются в целевое хранилище резервных копий. Промежуточное хранение предварительных данных на источнике не используется.

2. Кибер Бэкап поддерживает в качестве хранилищ резервных копий:
   - локальные папки;
   - сетевые папки;
   - NFS;
   - SFTP;
   - узлы хранения;
   - ленты.
3. Кибер Бэкап поддерживает следующие варианты расписания резервного копирования:
   - всегда полное;
   - еженедельно полное, ежедневно инкрементное;
   - еженедельно полное, ежедневно журнал транзакций;

- еженедельно полное, ежедневно инкрементное, ежечасно журнал транзакций;
- другое (пользовательская схема).

Подробнее о схемах см. подраздел ”Схемы резервного копирования” в разделе *Резервное копирование PostgreSQL*.

4. Кибер Бэкап поддерживает следующие варианты восстановления PostgreSQL:
   - восстановление экземпляра PostgreSQL в виде файлов;
   - подключение экземпляра PostgreSQL из архива;
   - восстановление отдельных баз данных в dump-файлы, исходные или новые базы данных;
   - восстановление отдельных баз данных на определенный момент времени (Point-in-Time Recovery, PITR).
5. Кибер Бэкап поддерживает режим повышенной производительности (многопоточности) для резервного копирования:
   - отдельных экземпляров PostgreSQL;
   - кластеров Jatoba (JaDog);
   - кластеров баз данных на основе Patroni.

   Этот режим можно включить при создании плана резервного копирования. Подробнее об этом см. в разделах *Резервное копирование PostgreSQL* и *Многопоточность*.

Предварительная настройка PostgreSQL

Создание учетной записи пользователя на сервере PostgreSQL

Создайте учетную запись пользователя на сервере PostgreSQL, с помощью которой Кибер Бэкап будет подключаться к PostgreSQL.

Учетная запись должна обладать привилегией SUPERUSER.

Например, можно использовать команду:

```
CREATE USER <replicator> SUPERUSER PASSWORD <password>
```

Где:

- `<replicator>` — имя учетной записи;
- `<password>` — пароль учетной записи.

Если планируется работать с кластером PostgreSQL, то на всех узлах кластера должна быть создана

учетная запись с одинаковым именем и паролем.

Примечание

В случае изменения данных этой учетной записи на сервере PostgreSQL, для корректного обновления данных в конфигурационных файлах Кибер Бэкап рекомендуется использовать специальную утилиту (см. раздел *Известные проблемы и их решения*).

Настройка аутентификации в PostgreSQL

Чтобы настроить соединение между Кибер Бэкап и PostgreSQL, внесите изменения в конфигурационные файлы `postgresql.conf` и `pg_hba.conf`. По умолчанию конфигурационные файлы находятся в каталоге с данными кластера базы данных.

Настройка конфигурационного файла postgresql.conf

Добавьте в файл `postgresql.conf` параметр `listen_addresses` и укажите, с каких адресов (агентов) возможно подключение к экземпляру PostgreSQL, например:

```
listen_addresses = 0.0.0.0
```

За более подробной информацией о параметре `listen_addresses` обратитесь к официальной документации PostgreSQL (например, параметры подключений).

Настройка конфигурационного файла pg_hba.conf

Укажите в файле `pg_hba.conf` параметры аутентификации с помощью новых записей.

Каждая запись в `pg_hba.conf` обозначает тип соединения, диапазон IP-адресов клиента (если он соотносится с типом соединения), имя базы данных, имя пользователя и способ аутентификации, который будет использован для соединения. Первая запись с подходящими параметрами применяется для аутентификации пользователя.

Значения полей:

TYPE

Тип подключения. Значение `local` управляет подключениями через Unix-сокеты. Без подобной записи подключения через Unix-сокеты невозможны. Значение `host` управляет подключениями, устанавливаемыми по TCP/IP.

DATABASE

Определяет, каким именам баз данных соответствует эта запись. Значение `all` определяет, что подходят все базы данных. Значение`replication` показывает, что запись соответствует, если

запрашивается подключение для физической репликации (имейте в виду, что для таких подключений не выбирается какая-то конкретная база данных). Несколько имён баз данных можно указать, разделяя их запятыми. Файл, содержащий имена баз данных, можно указать, поставив знак @ в начале его имени.

USER

Указывает, какому имени (или именам) пользователя базы данных соответствует эта запись. Значение `all` показывает, что запись соответствует всем пользователям. Несколько имён пользователей можно указать, разделяя их запятыми. Файл, содержащий имена пользователей, можно указать, поставив знак @ в начале его имени.

ADDRESS

Указывает адрес (или адреса) клиентской машины, которым соответствует данная запись. Это поле может содержать имя компьютера, диапазон IP-адресов или одно из ключевых слов.

Диапазон IP-адресов указывается в виде начального адреса диапазона, дополненного косой чертой (/) и длиной маски CIDR. Длина маски задаёт количество старших битов клиентского IP-адреса, которые должны совпадать с битами IP-адреса диапазона. Биты, находящиеся правее, в указанном IP-адресе должны быть нулевыми. Между IP-адресом, знаком / и длиной маски CIDR не должно быть пробельных символов.

METHOD

Метод-аутентификации.

Чтобы к PostgreSQL можно было подключаться с логином и паролем, укажите значение `md5`.

Для учетной записи пользователя PostgreSQL, с помощью которой происходит соединение с программой Кибер Бэкап (см. раздел *Предварительные требования*), укажите метод аутентификации `trust`.

За более подробной информацией о конфигурационном файле `pg_hba.conf` обратитесь к официальной документации PostgreSQL (например, файл pg_hba.conf).

Примеры записей

Записи для подключения агента с этого же сервера по адресу 127.0.0.1 для пользователя replicator:

```
# TYPE   DATABASE      USER         ADDRESS        METHOD
  host   all           replicator   127.0.0.1/32   trust
  host   replication   replicator   127.0.0.1/32   trust
```

Записи для подключения агента с другого сервера с адресом 10.10.10.100 для любого пользователя локальной системы по TCP/IP:

```
# TYPE   DATABASE      USER   ADDRESS           METHOD
  host   all           all    10.10.10.100/32   md5
  host   replication   all    10.10.10.100/32   md5
```

Пример файла `pg_hba.conf` с необходимыми записями:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     peer
# IPv4 local connections:
host    all             replicator      127.0.0.1/32            trust
host    all             all             0.0.0.0/0               md5
host    all             all             127.0.0.1/32            ident
# IPv6 local connections:
host    all             all             ::1/128                 ident
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication     all                                     peer
host    replication     replicator      127.0.0.1/32            trust
host    replication     all             0.0.0.0/0               md5
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 ident
```

Важно

Для настройки аутентификации при переходе с версии Кибер Бэкап 15 Обновление 2.6 или Кибер Бэкап Обновление 2.7 на Кибер Бэкап 16 обратитесь к разделу *Известные проблемы и их решения*.

После внесения изменений в файлы конфигурации перезапустите службу PostgreSQL:

```
systemctl restart postgresql
```

Установка и настройка агента для PostgreSQL

Установка и настройка включает в себя следующие шаги:

1. Установка агента для PostgreSQL и агента Кибер Бэкап для операционной системы, которую вы используете (Windows или Linux).
2. Добавление в веб-консоли Кибер Бэкап устройства PostgreSQL.

Установка агента для PostgreSQL

Агент для PostgreSQL может быть установлен как на сервер, на котором находятся базы данных PostgreSQL, так и на другую машину.

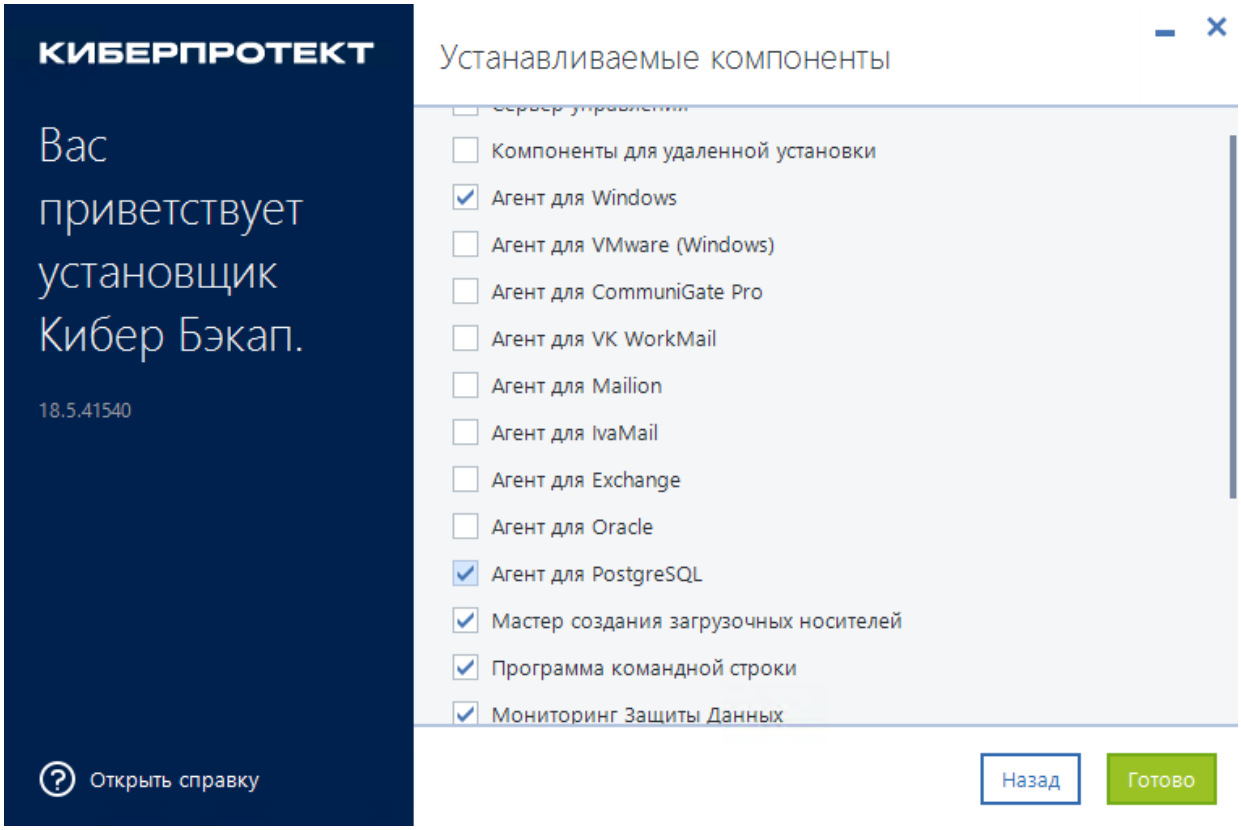
Если вы устанавливаете агент для PostgreSQL на другую машину:

1. Убедитесь, что машина с агентом и сервер PostgreSQL смогут обмениваться данными по сети. Откройте необходимые порты, настройте соединение, если требуется — настройте прокси-сервер.
2. На сервере PostgreSQL разрешите локальные входящие соединения типа replication.
3. Для гранулярного восстановления баз данных PostgreSQL на машине с агентом должен быть установлен экземпляр PostgreSQL той же версии, что и восстанавливаемый.
4. Обратите внимание, что восстановление экземпляра PostgreSQL в виде файлов возможно только на машину с агентом и в присоединенные к ней сетевые папки (см. раздел *Восстановление экземпляра PostgreSQL в виде файлов*).

Агент для PostgreSQL необходимо устанавливать совместно с агентом для операционной системы, которую вы используете (Windows или Linux).

В этом разделе рассмотрена установка агента для PostgreSQL на машину с ОС Windows. Для установки агента для PostgreSQL на машину с ОС Linux обратитесь к разделу *Установка агентов в ОС Linux вручную*.

1. Запустите установщик Кибер Бэкап.
2. Выберите **Настройка параметров установки**.
3. В блоке **Устанавливаемые компоненты** выберите **Изменить**.
4. Отметьте в списке **Агент для PostgreSQL**.



5. Нажмите **Готово**, затем нажмите **Установка**.

> **Примечание**
>
> Для СУБД Platform V Pangolin также выполните шаги, приведённые в статье базы знаний.

Добавление в веб-консоли Кибер Бэкап устройства PostgreSQL

1. В веб-консоли Кибер Бэкап в разделе **Устройства** нажмите **Добавить** и выберите приложение:
   - Если необходимо добавить сервер PostgreSQL, в блоке **Приложения** выберите **PostgreSQL**.
   - Если необходимо добавить кластер PostgreSQL СУБД Jatoba (JaDog), в блоке **Приложения** выберите **Jatoba**.
   - Если необходимо добавить кластер PostgreSQL на основе Patroni, в блоке **Приложения** выберите **Кластер PostgreSQL Patroni**.
2. В поле выбора агента из выпадающего списка выберите агент развёртывания для PostgreSQL. Выбранный агент будет использоваться для резервного копирования и восстановления данных сервера или кластера PostgreSQL.
3. Укажите настройки соединения с PostgreSQL:

- имя хоста или IP-адрес сервера PostgreSQL;
- порт подключения (по умолчанию для сервера PostgreSQL используется порт 5432, для кластера СУБД Jatoba (JaDog) — порт 54443, для кластера PostgreSQL Patroni — порт 8008);
- имя пользователя учётной записи для подключения к PostgreSQL;
- пароль учётной записи для подключения к PostgreSQL.

Убедитесь, что при настройке *параметров аутентификации* вы настроили метод аутентификации **trust**.

4. [Необязательно] Введите произвольный комментарий.
5. [Для кластера Jatoba (JaDog)] Добавьте следующие сертификаты:
   - клиентский сертификат;
   - приватный ключ клиента;
   - корневой сертификат сервера.

   Примечание

   Поддерживается только протокол TLS.
6. Нажмите кнопку **Добавить**.

В списке устройств отобразится раздел **PostgreSQL** с добавленным сервером или кластером.

Для кластера PostgreSQL в разделе **Сведения** отобразится информация об IP-адресах/именах узлов, доступности (Online/Offline) и статусах узлов (Leader/Replica или Master/Slave).

Методы резервного копирования PostgreSQL

В этом разделе описаны поддерживаемые методы резервного копирования данных PostgreSQL.

Резервное копирование с использованием библиотеки libpgprobackup

Установка библиотеки libpgprobackup

Библиотека libpgprobackup позволяет использовать технологию `probackup3` для резервного копирования экземпляров и кластеров баз данных PostgreSQL версий:

- Postgres Pro Standard 15—18;
- Postgres Pro Enterprise 15—18.

После установки библиотеки libpgprobackup Кибер Бэкап автоматически станет использовать технологию `probackup3` для резервного копирования. Чтобы перейти на резервное копирование с использованием функции создания сводок WAL, на машинах с агентом PostgreSQL удалите библиотеку libpgprobackup.

Для установки библиотеки libpgprobackup выполните следующие действия:

1. Скачайте и установите файлы библиотеки из репозитория PostgreSQL на машину с экземпляром PostgreSQL (на все узлы в случае кластера), например:

   ```
   wget --user <username> --password='<password>' https://repo.postgrespro.ru/pg_probackup3/pg_
   ↪probackup3/keys/pgpro-repo-add.sh
   bash ./pgpro-repo-add.sh
   apt update
   apt install libpb3-encoder
   ```

   где:

   - `<username>` — имя учетной записи с правом на выполнение и правом суперпользователя;
   - `<password>` — пароль от учетной записи;
   - https://repo.postgrespro.ru/pg_probackup3/pg_probackup3/keys/pgpro-repo-add.sh — адрес репозитория PostgreSQL.

2. Добавьте в конфигурационный файл `postgresql.conf` параметры `shared_preload_libraries`, `walsender_plugin_libraries` со значениями `pgpro_bindump`, например:

   ```
   shared_preload_libraries='pgpro_bindump'
   walsender_plugin_libraries=pgpro_bindump
   ```

3. Перезапустите службу PostgreSQL:

   ```
   systemctl restart postgresql
   ```

4. Скачайте и установите файлы библиотеки из репозитория PostgreSQL на все машины с агентами PostgreSQL, которые участвуют в резервном копировании, например:

   ```
   wget --user <username> --password='<password>' https://repo.postgrespro.ru/pg_probackup3/pg_
   ↪probackup3/keys/pgpro-repo-add.sh
   bash ./pgpro-repo-add.sh
   apt update
   apt install libpgprobackup3
   ```

   где:

- `<username>` — имя учетной записи с правом на выполнение и правом суперпользователя;
- `<password>` — пароль от учетной записи;
- https://repo.postgrespro.ru/pg_probackup3/pg_probackup3/keys/pgpro-repo-add.sh — адрес репозитория PostgreSQL.

Отключение режима резервного копирования с библиотекой libpgprobackup

1. На машинах с агентом PostgreSQL удалите библиотеку libpgprobackup:

```
apt remove libpgprobackup3
```

2. Перезапустите службы aakore и агента PostgreSQL:

```
systemctl restart aakore.service acronis_mms.service
```

Резервное копирование с использованием функции создания сводок WAL

Создание сводок WAL (WAL summarization) — это встроенная функция СУБД PostgreSQL, которая позволяет ускорить создание инкрементных резервных копий.

Для работы и использования функции необходимы:

- Кибер Бэкап версии 19.0 или новее;
- PostgreSQL версии 17 или новее.

Чтобы включить функцию, выполните следующие действия на сервере PostgreSQL:

1. Запустите команду:

```
sudo -u postgres psql -c ”ALTER SYSTEM SET summarize_wal = 'on';” -c ”SELECT pg_reload_
↪conf();”
```

2. Убедитесь, что запустился процесс walsummarizer:

```
ps -u postgres -f | grep walsummarizer
```

После включения функции инкрементные резервные копии будут создаваться на основе сводок WAL.

Особенности использования функции:

- После включения функции создания сводок WAL будет создана полная резервная копия, даже если согласно расписанию плана резервного копирования должна быть создана инкрементная.
- Если установлена и настроена *библиотека libpgprobackup*, то именно она будет использоваться

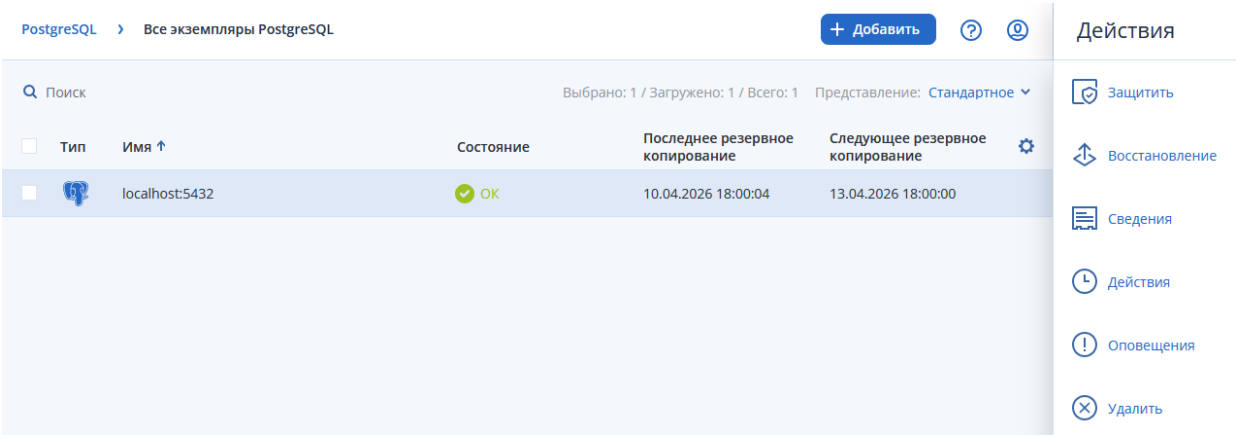
для выполнения резервного копирования (в том числе и для создания инкрементных резервных копий), даже если включена функция создания сводок WAL.

> **Примечание**
>
> Библиотека libpgprobackup версии 3.4.1 или более ранней не поддерживает функцию создания сводок WAL. Сведения о поддержке функции в более поздних версиях см. в документации библиотеки.

Резервное копирование PostgreSQL

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** → **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который вы хотите защитить.
3. Перейдите на вкладку справа **Защитить**.

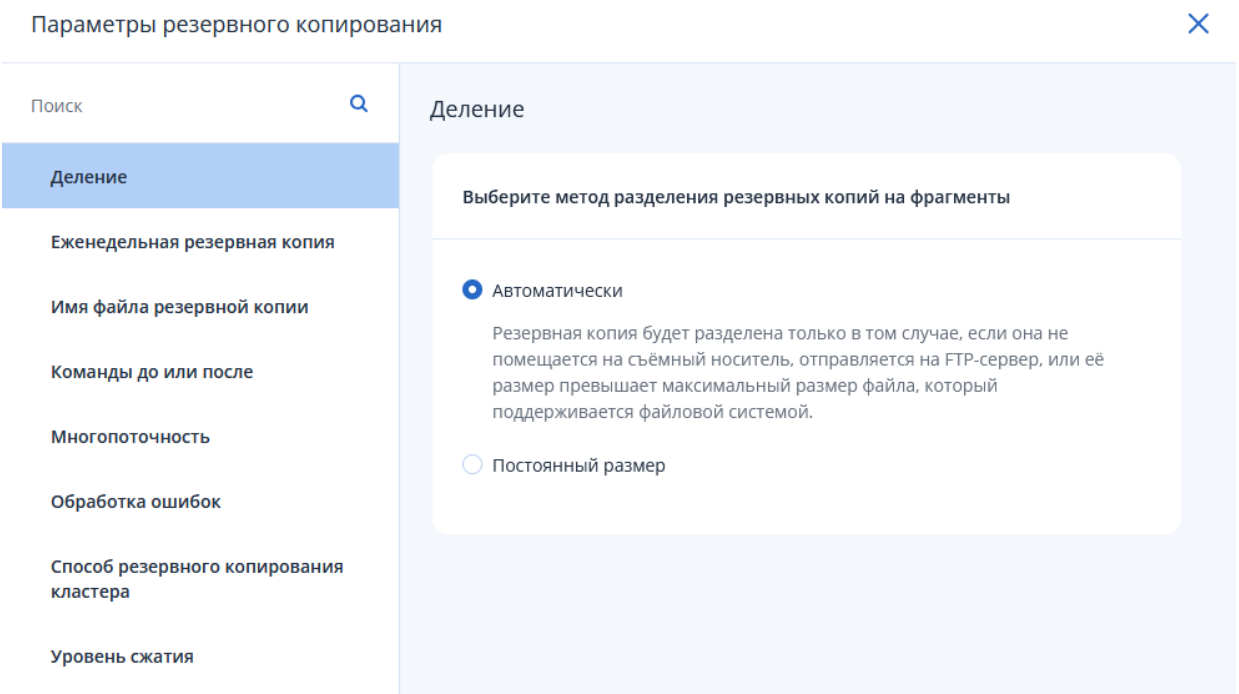


4. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.

   Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

5. В поле **Расписание** укажите схему и периодичность выполнения резервного копирования. Подробнее о расписании см. в разделе *Расписание*. В текущей версии доступны полное резервное копирование, инкрементное резервное копирование и резервное копирование журнала транзакций. Подробнее о схемах см. далее подраздел ”Схемы резервного копирования”.
6. В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища. Подробнее см. в разделе *Правила хранения*.

7. При необходимости защитите резервные копии паролем. Подробнее см. в разделе *Защита паролем*.
8. [Необязательно] В поле **Параметры резервного копирования** нажмите **Изменить** и укажите следующие параметры:
   - **Деление**. Выберите метод разделения резервных копий на меньшие по размеру фрагменты.
   - **Еженедельная резервная копия**. Укажите день недели для создания еженедельной копии.
   - **Имя файла резервной копии**. Укажите шаблон для наименований файлов резервных копий.
   - **Команды до или после**. Укажите команды, которые должны выполняться перед резервным копированием или после него.
   - **Многопоточность**. Выберите вариант использования многопоточности.
   - **Обработка ошибок**. Укажите порядок обработки ошибок, возникающих при резервном копировании.
   - **Способ резервного копирования кластера**. Подробнее см. в разделе *Способ резервного копирования кластера*.
   - **Управление лентами**. Укажите порядок записи резервных копий на ленточные устройства.
   - **Уровень сжатия**. Укажите уровень сжатия данных при резервном копировании.



   Подробнее см. в разделе *Параметры резервного копирования*.
9. Нажмите **Применить**. Новый план защиты появится в списке планов.

В результате вы сможете:

- выполнять резервное копирование баз данных PostgreSQL;
- выполнять восстановление баз данных PostgreSQL из резервных копий.

Схемы резервного копирования

> **Примечание**
>
> Начиная с версии 18.5 в Кибер Бэкап для инкрементного резервного копирования требуется, чтобы агент располагался на одной машине с экземпляром PostgreSQL.

В Кибер Бэкап для PostgreSQL реализованы следующие схемы резервного копирования:

- **Всегда полное**. При этой схеме всегда выполняется полное резервное копирование.
- **Еженедельно полное, ежедневно инкрементное**. В версиях Кибер Бэкап ранее 18.5 в этой схеме вместо инкрементного резервного копирования выполнялось резервное копирование журнала транзакций. Если агент для PostgreSQL установлен на машине, на которой нет баз данных, то резервное копирование всегда будет полным.
- **Еженедельно полное, ежедневно журнал транзакций**. Эта схема в версии Кибер Бэкап ранее 18.5 называлась **Еженедельно полное, ежедневно инкрементное**.
- **Еженедельно полное, ежедневно инкрементное, ежечасно журнал транзакций**. Эта схема доступна начиная с версии Кибер Бэкап 18.5. Если агент для PostgreSQL установлен на машине, на которой нет баз данных, вместо инкрементного резервного копирования будет совершаться полное.
- **Другое**. Эта схема является пользовательской.

> **Примечание**
>
> Инкрементное резервное копирование выполняется только для экземпляров PostgreSQL. Для кластеров Jatoba (JaDog) и Patroni этот тип резервного копирования недоступен.

Особенности использования

- Если выполнить обновление сервера управления, это приведет к следующим изменениям:
  - схема резервного копирования **Еженедельно полное, ежедневно инкрементное** сменит свое название на **Еженедельно полное, ежедневно журнал транзакций**;

    - в интерфейсе веб-консоли **Хранилища резервных копий** названия резервных копий **Инкрементное** останутся неизменными;
    - в схеме резервного копирования **Другое** изменится название с **Инкрементное резервное копирование** на **Резервное копирование журналов транзакций**;
    - при дальнейших запусках **Журнал транзакций** будет отображаться в резервных копиях как **Инкрементальное** (новый тип резервного копирования не будет поддерживаться).
- Если выполнить обновление агента, это приведет к следующим изменениям:
    - все старые инкрементные резервные копии останутся с названием **Инкрементное**;
    - при первом запуске схемы **Журнал транзакций** будет выполнено полное резервное копирование; при последующих запусках будет выполняться резервное копирование по схеме **Журнал транзакций**.
- Если *правилами хранения* установлены такие сроки хранения, при которых резервные копии должны быть удалены, одна резервная копия журнала транзакций всё равно сохранится.
- После смены лидера в кластере Patroni следующее резервное копирование будет полным.

Что дальше

- *Подключение экземпляра PostgreSQL из архива*
- *Восстановление экземпляра PostgreSQL в виде файлов*
- *Гранулярное восстановление баз данных PostgreSQL*

Восстановление баз данных PostgreSQL

Восстановление всех поддерживаемых версий баз данных PostgreSQL, развернутых в простой или кластерной конфигурации (Jatoba (JaDog), Patroni), происходит по единым сценариям, приведенным в этом разделе.

Кибер Бэкап поддерживает следующие варианты восстановления баз данных:

- *Восстановление экземпляра PostgreSQL в виде файлов*.
- *Подключение экземпляра PostgreSQL из архива*.
- *Гранулярное восстановление баз данных PostgreSQL*.

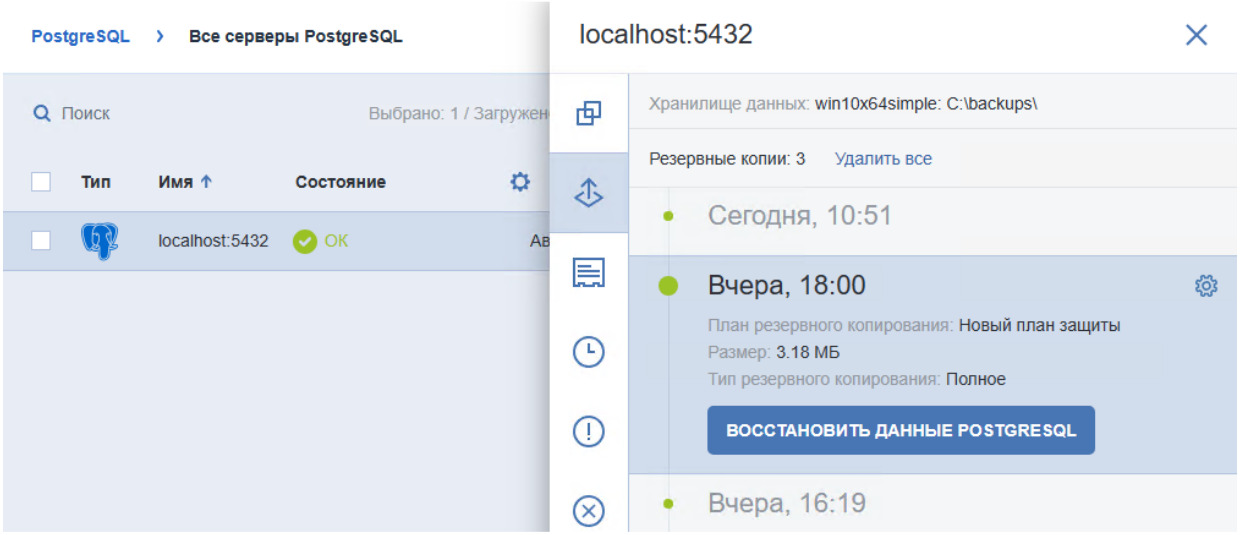
Восстановление экземпляра PostgreSQL в виде файлов

Для восстановления всего экземпляра PostgreSQL в виде файлов:

1. Перейдите в **Устройства** → **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно восстановить.
3. Перейдите на вкладку справа **Восстановление**.

> **Примечание**
>
> Либо перейдите в **Хранилища резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Выберите нужную копию для восстановления и нажмите **Восстановить данные PostgreSQL**.



5. Выберите архив и нажмите справа **Восстановить как файлы**.
6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Выберите место для восстановления файлов. Возможные варианты: локальные папки машины, на которой установлен агент, и присоединенные к ней сетевые папки.
8. Проверьте остальные настройки и нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

После успешного восстановления на машине под управлением ОС Windows необходимо подключить восстановленные файлы к PostgreSQL, как описано в статье Подключение баз данных PostgreSQL после восстановления.

Подключение экземпляра PostgreSQL из архива

Подключение экземпляра PostgreSQL из архива может понадобиться для просмотра содержимого резервной копии или других операций с базой данных средствами PostgreSQL.

Предварительные требования:

- На машине с агентом PostgreSQL и на сервере PostgreSQL, которому принадлежит резервная копия, должны совпадать операционная система, версия и редакция PostgreSQL.
- На машине с агентом PostgreSQL в конфигурационном файле `/opt/acronis/var/dsp.database.pg/postgresql-agent.json` в секции `server > recovery_instance > binaries` необходимо указать путь к исполняемым файлам PostgreSQL. Например:

```
”recovery_instance”: {
    ”run_as_user”: ”postgres”,
    ”binaries”: [”/usr/pgsql-15/bin/postgres”]
}
```

  Далее перезапустите службу агента PostgreSQL:

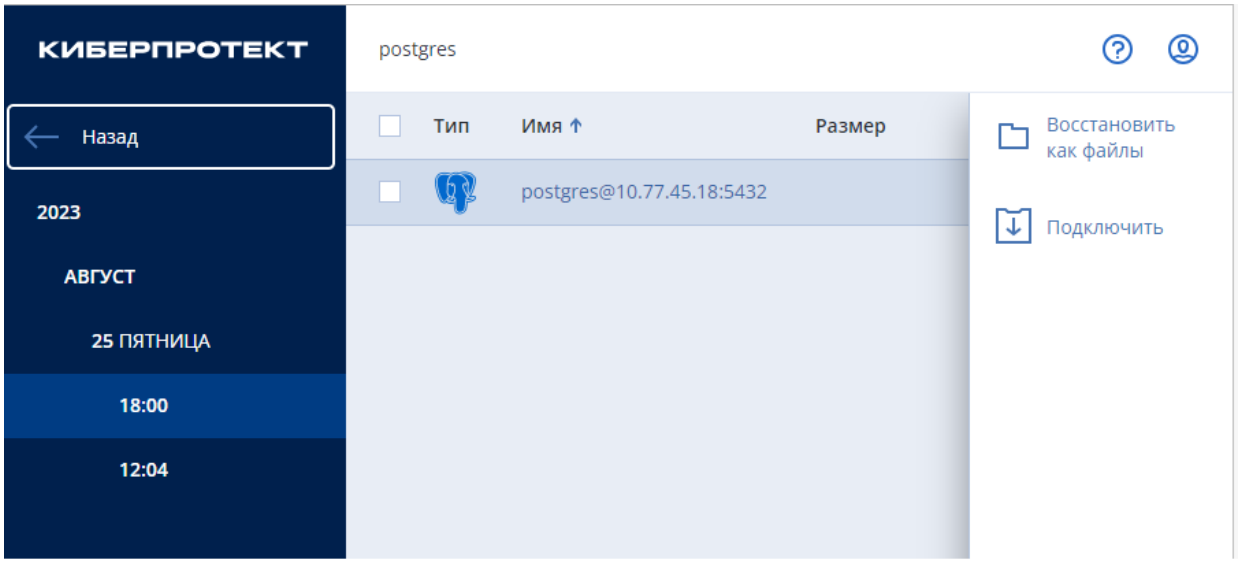
```
systemctl restart aakore
systemctl restart acronis_mms
```

Для подключения экземпляра PostgreSQL из архива:

1. Перейдите в **Устройства** → **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно подключить.
3. Перейдите на вкладку справа **Восстановление**.

> **Примечание**
>
> Либо перейдите в **Хранилища резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Выберите нужный архив для подключения и нажмите **Восстановить данные PostgreSQL**.
5. Выберите архив и нажмите справа **Подключить**.



6. Проверьте настройки и нажмите **Монтировать**.
7. Подключитесь к восстановленной базе данных и совершите необходимые действия средствами PostgreSQL.
8. Перейдите в **Панель Мониторинга** → **Действия** и выберите операцию подключения базы данных. Прервите подключение архива базы данных.

Что дальше

- *Восстановление экземпляра PostgreSQL в виде файлов*
- *Гранулярное восстановление баз данных PostgreSQL*

Гранулярное восстановление баз данных PostgreSQL

Гранулярное восстановление доступно только для баз данных PostgreSQL, установленных на машинах под управлением ОС Linux. Доступно восстановление отдельных баз данных из единого архива резервной копии.

Восстановление на определенный момент времени (Point-in-Time Recovery, PITR) доступно только для резервных копий журналов транзакций.

Предварительные требования:

- На машине с агентом PostgreSQL и на сервере PostgreSQL, которому принадлежит резервная копия, должны совпадать операционная система, версия и редакция PostgreSQL.
- На машине с агентом PostgreSQL в конфигурационном файле `/opt/acronis/var/dsp.database.pg/postgresql-agent.json` в секции `server > recovery_instance >`

`binaries` необходимо указать путь к исполняемым файлам PostgreSQL. Например:

```
”recovery_instance”: {
    ”run_as_user”: ”postgres”,
    ”binaries”: [”/usr/pgsql-15/bin/postgres”]
}
```

Далее перезапустите службу агента PostgreSQL:

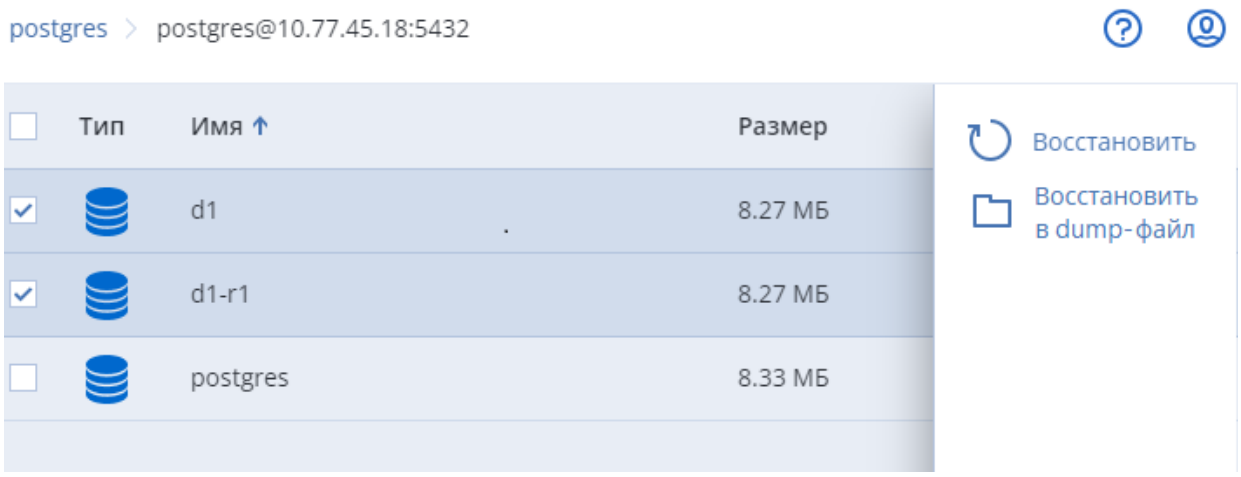
```
systemctl restart aakore
systemctl restart acronis_mms
```

Для восстановления отдельных баз данных PostgreSQL:

1. Перейдите в **Устройства** → **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, из которого вы хотите восстановить базы данных.
3. Перейдите на вкладку справа **Восстановление**.

> **Примечание**
>
> Либо перейдите в **Хранилища резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

4. Нажмите на имя резервной копии и выберите необходимые для восстановления базы из архива.

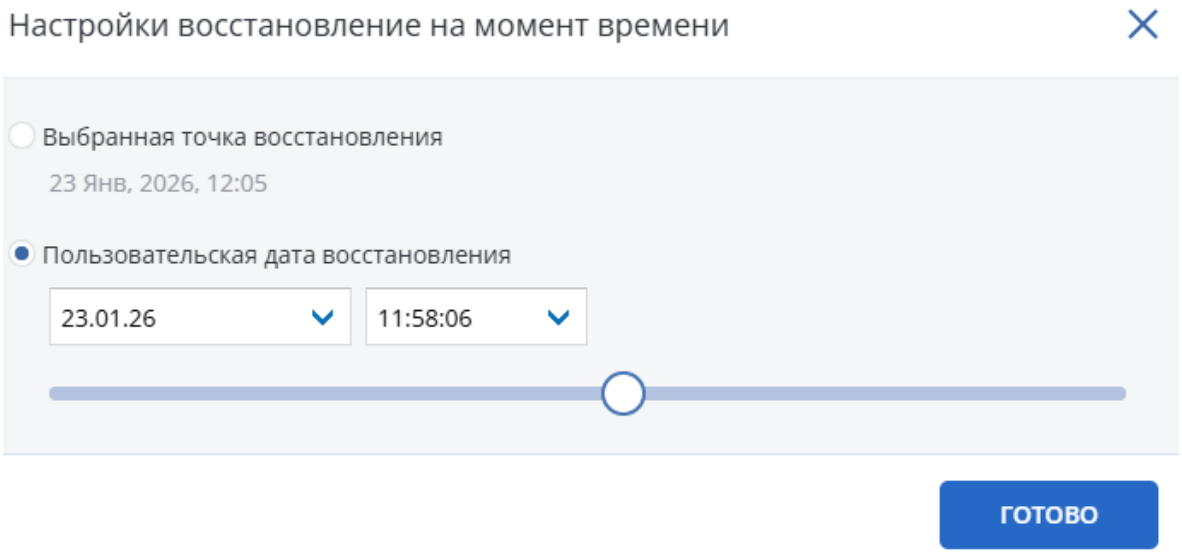


5. Выберите способ восстановления:
   - Если необходимо сразу восстановить выбранные базы из архива, нажмите справа **Восстановить**.
   - Если необходимо сохранить выбранные базы из архива в отдельные dump-файлы, нажмите

справа **Восстановить в dump-файл**.

6. [Если выбрано восстановление баз из архива] Укажите следующие настройки:

   - Выберите время восстановления. Можно оставить время создания резервной копии или указать время между созданием предыдущей резервной копии и выбранной (PITR).



   - Экземпляр PostgreSQL, куда будет происходить восстановление.

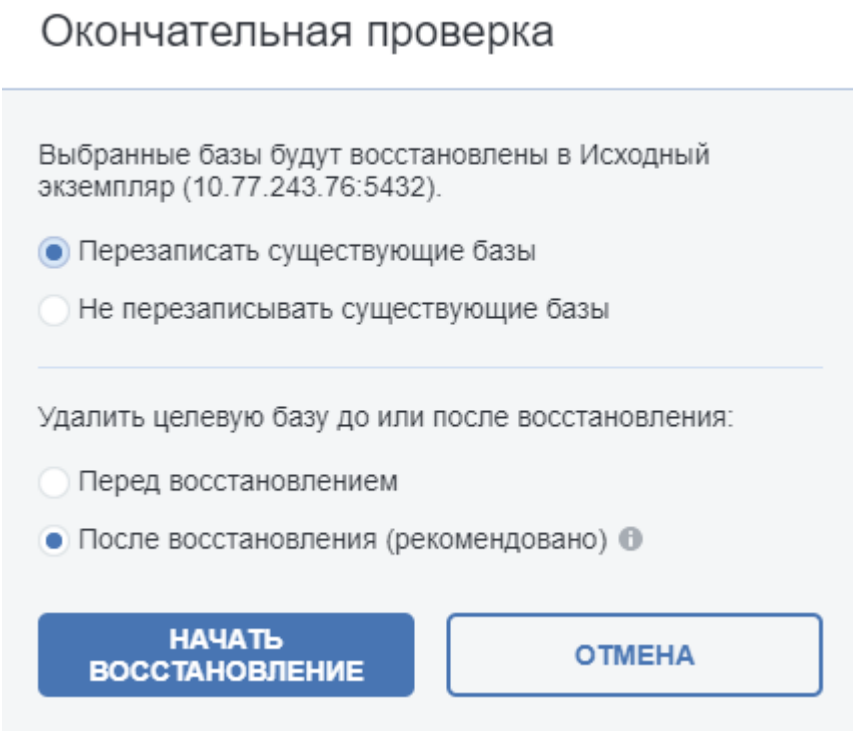
> **Примечание**
>
> Версия экземпляра PostgreSQL, куда будет происходить восстановление, должна быть не ниже восстанавливаемой. Редакции экземпляров PostgreSQL должны совпадать. Экземпляр, созданный из кластеризованного экземпляра, можно восстановить на некластеризованный экземпляр и наоборот.

   - Для каждой выбранной базы из архива укажите место для восстановления. Возможные варианты: в исходную базу, в новую базу.

7. [Если выбрано сохранение баз данных в dump-файлы] Укажите следующие настройки:

   - Выберите время восстановления. Можно оставить время создания резервной копии или указать время между созданием предыдущей резервной копии и выбранной (PITR).
   - Место хранения dump-файлов.

8. Нажмите **Начать восстановление**.
9. [Если выбрано восстановление в исходную базу данных] Укажите порядок восстановления баз данных и нажмите **Начать восстановление**.



Ход выполнения восстановления показан на вкладке **Действия**.

Ограничения

- Не поддерживается полное резервное копирование баз данных PostgreSQL в хранилище под управлением узла хранения с включенной дедупликацией резервных копий.
- Не поддерживается резервное копирование баз данных PostgreSQL в защищенное паролем хранилище под управлением узла хранения.
- Не поддерживается гранулярное восстановление на машинах под управлением ОС Windows.
- Не поддерживается гранулярное восстановление для резервных копий на ленточных накопителях.

Известные проблемы и их решения

Настройка аутентификации

Если вы выполняли настройку аутентификации PostgreSQL в Кибер Бэкап 15 версий Обновление 2.6 или Обновление 2.7 в соответствии с инструкцией в разделе *Предварительная настройка PostgreSQL* и впоследствии перешли на версию Кибер Бэкап 16, резервное копирование PostgreSQL может завершаться с ошибкой.

```
{"error": "FATAL: no pg_hba.conf entry for host "10.77.242.110", user "postgres", database
↪"template1", no encryption (SQLSTATE 28000)","request-id": "bff753db-34f0-4ee9-bbda-d429f45b4ea3
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
↪”,”service”: ”PostgreSQL”,”serviceMsg”: ”FATAL: no pg_hba.conf entry for host ”10.77.242.110”,¬
↪user ”postgres”, database ”template1”, no encryption (SQLSTATE 28000)”}
```

Решение

В пункте IPv4 local connections файла pg_hba.conf укажите настройки так, как показано в следующем примере:

```
host all all 127.0.0.1/32 trust
host all all 0.0.0.0/0 md5
```

После того, как вы изменили настройки, перезапустите PostgreSQL.

Примечание

Укажите ip-адреса в соответствии со своей конфигурацией.

Изменение данных учетной записи пользователя, с помощью которой происходит соединение с PostgreSQL

В некоторых случаях при обновлении Кибер Бэкап или при изменении пароля пользователя средствами PostgreSQL, новый пароль для учетной записи пользователя не обновляется автоматически во всех конфигурационных файлах Кибер Бэкап.

Решение

Для корректного изменения данных учетной записи используйте утилиту, которая устанавливает новые имя пользователя и пароль во всех конфигурационных файлах Кибер Бэкап.

Выполните команду:

```
/usr/lib/Acronis/AMS/postgresql_credentials_changer 'postgres_username' 'postgres_password'
```

Где:

- `postgres_username` — имя учетной записи;
- `postgres_password` — пароль учетной записи.

После успешного изменения данных отображается сообщение ”Successfully changed PostgreSQL credentials in CyberBackup configs”.

Слоты репликации

Резервное копирование по расписанию останавливается с ошибкой после нескольких созданий, запусков по расписанию и удалений планов резервного копирования.

```
ОШИБКА: используются все слоты репликации (SQLSTATE 53400)ОШИБКА: syntax error (SQLSTATE 42601)
```

Решение

Удалите ненужные слоты репликации вручную, используя следующие команды:

- Получить все слоты:

  ```
  select * from pg_replication_slots where slot_name like 'cp%'
  ```

- Удалить слот:

  ```
  select pg_drop_replication_slot('cp_3odiqs5psps0knx0bgjz3g_dsuqc5akrjsnln9fhr6srg')
  ```

Защита данных MySQL и MariaDB

Данные MySQL или MariaDB можно защитить с помощью резервного копирования на уровне дисков с поддержкой приложений. При этом собираются метаданные приложения и обеспечивается детальное восстановление на уровне экземпляра, базы данных или таблицы.

Примечание

Резервное копирование данных MySQL или MariaDB с поддержкой приложений доступно при выборе одного из вариантов лицензии Кибер Бэкап Расширенная.

Защита данных СУБД MySQL и MariaDB поддерживается начиная с версии Кибер Бэкап 15 обновление 2.7.

Поддерживаемые версии MySQL и MariaDB указаны в разделе *Поддерживаемые СУБД*.

Чтобы защитить физическую или виртуальную машину, на которой запущены экземпляры MySQL или MariaDB, с помощью резервного копирования с поддержкой приложений, необходимо установить агент для MySQL/MariaDB на этой машине. Агент для MySQL/MariaDB устанавливается вместе с агентом для Linux.

Загрузка установочного файла агента для Linux:

1. Войдите в веб-консоль Кибер Бэкап.

2. Нажмите на значок учетной записи в правом верхнем углу и затем выберите **Загрузки**.
3. Выберите **Установщик для Linux**.

   Установочный файл будет загружен на ваш компьютер. Чтобы установить агента, выполните действия, как описано в разделе *Установка агентов* или *Автоматическая установка или автоматическое удаление в Linux*. Убедитесь, что вы выбрали параметр **Агент для MySQL/MariaDB**.

Известные проблемы и ограничения

- Кластеры MySQL или MariaDB не поддерживаются.
- Экземпляры MySQL или MariaDB, работающие в контейнерах Docker, не поддерживаются.
- Экземпляры MySQL или MariaDB, работающие в операционных системах, использующих файловую систему BTRFS, не поддерживаются.
- Системные базы данных (`sys`, `mysql`, `information-schema`, и `performance_schema`) и базы данных, которые не содержат никаких таблиц, не могут быть восстановлены в запущенные экземпляры. Однако эти базы данных могут быть восстановлены в виде файлов при восстановлении всего экземпляра.
- Восстановление из резервных копий, хранящихся в Зоне безопасности, не поддерживается.
- Восстановление из резервных копий, расположенных на узлах хранения, не поддерживается.
- Восстановление в целевые базы данных, настроенные с использованием символических ссылок, не поддерживается. Вы можете восстановить резервные копии баз данных как новые базы данных, изменив их имя.
- Если у вас возникли проблемы при восстановлении данных из защищенных паролем общих ресурсов Samba, выйдите из веб-консоли, а затем снова войдите в нее. Выберите нужную точку восстановления, а затем нажмите **Базы данных MySQL/MariaDB**. Не нажимайте **Вся машина** или **Файлы/папки**.

Настройка резервного копирования с поддержкой приложений

Предварительные требования

- На выбранной машине должен быть запущен хотя бы один экземпляр MySQL или MariaDB.
- На компьютере, на котором запущен экземпляр MySQL или MariaDB, агент защиты должен быть запущен от имени пользователя root.
- Резервное копирование с поддержкой приложений доступно только в том случае, если в плане

защиты в качестве источника резервного копирования выбрано **Вся машина**.

- Опция резервного копирования **Sector-by-sector (Посекторно)** должна быть отключена в плане защиты. В противном случае восстановить данные приложения будет невозможно.

Чтобы настроить резервное копирование с поддержкой приложений:

1. В веб-консоли Кибер Бэкап выберите один или несколько компьютеров, на которых запущены экземпляры MySQL или MAriaDB. На каждом компьютере может быть один или несколько экземпляров.
2. Создайте план защиты с включенным модулем резервного копирования.
3. В разделе **Выбор данных** выберите **Вся машина**.
4. Нажмите **Резервное копирование приложения**, а затем включите параметр **Сервер MySQL/MariaDB**.
5. Выберите способ указания экземпляров MySQL или MariaDB:
   - **Для всех рабочих нагрузок**

     Используйте этот параметр, если вы запускаете экземпляры с одинаковыми конфигурациями на нескольких серверах. Для всех экземпляров будут использоваться одни и те же параметры подключения и учетные данные доступа.
   - **Для конкретных рабочих нагрузок**

     Используйте этот параметр, чтобы указать параметры подключения и учетные данные доступа для каждого экземпляра.
6. Для настройки параметров подключения и учетных данных доступа нажмите **Добавить экземпляр**.
   1. Выберите тип соединения, а затем укажите следующие данные:
      - [Для сокета TCP] IP-адрес и порт.
      - [Для сокета Unix] путь к сокету.
   2. Укажите данные учетной записи пользователя, которая имеет следующие привилегии для экземпляра:
      - `FLUSH_TABLES` или `RELOAD` для всех баз данных и таблиц(`\*.*`)
      - `SELECT` для `information_schema.tables`
   3. Нажмите **OK**.
7. Нажмите **Готово**.

Восстановление данных из резервной копии с поддержкой приложений

Из резервной копии с поддержкой приложений можно восстановить экземпляры, базы данных и таблицы MySQL или MariaDB. Также можно восстановить весь сервер, на котором запущены экземпляры, или восстановить файлы и папки с этого сервера.

В таблице ниже приведены все варианты восстановления.

Объект	Данные	Путь
Сервер MySQL Сервер MariaDB	Вся машина	Компьютер[1], на котором установлен агент для Linux
Сервер MySQL Сервер MariaDB	Файлы или папки	Компьютер[1], на котором установлен агент для Linux
Экземпляр	Файлы	Компьютер[1], на котором установлен агент для MySQL/MariaDB
База данных	Та же база данных Новая база данных	Компьютер[1], на котором установлен агент для MySQL/MariaDB • Исходный экземпляр • Другой экземпляр • Исходная база данных • Новая база данных
Таблица	Та же таблица Новая таблица	Компьютер[1], на котором установлен агент для MySQL/MariaDB • Исходный экземпляр • Другой экземпляр • Исходная база данных • Исходная таблица • Новая таблица

Восстановление всего сервера

Чтобы узнать, как восстановить весь сервер, на котором запущены экземпляры MySQL или MariaDB, обратитесь к разделу *Восстановление машины*.

[1] С точки зрения резервного копирования, виртуальная машина с агентом внутри рассматривается как физическая машина.

Восстановление экземпляров

Из резервной копии с поддержкой приложений можно восстановить экземпляры MySQL или MariaDB в виде файлов.

Восстановление экземпляра

Выполните следующие действия:

1. В веб-консоли Кибер Бэкап выберите компьютер, на котором изначально находились данные, которые вы хотите восстановить.
2. Нажмите **Восстановление**.
3. Выберите точку восстановления. Обратите внимание, что точки восстановления отфильтрованы по месторасположению.
4. Если компьютер находится в автономном режиме, точки восстановления не отображаются. Выполните одно из следующих действий:
   - Если местом резервного копирования является облако или общее хранилище (то есть, к нему могут получить доступ другие агенты), нажмите **Выбрать машину**, выберите компьютер в сети, на котором установлен агент для MySQL/MariaDB, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке **Хранилища резервных копий**.

   Машина, выбранная для просмотра в любом из вышеуказанных действий, становится целевой машиной для восстановления.
5. Выберите **Восстановить** → **Базы данных MySQL/MariaDB**.
6. Выберите экземпляр, который вы хотите восстановить, а затем нажмите **Восстановить как файлы**.
7. В разделе **Путь** выберите каталог, в который будут восстановлены файлы.
8. Щёлкните **Начать восстановление**.

Восстановление баз данных

Из резервной копии с поддержкой приложений можно восстановить базы данных в запущенные экземпляры MySQL или MariaDB.

Выполните следующие действия:

1. В веб-консоли Кибер Бэкап выберите компьютер, на котором изначально находились данные, которые вы хотите восстановить.
2. Нажмите **Восстановление**.

3. Выберите точку восстановления. Обратите внимание, что точки восстановления отфильтрованы по месторасположению.
4. Если компьютер находится в автономном режиме, точки восстановления не отображаются. Выполните одно из следующих действий:
   - Если местом резервного копирования является облако или общее хранилище (то есть, к нему могут получить доступ другие агенты), нажмите **Выбрать машину**, выберите компьютер в сети, на котором установлен агент для MySQL/MariaDB, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке **Хранилища резервных копий**.

   Машина, выбранная для просмотра в любом из вышеуказанных действий, становится целевой машиной для восстановления.
5. Выберите **Восстановить** → **Базы данных MySQL/MariaDB**.
6. Щёлкните имя нужного экземпляра, чтобы перейти к его базам данных.
7. Выберите одну или несколько баз данных, которые вы хотите восстановить.
8. Нажмите **Восстановление**.
9. Нажмите **Целевой экземпляр MySQL/MariaDB** для указания параметров подключения и учетных данных доступа к целевому экземпляру.
10. Проверьте экземпляр, в который вы хотите восстановить данные. По умолчанию выбран исходный экземпляр.
11. Укажите данные учетной записи пользователя, которая может получить доступ к целевому экземпляру. Эта учетная запись пользователя должна иметь следующие привилегии для всех баз данных и таблиц (`\*.*`):
    - `INSERT`
    - `CREATE`
    - `DROP`
    - `LOCK_TABLES`
    - `ALTER`
    - `SELECT`
12. Нажмите **OK**.
13. Проверьте целевую базу данных.

    По умолчанию выбрана исходная база данных.

Чтобы восстановить базу данных как новую, щёлкните имя целевой базы данных и измените его. Это действие доступно только при восстановлении одной базы данных.

14. В разделе **Перезапись существующих баз данных** выберите режим перезаписи.

    По умолчанию перезапись включена, и резервная база данных заменит целевую базу данных с тем же именем.

    Если перезапись отключена, резервная база данных будет пропущена во время операции восстановления и не заменит целевую базу данных с тем же именем.

15. Щёлкните **Начать восстановление**.

Восстановление таблиц

Из резервной копии с поддержкой приложений можно восстановить таблицы в запущенные экземпляры MySQL или MariaDB.

Выполните следующие действия:

1. В веб-консоли Кибер Бэкап выберите компьютер, на котором изначально находились данные, которые вы хотите восстановить.
2. Нажмите **Восстановление**.
3. Выберите точку восстановления. Обратите внимание, что точки восстановления отфильтрованы по месторасположению.
4. Если компьютер находится в автономном режиме, точки восстановления не отображаются. Выполните одно из следующих действий:

    - Если местом резервного копирования является облако или общее хранилище (то есть, к нему могут получить доступ другие агенты), нажмите **Выбрать машину**, выберите компьютер в сети, на котором установлен агент для MySQL/MariaDB, а затем выберите точку восстановления.
    - Выберите точку восстановления на вкладке **Хранилища резервных копий**.

    Машина, выбранная для просмотра в любом из вышеуказанных действий, становится целевой машиной для восстановления.

5. Выберите **Восстановить** → **Базы данных MySQL/MariaDB**.
6. Щёлкните имя нужного экземпляра, чтобы перейти к его базам данных.
7. Щёлкните имя нужной базы данных, чтобы перейти к ее таблицам.
8. Выберите одну или несколько таблиц, которые вы хотите восстановить.
9. Нажмите **Восстановление**.

10. Нажмите **Целевой экземпляр MySQL/MariaDB** для указания параметров подключения и учетных данных доступа к целевому экземпляру.
11. Проверьте экземпляр, в который вы хотите восстановить данные. По умолчанию выбран исходный экземпляр.
12. Укажите данные учетной записи пользователя, которая может получить доступ к целевому экземпляру. Эта учетная запись пользователя должна иметь следующие привилегии для всех баз данных и таблиц (`\*.*`):
    - `INSERT`
    - `CREATE`
    - `DROP`
    - `LOCK_TABLES`
    - `ALTER`
    - `SELECT`
13. Нажмите **OK**.
14. Проверьте целевую таблицу.

    По умолчанию выбрана исходная таблица.

    Чтобы восстановить таблицу как новую, щёлкните имя целевой таблицы и измените его. Это действие доступно только при восстановлении одной таблицы.
15. В разделе **Перезапись существующих таблиц** выберите режим перезаписи.

    По умолчанию перезапись включена, и резервная копия таблицы заменит целевую таблицу с тем же именем.

    Если перезапись отключена, резервная копия таблицы будет пропущена во время операции восстановления и не заменит целевую таблицу с тем же именем.
16. Нажмите кнопку **Начать восстановление**.

Защита баз данных РЕД База Данных

Защита данных СУБД РЕД База Данных поддерживается начиная с версии Кибер Бэкап 15 обновление 2.7.

Поддерживаемые версии РЕД База Данных указаны в разделе *Поддерживаемые СУБД*.

Условия для резервного копирования

Для выполнения резервного копирования нужно установить агент Кибер Бэкап для операционной системы (агент для Windows или агент для Linux) на машину с СУБД РЕД База Данных.

Список поддерживаемых операционных систем Windows и Linux см. в разделе *Поддерживаемые операционные системы*.

Для установки агента для Linux обратитесь к разделу *Установка в Linux*.

Для установки агента для Windows обратитесь к разделу *Установка в Windows*.

Предварительная настройка базы данных

При настройке резервного копирования базы данных СУБД РЕД База Данных рекомендуется заблокировать базы данных на время резервного копирования. При такой блокировке основной файл базы данных замораживается, изменения при этом фиксируются во временном файле дельты. После окончания резервного копирования основной файл базы данных разблокируется, и временный файл дельты и основной файл базы данных объединяются.

Скачивание скриптов

Скачайте скрипты для блокировки базы данных (БД) на время резервного копирования.

Разархивирование скриптов

Распакуйте скачанные файлы `conf.sh` (Linux) и `conf.bat` (Windows) в рабочий каталог скриптов.

Настройка конфигурации

Укажите в файле `conf.*` следующие параметры:

- `RDB` — каталог установки СУБД;
- `DBNAME` — путь к файлу БД или псевдоним (database alias);
- `USER` — имя пользователя для подключения к БД;
- `PASS` — пароль;
- `NBL_DIR` — путь к каталогу с файлом журнала.

Разрешение запуска скриптов блокировки и разблокировки

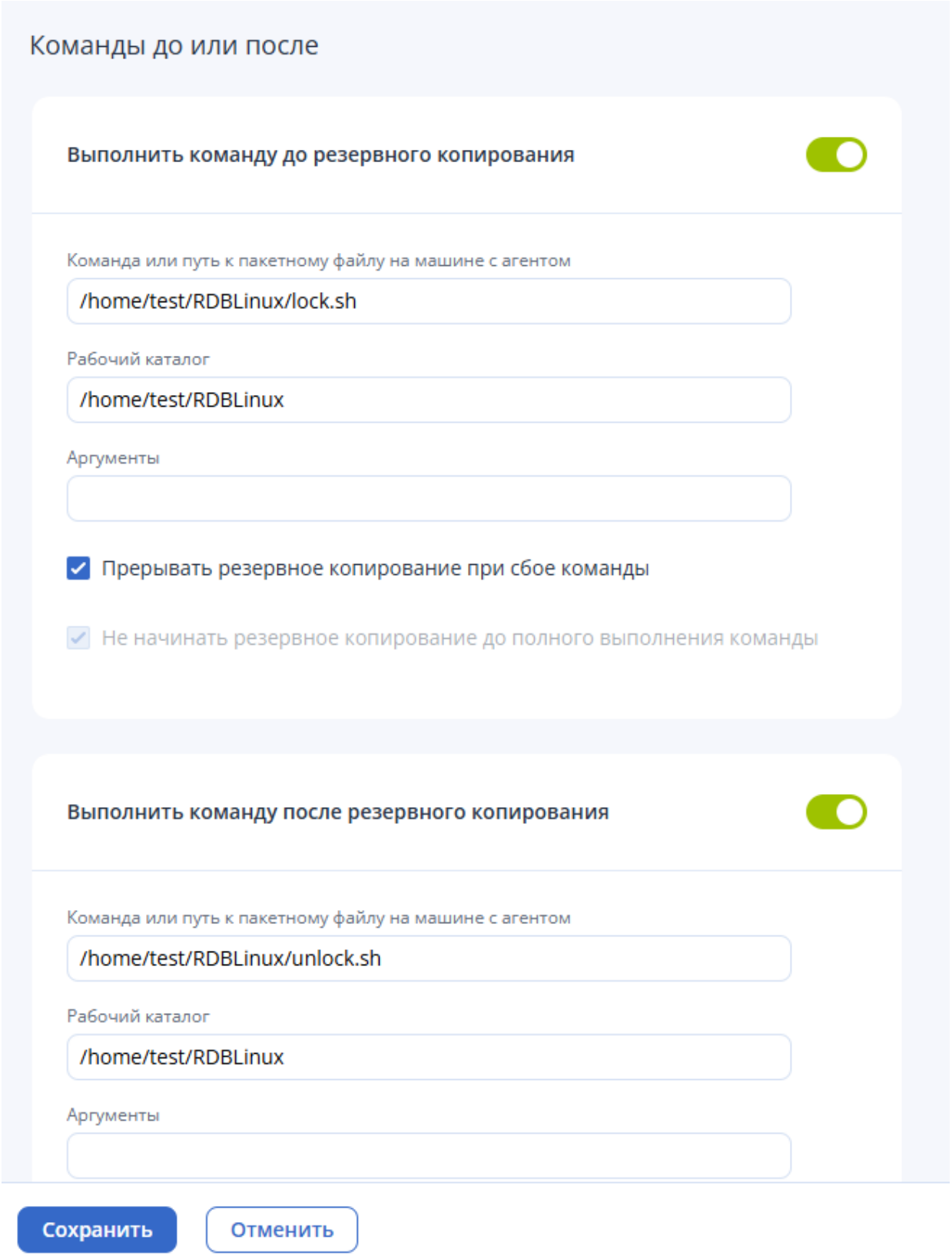
В случае использования ОС Linux необходимо задать права на выполнение для скриптов блокировки и разблокировки. Для этого перейдите в рабочий каталог скриптов и выполните следующие команды:

```
chmod +x ./lock.sh
chmod +x ./unlock.sh
```

Резервное копирование РЕД База Данных

Для создания плана защиты выполните следующие действия:

1. Перейдите в раздел **Устройства** и выберите машину с РЕД База Данных, которую вы хотите защитить.
2. Перейдите на вкладку справа **Защитить** и нажмите **Добавить план**.
3. В разделе **Выбор данных** выберите **Файлы/папки**.
4. В поле **Элементы для резервного копирования** нажмите **Указать** и выберите файл базы данных.
5. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий.
6. В поле **Параметры резервного копирования** нажмите **Изменить**.
7. Выберите параметр **Команды до или после**.
    1. Включите переключатель **Выполнить команду до резервного копирования**.
        - В поле **Команда или путь к пакетному файлу на машине с агентом** укажите путь к файлу `lock.sh`.
        - В поле **Рабочий каталог** укажите каталог, в котором находится файл `lock.sh`.
    2. Включите переключатель **Выполнить команду после резервного копирования**.
        - В поле **Команда или путь к пакетному файлу на машине с агентом** укажите путь к файлу `unlock.sh`.
        - В поле **Рабочий каталог** укажите каталог, в котором находится файл `unlock.sh`.
    3. Нажмите **Сохранить**.



8. При необходимости укажите другие параметры плана защиты. Подробнее см. в разделе *Резервное копирование*.

9. Нажмите **Применить**. Новый план защиты появится в списке планов и будет применен к

выбранным данным.

См. также информацию в разделе *План защиты и модули*.

Восстановление базы данных

Чтобы восстановить базу данных, выполните следующие действия:

1. Перейдите в раздел **Хранилища резервных копий** и выберите в списке нужную резервную копию.
2. Выберите справа **Показать резервные копии**.
3. Нажмите **Восстановить данные**.
4. Выберите резервную копию для восстановления, затем выберите справа **Восстановить**.
5. Выберите место для восстановления резервной копии. Возможные варианты:
   - Исходное расположение. База данных из резервной копии будет восстановлена на место существующей.
   - Пользовательское расположение.
6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.
8. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

После восстановления базы данных из резервной копии, она будет заблокирована. Для разблокировки восстановленной копии выполните команду:

```
nbackup -user USER_NAME -pass PASS -F /path/to/db_copy.fd
```

где

- `USER_NAME` — имя учетной записи с правами на выполнение скриптов разблокировки;
- `PASS` — пароль от учетной записи;
- `db_copy.fd` — имя восстановленного файла базы данных.

Защита баз данных MongoDB

Данные MongoDB можно защитить с помощью резервного копирования с использованием встроенных инструментов MongoDB (например, утилит mongodump и mongorestore). При этом обеспечивается восстановление на уровне серверов СУБД, баз данных и коллекций MongoDB.

Защита данных MongoDB поддерживается начиная с версии Кибер Бэкап 15 обновление 2.7.

Поддерживаемые версии MongoDB указаны в разделе *Поддерживаемые СУБД*.

Чтобы защитить физическую или виртуальную машину, на которой запущен экземпляр MongoDB, необходимо установить агент для Windows или агент для Linux (в зависимости от операционной системы сервера).

Агент защиты может быть установлен как на хост, на котором находятся базы данных MongoDB, так и на другой хост. Если вы устанавливаете агент защиты на другой хост, убедитесь, что хосты с агентом и MongoDB могут обмениваться данными по сети.

Чтобы установить агент защиты, выполните действия, как описано в разделе *Установка агентов* или *Автоматическая установка или автоматическое удаление в Linux*.

Настройка резервного копирования баз данных MongoDB

Для резервного копирования баз данных MongoDB используйте план защиты со скриптом, в котором описаны команды для встроенного инструмента MongoDB — утилиты mongodump.

Предварительные требования

- Агент защиты и утилита mongodump должны находиться на одном хосте.
- В случае если база данных находится на отдельном хосте, настройте доступ утилиты mongodump к базе данных MongoDB.

Настройка удаленного подключения к базе данных MongoDB

Для настройки удаленного подключения необходимо задать значение параметра `bindIp`:

1. Отредактируйте конфигурационный файл `/etc/mongod.conf`, например, добавьте строки:

   ```
   ...
   net:
     port: 27017
     bindIp: 0.0.0.0
   ...
   ```

2. Перезапустите сервер MongoDB:

   ```
   systemctl restart mongod.service
   ```

Подробнее см. в официальной документации MongoDB.

Создание скрипта с командами для утилиты mongodump

В скрипте необходимо указать параметры для утилиты mongodump. Подробнее см. в официальной документации MongoDB.

Пример скрипта:

```
#!/bin/bash

# Exit on error:
set -e

epoch_time=$(date +%s)
script_dir=$(pwd)
main_dir=/home/mongo_dump
backup_dir=${main_dir}/latest
info_file=${backup_dir}/README.txt
error_file=${backup_dir}/ERROR.txt

host_db=”localhost:27017”
mongo_db_name=”my-db”
mongo_db_collection=”my-collection”

if [ ! -d ${backup_dir} ]; then
  mkdir -p ${backup_dir}
  echo -e ”${epoch_time}\n$(date -d @${epoch_time})” > ${info_file}
  echo -e ”$(date -d @${epoch_time}): ${backup_dir} doesnt exist and has been created now.¬
↪Restart backup task” >> ${error_file}
  echo ”$(date -d @${epoch_time}): ${backup_dir} doesnt exist and has been created now. Restart¬
↪backup task” >&2
  exit 1
else
  # For move existing old data to a new dir
  mv ${backup_dir} ${main_dir}/$(head -n 1 ${info_file})
  # Or comment mv above and delete existing files:
  # rm -rf ${backup_dir}
  # Re-create backup dir:
  mkdir -p ${backup_dir}
fi

cd ${script_dir}
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
echo -e "${epoch_time}\n$(date -d @${epoch_time})" > ${info_file}
echo -e "\n\nRun: /usr/bin/mongodump --host=${host_db} --db ${mongo_db_name} --collection=${mongo_
↪db_collection} --out ${backup_dir}" >> ${info_file}
/usr/bin/mongodump --host=${host_db} --db=${mongo_db_name} --collection=${mongo_db_collection} --
↪out ${backup_dir} >> ${info_file} 2>&1
```

где:

- `localhost:27017` — имя хоста развертывания MongoDB;
- `my-db` — имя базы данных MongoDB;
- `my-collection` — имя коллекции базы данных MongoDB;
- `/home/mongo_dump/latest` — место хранения резервной копии;
- `README.txt` — файл с результатами работы скрипта;
- `ERROR.txt` — файл с ошибками при сбое в работе скрипта.

Пример содержимого файла README.txt:

```
1694175355
Fri Sep  8 15:15:55 MSK 2023

Run: /usr/bin/mongodump --host=localhost:27017 --db my-db --collection=my-collection --out /home/
↪mongo_dump/latest
Unknown or unsupported stacktrace method requested: generic_fp. Ignoring it
2023-09-08T15:15:56.014+0300    writing my-db.my-collection to /home/mongo_dump/latest/my-db/my-
↪collection.bson
2023-09-08T15:15:56.015+0300    done dumping my-db.my-collection (11 documents)
```

Создание плана резервного копирования

Для создания плана защиты выполните следующие действия:

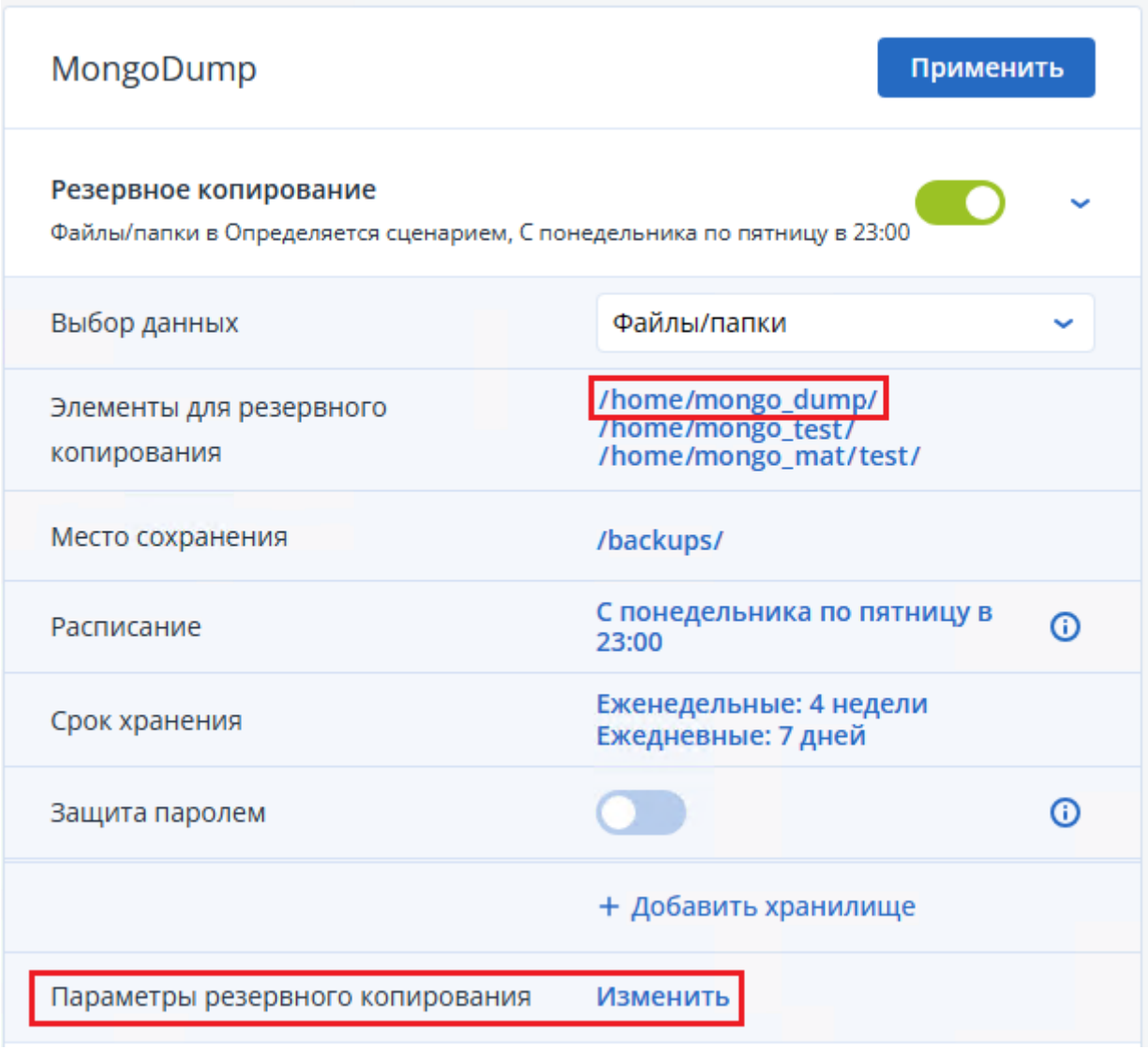
1. Перейдите в **Устройства** и выберите машину с базой данных MongoDB, которую вы хотите защитить.
2. Перейдите на вкладку справа **Защитить**.
3. В разделе **Выбор данных** укажите данные для резервного копирования. Возможные варианты:
   - Вся машина. Обратите внимание, что внешние диски не включаются в резервную копию всей машины (подробнее см. в разделе *Выбор всей машины*).

- Диски/тома.
- Файлы/папки.

В поле **Элементы для резервного копирования** нажмите **Указать** и выберите данные для резервного копирования. Папки, указанные в поле **Элементы для резервного копирования**, должны существовать до запуска резервного копирования (дочерние элементы могут быть созданы в ходе выполнения скрипта).

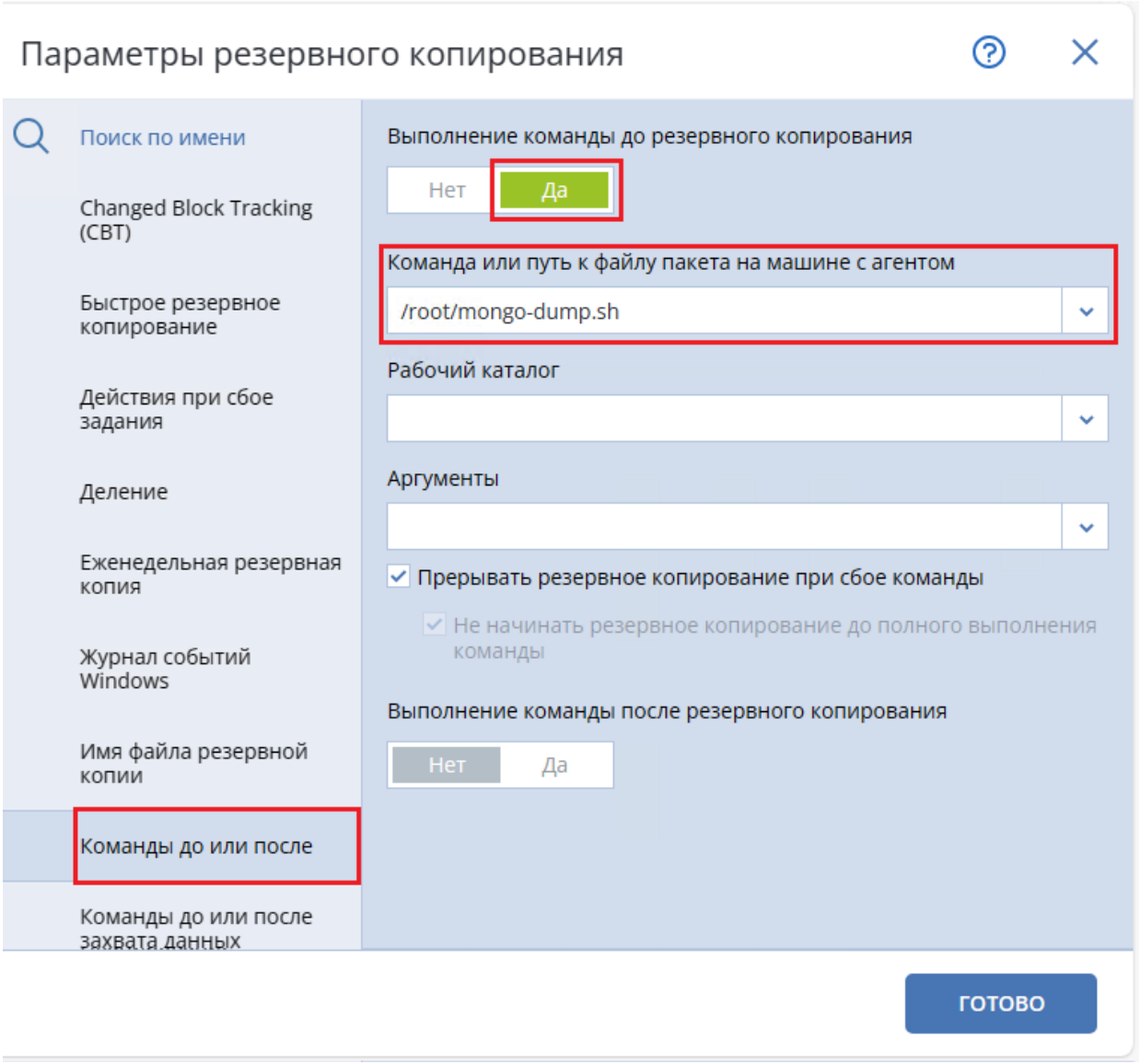
Место хранения резервной копии из скрипта (например, `/home/mongo_dump/latest`) должно попадать в список данных для резервного копирования (либо явно, либо как дочерний элемент).

4. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий.
5. В поле **Параметры резервного копирования** нажмите **Изменить**.



6. Выберите параметр **Команды до или после** (Также можно использовать параметр **Команды до или после захвата данных**). Включите переключатель **Выполнение команды до резервного копирования**

и укажите путь до файла со скриптом с командами для утилиты mongodump:



Примечание

Если работа утилиты mongodump завершается ошибкой (например, если mongodump не смогла установить соединение с базой данных), то при установленном флажке **Прерывать резервное копирование при сбое команды** Кибер Бэкап не начинает резервное копирование и отображает в интерфейсе сообщение об ошибке.

Однако, если утилита mongodump завершает работу без ошибки (return code = 0), то в Кибер Бэкап такая операция помечается как успешно выполненная при любых результатах работы mongodump.

Рекомендуем проверять результаты работы утилиты mongodump (например, в файле README.txt), чтобы убедиться, что резервная копия создана успешно.

Нажмите **Готово**.

7. При необходимости укажите другие параметры плана защиты. Подробнее см. в разделе *Резервное копирование*.
8. Нажмите **Применить**.

Новый план защиты появится в списке планов.

Восстановление данных MongoDB

Восстановление данных MongoDB выполняется в два этапа: с помощью Кибер Бэкап из резервной копии восстанавливаются файлы дампов баз данных или коллекций MongoDB, затем из файлов дампов с помощью утилиты mongorestore восстанавливаются базы данных или коллекции.

Восстановление файлов дампов

Чтобы восстановить файлы дампов, выполните следующие действия:

1. Перейдите в раздел **Хранилища резервных копий** и выберите в списке нужную резервную копию.
2. Выберите справа **Показать резервные копии**.
3. Нажмите **Восстановить данные**.
4. Выберите резервную копию для восстановления, затем выберите справа **Восстановить**.
5. Выберите место для восстановления резервной копии.
6. [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.
7. Проверьте правильность заполнения полей и затем нажмите **Начать восстановление**.
8. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

Восстановление баз данных и коллекций MongoDB

Для восстановления баз данных или коллекций используйте утилиту mongorestore. Подробнее см. в официальной документации MongoDB.

Пример:

```
# /usr/bin/mongorestore --host="localhost:27017" --db=my-db --collection=my-collection /home/
↪mongo_dump/restored_my-db/my-collection.bson
```

где:

- `localhost:27017` — имя хоста развертывания MongoDB;
- `my-db` — конечная база данных для восстановления;
- `my-collection` — коллекция базы данных для восстановления;
- `/home/mongo_dump/restored_my-db/my-collection.bson` — место хранения и восстановленный файл резервной копии.

Защита Kubernetes

С помощью Кибер Бэкап можно выполнять резервное копирование пространств имен и постоянных томов Kubernetes. При использовании Кибер Бэкап и Kubernetes регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователя и различных сбоев. Удаленные и поврежденные элементы можно восстановить из резервной копии.

Условия для резервного копирования Kubernetes

Для резервного копирования данных Kubernetes понадобятся установленные и настроенные продукты:

- Кибер Бэкап версии 17 или выше с лицензией Кибер Бэкап Расширенная редакция универсальная лицензия.
- Kubernetes (поддерживаемые версии приведены в разделе *Поддерживаемые приложения*).
  - Для создания моментальных снимков томов в кластере Kubernetes должны быть установлены CSI-драйвер с поддержкой функции Snapshot и контроллер моментальных снимков томов (см. раздел *Подготовка кластера Kubernetes*).
  - Из кластера должен быть доступ к Docker-репозиторию `https://registry.cyberprotect.ru/registry`. В случае среды без доступа в Интернет можно разместить Docker-образ, необходимый агенту для Kubernetes, во внутреннем Docker-репозитории (см. раздел *Резервное копирование постоянных томов в хранилище Кибер Бэкап*).

Примечание

Защита каждого кластера Kubernetes требует отдельной лицензии Кибер Бэкап Расширенная редакция универсальная лицензия. Информацию о лицензиях см. в разделе *Издания и лицензии Кибер Бэкап*.

Для выполнения резервного копирования требуется установка агента для Kubernetes.

Полный список поддерживаемых операционных систем Linux см. в разделе *Поддерживаемые*

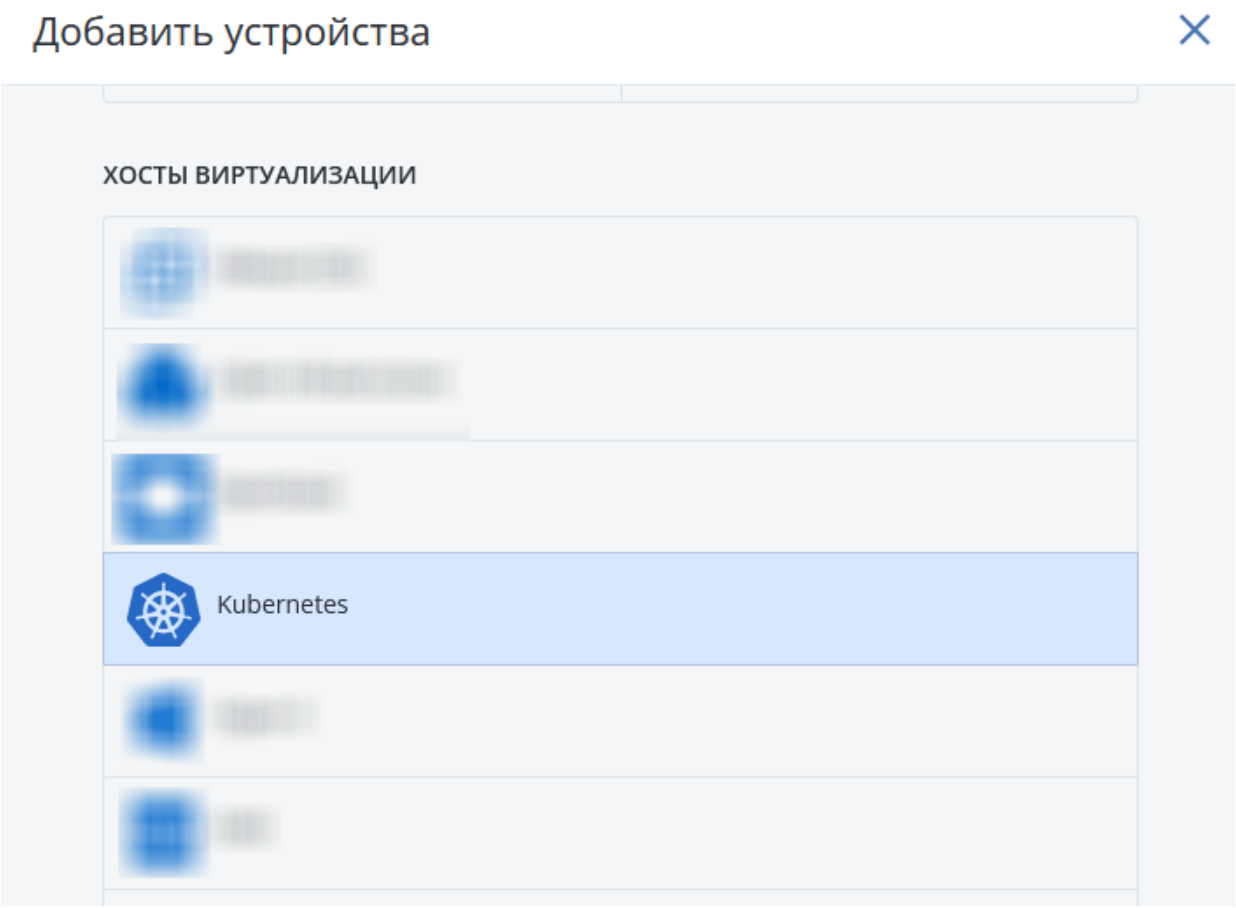
операционные системы.

Перед установкой продукта в системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например, выполнив следующую команду в качестве суперпользователя: `apt-get install rpm`.

Установка агента для Kubernetes

Установите агент для Kubernetes:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Физические и виртуальные машины**.
2. Справа вверху щёлкните **Добавить** и выберите в списке Kubernetes.



3. Выберите **Скачать и установить агент для Kubernetes** и укажите место сохранения установщика.



4. Запустите установщик Кибер Бэкап от имени привилегированного пользователя на сервере, на котором планируете установить агент.
5. Следуя инструкциям на экране, установите агент для Linux, агент для Kubernetes и, если необходимо, прочие компоненты.

См. также *Установка в Linux*.

Если агенту не удалось подключиться к серверу управления, выполните это подключение вручную, как описано в статье Ручная регистрация агента на сервере управления.

Подготовка кластера Kubernetes

Перед добавлением кластера в Кибер Бэкап подготовьте его, как описано в этом разделе.

Требования к CSI-драйверу

Для создания моментальных снимков томов в кластере должен быть установлен CSI-драйвер с поддержкой функции Snapshot.

Для резервного копирования томов в хранилище Кибер Бэкап CSI-драйвер должен поддерживать функцию Raw Block. Если ваш драйвер её не поддерживает, то следует добавить аннотацию в соответствующие ему объекты VolumeSnapshotClass:

```
kubectl annotate volumesnapshotclass <volume_snapshot_class_name> cyberprotect.ru/convert-to-
↪block-mode=false
```

Список CSI-драйверов и сведения о поддерживаемых ими функциях см. в документации разработчика Kubernetes.

Установка контроллера моментальных снимков томов

Установите контроллер моментальных снимков томов, если он еще не установлен. Сведения об установке см. в статье. Подробные сведения о моментальных снимках томов см. в документации Kubernetes.

В процессе добавления кластера в веб-консоль управления агент для Kubernetes проверяет наличие установленного контроллера с помощью запроса в API-интерфейс Kubernetes, аналогичного следующей команде:

```
kubectl get volumesnapshots -n kube-system
```

В случае успешного выполнения запроса считается, что контроллер установлен.

Если в кластере есть несколько классов моментальных снимков томов (VolumeSnapshotClass), то каждый класс хранилища (StorageClass) необходимо привязать к одному из них с помощью аннотации:

```
kubectl annotate storageclass <storage_class_name> cyberprotect.ru/volume-snapshot-class=<volume_
↪snapshot_class_name>
```

В этой команде `storage_class_name` — имя класса хранилища, `volume_snapshot_class_name` — имя класса моментальных снимков томов.

В классе моментальных снимков томов, который будет использоваться агентом для Kubernetes, в поле `deletionPolicy` должно быть установлено значение `Delete`. Если это не так, то будет использоваться созданная автоматически копия класса, в которой в поле `deletionPolicy` установлено значение `Delete`.

Создание служебной учетной записи для агента Kubernetes

Перед добавлением кластера Kubernetes в Кибер Бэкап создайте в нем служебную учетную запись для агента Kubernetes.

1. Создайте файл `prepare-cluster.yaml` с содержимым, приведенным ниже.

   prepare-cluster.yaml

   ```
   apiVersion: v1
   kind: Namespace
   metadata:
     name: cyberprotect
   ---
   apiVersion: v1
   kind: ServiceAccount
   metadata:
   ```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  name: cyberprotect
  namespace: cyberprotect
---
apiVersion: v1
kind: Secret
metadata:
 name: cyberprotect
 namespace: cyberprotect
 annotations:
  kubernetes.io/service-account.name: cyberprotect
type: kubernetes.io/service-account-token
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-discovery-generic
rules:
# Get cluster id
- apiGroups: [””]
  resources: [”namespaces”]
  resourceNames: [”kube-system”]
  verbs: [”get”]
# List nodes
- apiGroups: [””]
  resources: [”nodes”]
  verbs: [”list”]
# List namespaces
- apiGroups: [””]
  resources: [”namespaces”]
  verbs: [”list”]
# List storage classes
- apiGroups: [”storage.k8s.io”]
  resources: [”storageclasses”]
  verbs: [”list”]
# List cluster resources
- apiGroups: [”*”]
  resources: [”*”]
  verbs: [”list”]
# Create cyberprotect namespace
- apiGroups: [””]
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  resources: [”namespaces”]
  verbs: [”create”]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-discovery-generic
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-discovery-generic
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: cyberprotect-discovery-volume-backup
  namespace: cyberprotect
rules:
# Manage pods
- apiGroups: [””]
  resources: [”pods”]
  verbs: [”*”]
# Manage jobs
- apiGroups: [”batch”]
  resources: [”jobs”]
  verbs: [”*”]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: cyberprotect-discovery-volume-backup
  namespace: cyberprotect
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
roleRef:
  kind: Role
  name: cyberprotect-discovery-volume-backup
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-backup-generic
rules:
# List cluster resources
- apiGroups: [”*”]
  resources: [”*”]
  verbs: [”list”]
# Get persistent volume claims
- apiGroups: [””]
  resources: [”persistentvolumeclaims”]
  verbs: [”get”]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-backup-generic
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-backup-generic
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-backup-snapshotter
rules:
# Manage volume snapshots
- apiGroups: [”snapshot.storage.k8s.io”]
  resources: [”*”]
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  verbs: ["*"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-backup-snapshotter
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-backup-snapshotter
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-backup-data-mover
rules:
# Create/delete pods, services and persistent volume claims. Execute commands in pods.
- apiGroups: [""]
  resources: ["pods", "pods/exec", "services", "persistentvolumeclaims"]
  verbs: ["create", "get", "delete"]
# Watch events
- apiGroups: [""]
  resources: ["events"]
  verbs: ["watch"]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-backup-data-mover
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-backup-data-mover
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  apiGroup: rbac.authorization.k8s.io
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: cyberprotect-restore
rules:
# Manage namespaces
- apiGroups: [””]
  resources: [”namespaces”]
  verbs: [”create”, ”get”, ”update”, ”delete”]
# Manage core resources
- apiGroups: [””]
  resources: [”*”]
  verbs: [”*”]
# Manage workloads
- apiGroups: [”apps”]
  resources: [”*”]
  verbs: [”*”]
# Manage other cluster resources
- apiGroups: [”*”]
  resources: [”*”]
  verbs: [”create”, ”get”, ”update”, ”delete”, ”deletecollection”]
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: cyberprotect-restore
subjects:
- kind: ServiceAccount
  name: cyberprotect
  namespace: cyberprotect
roleRef:
  kind: ClusterRole
  name: cyberprotect-restore
  apiGroup: rbac.authorization.k8s.io
```

2. Создайте в кластере ресурсы, перечисленные в файле `prepare-cluster.yaml`:

```
kubectl create -f prepare-cluster.yaml
```

3. Разрешите запуск привилегированных подов в пространстве имён `cyberprotect`:

```
kubectl label --overwrite ns cyberprotect pod-security.kubernetes.io/enforce=privileged
```

4. Получите и сохраните токен служебной учетной записи `cyberprotect`:

```
kubectl -n cyberprotect describe secret cyberprotect
```

Дополнительные действия для кластера Deckhouse

Разрешите запуск привилегированных подов в пространстве имён `cyberprotect`:

```
kubectl label --overwrite ns cyberprotect security.deckhouse.io/pod-policy=privileged
```

Для защиты системных пространств имен кластера Deckhouse

1. Создайте ресурс `Secret` с токеном для служебной учетной записи `deckhouse`:

```
apiVersion: v1
kind: Secret
metadata:
 name: deckhouse-secret
 namespace: d8-system
 annotations:
  kubernetes.io/service-account.name: deckhouse
type: kubernetes.io/service-account-token
```

2. Выполните следующую команду:

```
kubectl -n d8-system describe secret deckhouse-secret
```

3. Получите и сохраните токен служебной ученой записи `deckhouse`:

```
root@k8s-d-node1:/home/myuser# kubectl -n d8-system describe secret deckhouse-secret
Name:         deckhouse-secret
Namespace:    d8-system
Labels:       <none>
Annotations:  kubernetes.io/service-account.name: deckhouse
              kubernetes.io/service-account.uid: 1db29c03-13d5-4a9d-a084-00348b739b05
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Type:  kubernetes.io/service-account-token

Data
====
ca.crt:     1107 bytes
namespace:  9 bytes
token:      <...>
```

Подготовка файла kubeconfig

Перед добавлением кластера Kubernetes в Кибер Бэкап подготовьте конфигурационный файл `kubeconfig`.

Процедура подготовки файла далее описана для двух случаев:

- создание резервной копии и восстановление пользовательских пространств имен Kubernetes;
- создание резервной копии и восстановление системных пространств имен Deckhouse.

Подготовка файла в случае защиты пользовательских пространств имен Kubernetes

1. Загрузите на рабочую машину файл конфигурации `kubeconfig` по умолчанию. Путь к файлу конфигурации по умолчанию — `/etc/kubernetes/admin.conf`.
2. Внесите в файл следующие изменения:
   - замените имя исходной служебной учетной записи (например, `admin`) на `cyberprotect`;
   - замените сертификат для аутентификации пользователя (`client-certificate-data: <...>`) на токен (`token: <...>`), который был подготовлен в разделе *Создание служебной учетной записи для агента Kubernetes*.
3. Сохраните внесенные изменения.

Пример файла, который должен получиться в итоге:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <...>
    server: https://192.168.1.100:6443
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  name: myk8scluster
contexts:
- context:
    cluster: myk8scluster
    user: cyberprotect
  name: default
current-context: default
kind: Config
preferences: {}
users:
- name: cyberprotect
  user:
    token: <...>
```

Подготовка файла в случае защиты системных пространств имен Deckhouse

1. Загрузите на рабочую машину файл `kubeconfig` по умолчанию.
2. Внесите в файл следующие изменения:
   - замените имя исходной служебной учетной записи (например, `kubernetes-admin`) на `deckhouse`;
   - замените сертификат для аутентификации пользователя (`client-certificate-data: <...>`) на токен (`token: <...>`), который был подготовлен в разделе *Создание служебной учетной записи для агента Kubernetes*.
3. Сохраните внесенные изменения.

Пример файла, который должен получиться в итоге:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <...>
    server: https://10.11.12.13:6443
  name: deckhouse
contexts:
- context:
    cluster: deckhouse
    user: deckhouse
  name: deckhouse@deckhouse
current-context: deckhouse@deckhouse
```

(продолжается на следующей странице)

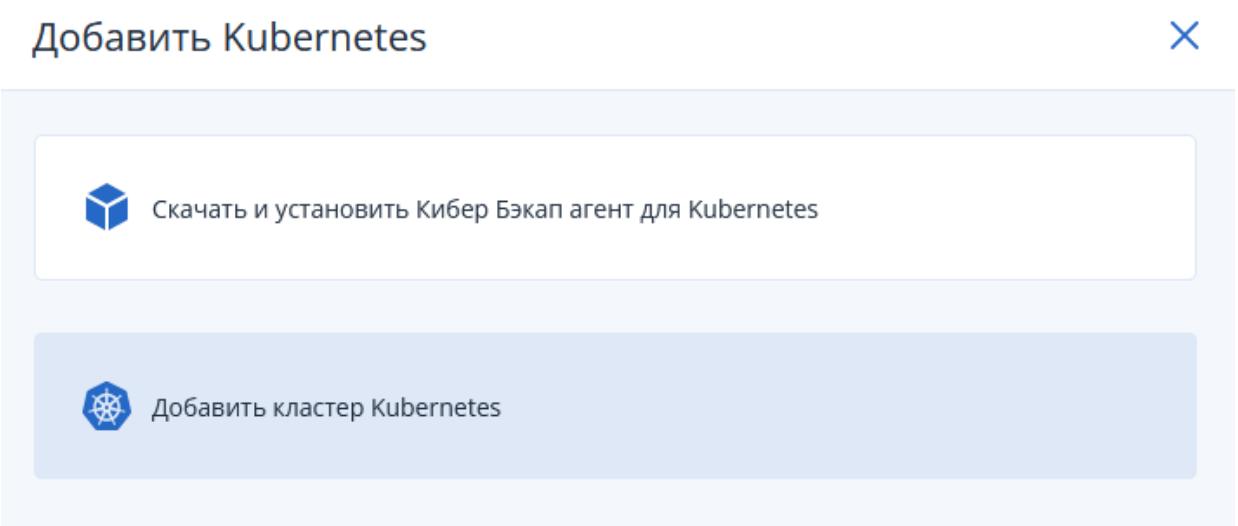
(продолжение с предыдущей страницы)

```
kind: Config
preferences: {}
users:
- name: deckhouse
  user:
    token: <...>
```

Добавление кластера Kubernetes

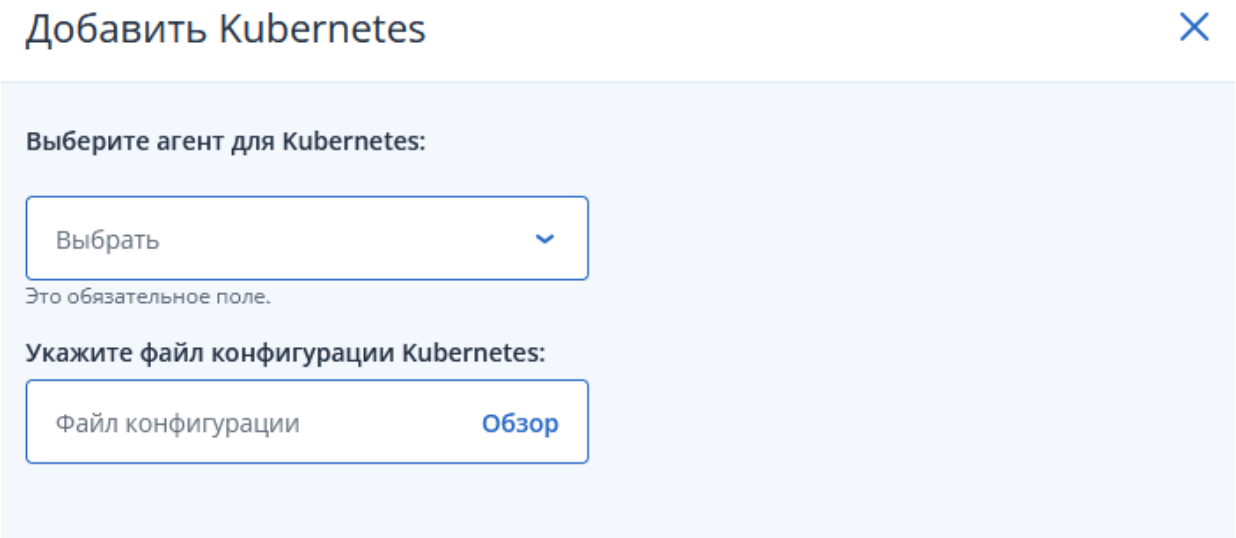
Добавьте кластер Kubernetes в Кибер Бэкап:

1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Физические и виртуальные машины**.
2. Справа вверху щёлкните **Добавить** и выберите в списке **Kubernetes**.
3. Выберите **Добавить кластер Kubernetes**.



4. Укажите агент для Kubernetes, для которого будет выполнена регистрация, и файл конфигурации `kubeconfig`, который был подготовлен в разделе *Подготовка файла kubeconfig*.

   Для подключения к кластеру Kubernetes файл конфигурации должен содержать адрес кластера, имя пользователя и токен.



После заполнения полей нажмите **Добавить** и дождитесь окончания установки.

5. В веб-консоли перейдите в раздел **Устройства** и убедитесь, что кластер Kubernetes добавлен в вашу конфигурацию.
6. В веб-консоли перейдите в раздел **Настройки** → **Агенты** и убедитесь, что агент для Kubernetes отображается в списке агентов.

Резервное копирование Kubernetes

Предварительные требования

Перед резервным копированием убедитесь, что вы выполнили следующие действия:

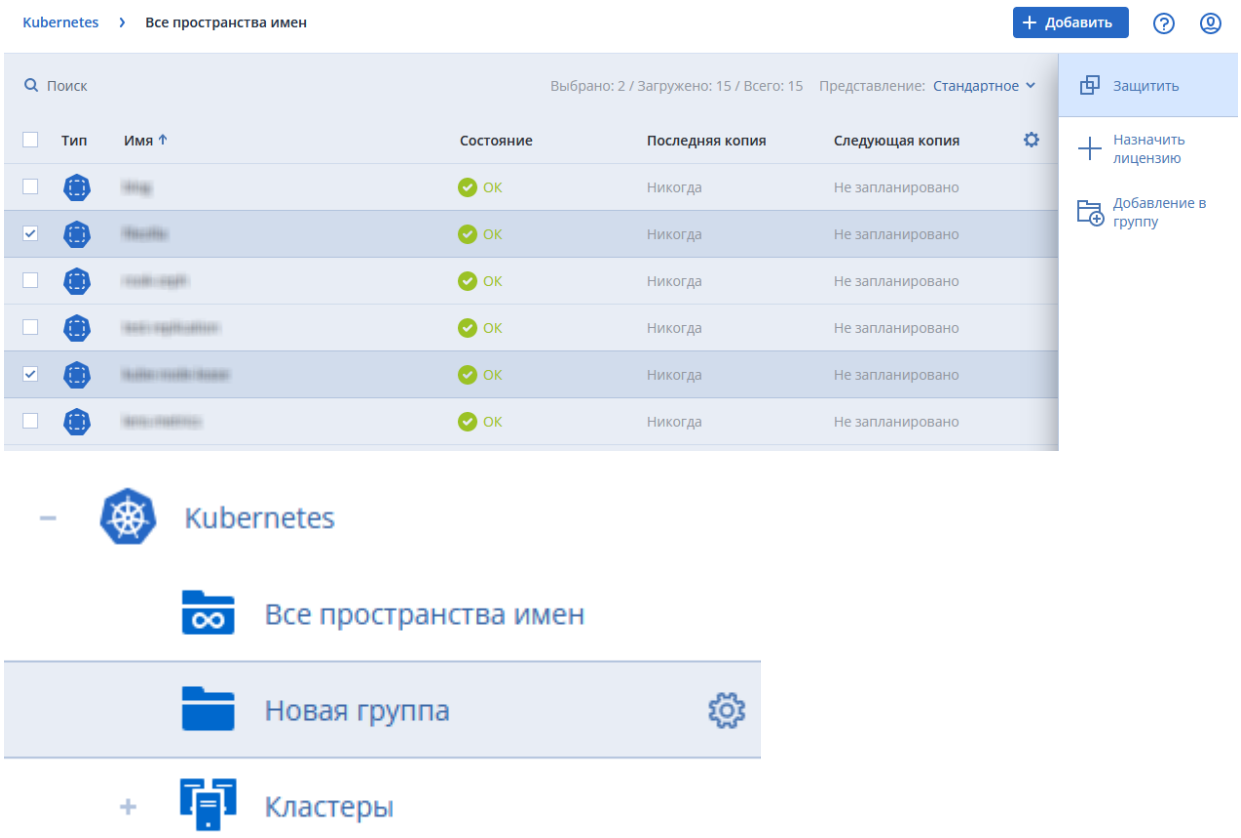
1. Установка агента Кибер Бэкап для Kubernetes и подключение кластера Kubernetes к Серверу управления (см. *Установка агента для Kubernetes* и *Добавление кластера Kubernetes*).
2. Настройка хранилища. Настройте ваше хранилище для работы с Кибер Бэкап и Kubernetes.

Создание плана защиты

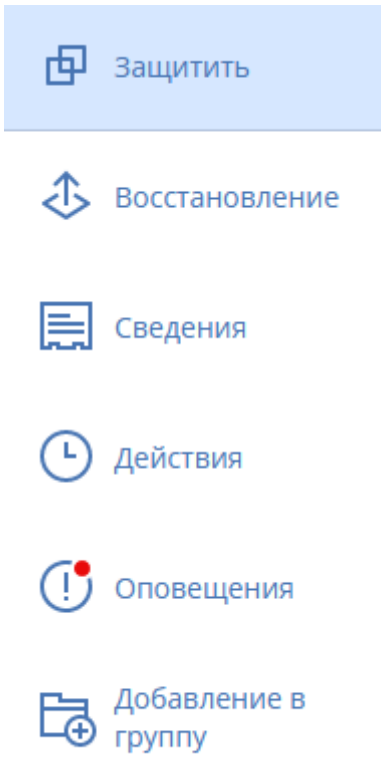
Создание плана защиты из веб-консоли возможно двумя способами: через пункт веб-консоли **Устройства** и через пункт **Планы** (см. также *Создание плана защиты*).

Создание плана через пункт веб-консоли ”Устройства”

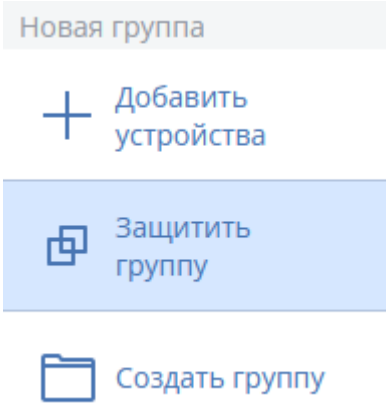
1. В веб-консоли Кибер Бэкап перейдите в раздел **Устройства** → **Kubernetes**.
2. Выберите пространства имен (или группу с пространствами имен) для защиты.



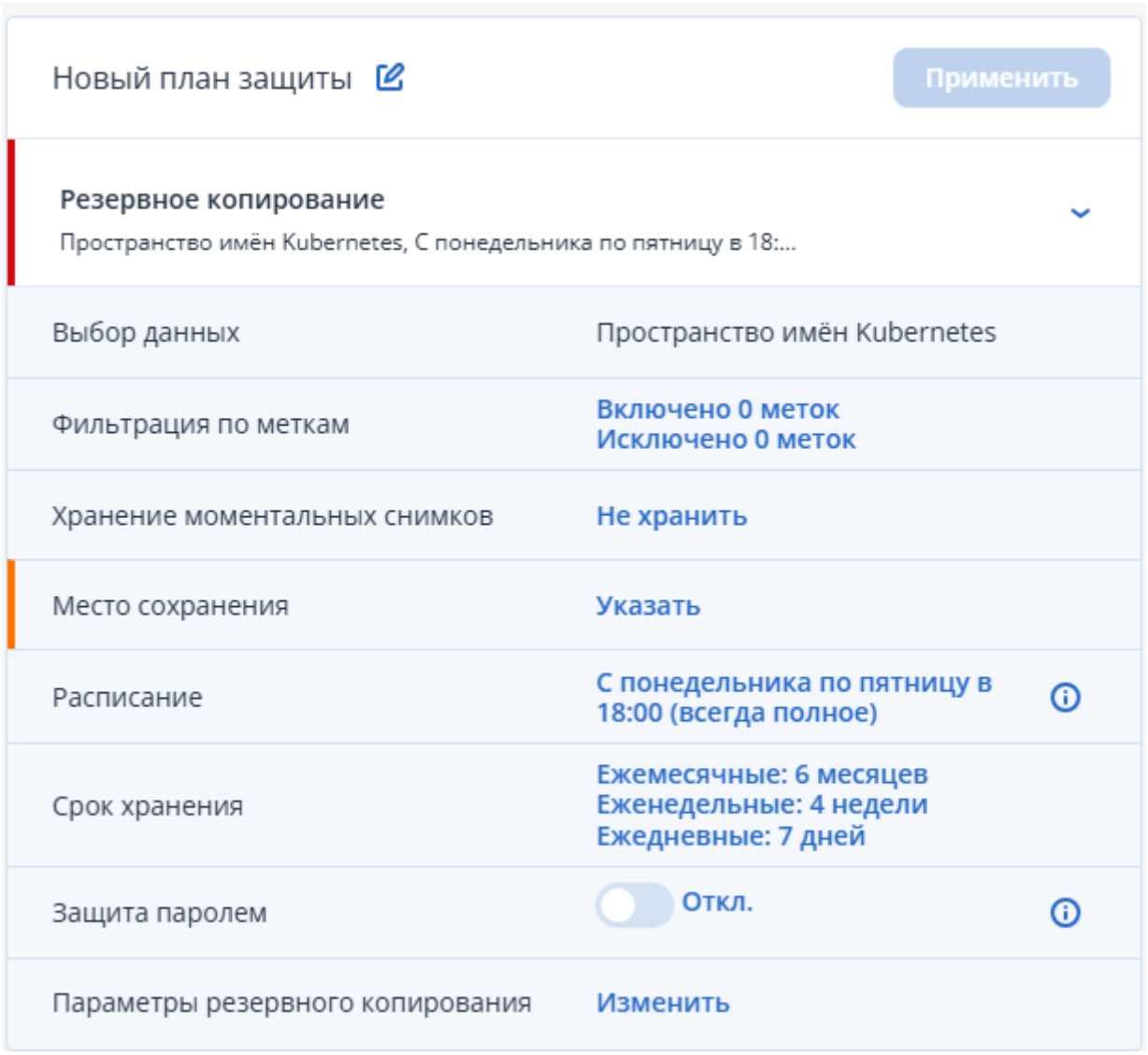
3. Нажмите справа вверху **Защитить**.



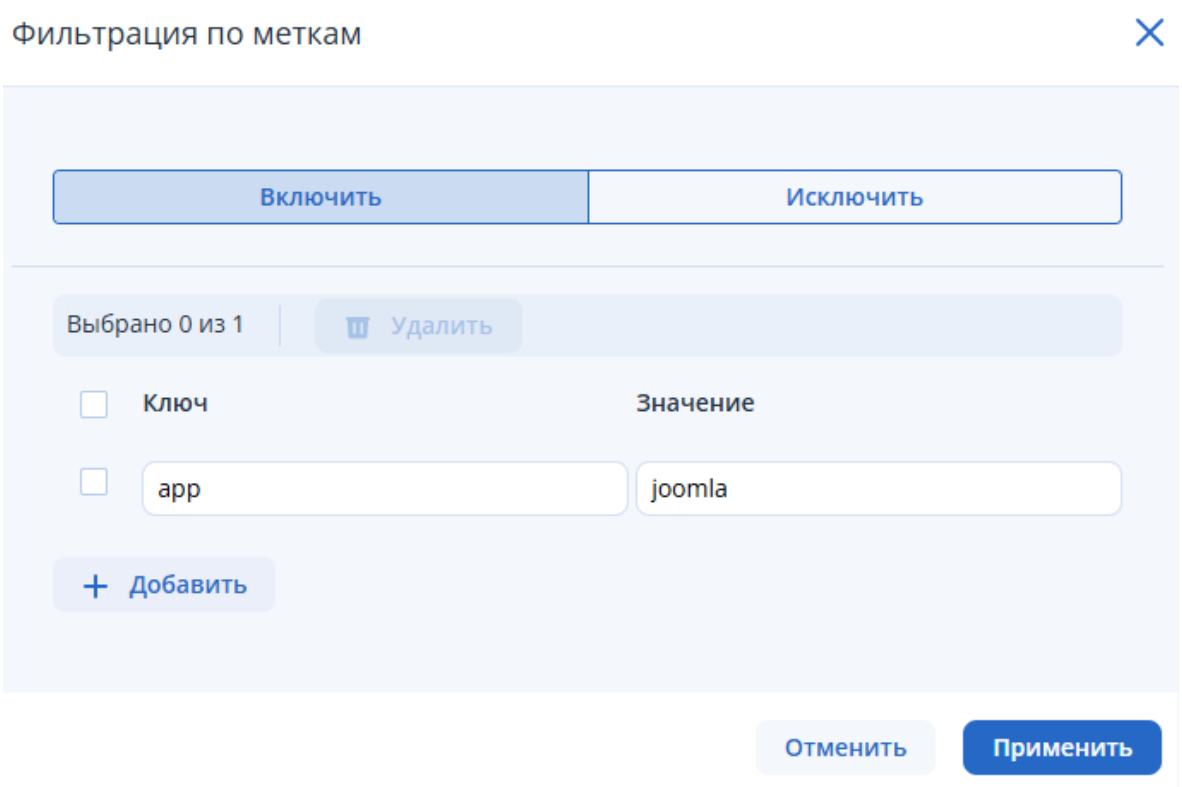
Для защиты группы выберите **Защитить группу**.



4. Щёлкните **Создать план** (если план не применен) или **Добавить план** (если какой-либо план в данный момент применен).
5. Выберите необходимые вам настройки плана защиты, заполнив соответствующие поля:



1. **Фильтрация по меткам**. Укажите метки ресурсов Kubernetes, по которым ресурсы будут включаться в план защиты.



Особенности резервного копирования в рамках плана защиты с метками:

- В резервную копию попадает не только ресурс с включающей меткой, но и вся цепочка связанных с ним ресурсов. Например, для цепочки ресурсов `Deployment` → `ReplicaSet` → `Pod` при указании включающей метки ресурса `Pod` Кибер Бэкап производит резервное копирование только ресурса `Deployment`, при этом попадает в резервную копию и восстанавливается вся цепочка ресурсов.

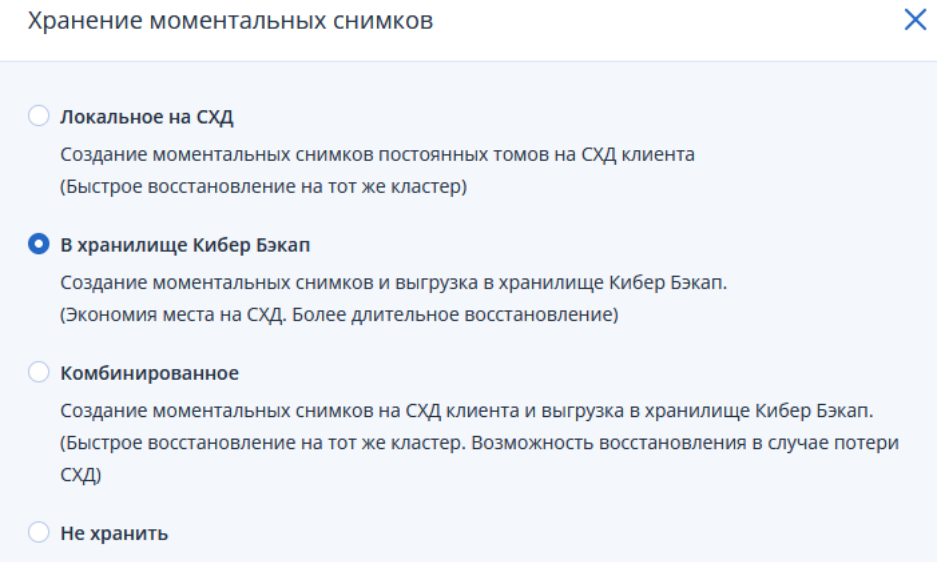
  Примечание

  Восстановление цепочек зависимостей ресурсов `Custom Resources` может работать некорректно.

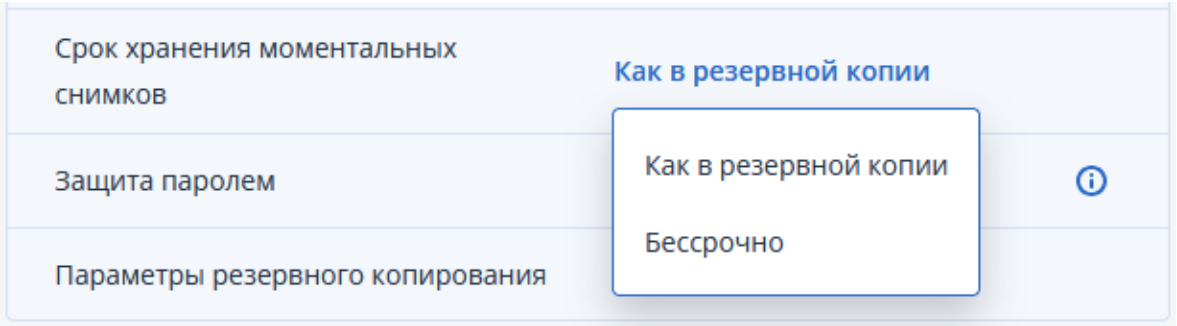
- Ресурс, который имеет как включающую, так и исключающую метку, не будет включен в план защиты.
- Для резервного копирования постоянного тома должна присутствовать включающая метка самого тома (`Persistent Volume`) или запроса на хранилище тома (`Persistent Volume Claim`). При резервном копировании постоянного тома в резервную копию всегда включаются ресурсы `Persistent Volume`, `Persistent Volume Claim` и `Storage Class`.

- Если в плане защиты включено хранение моментальных снимков, то в резервную копию включаются ресурсы `Volume Snapshot`, `Volume Snapshot Class` и `Volume Snapshot Content`.

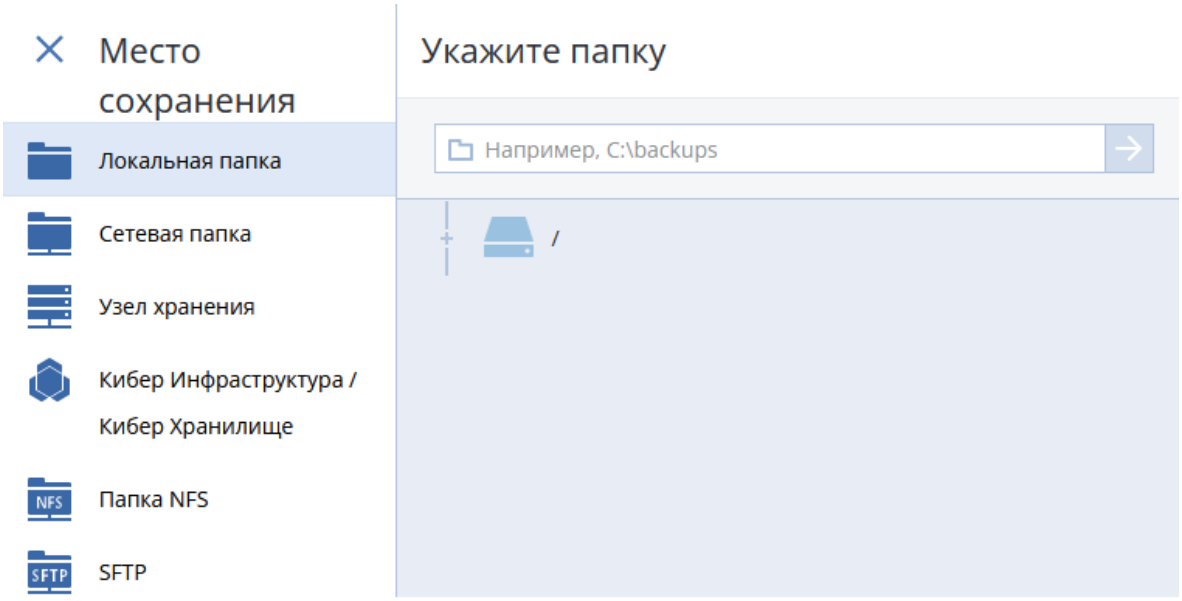
2. **Хранение моментальных снимков**. Укажите место, где будут сохраняться моментальные снимки.



При выборе варианта хранения **Локальное на СХД** укажите также срок хранения моментальных снимков в появившейся области **Срок хранения моментальных снимков**.

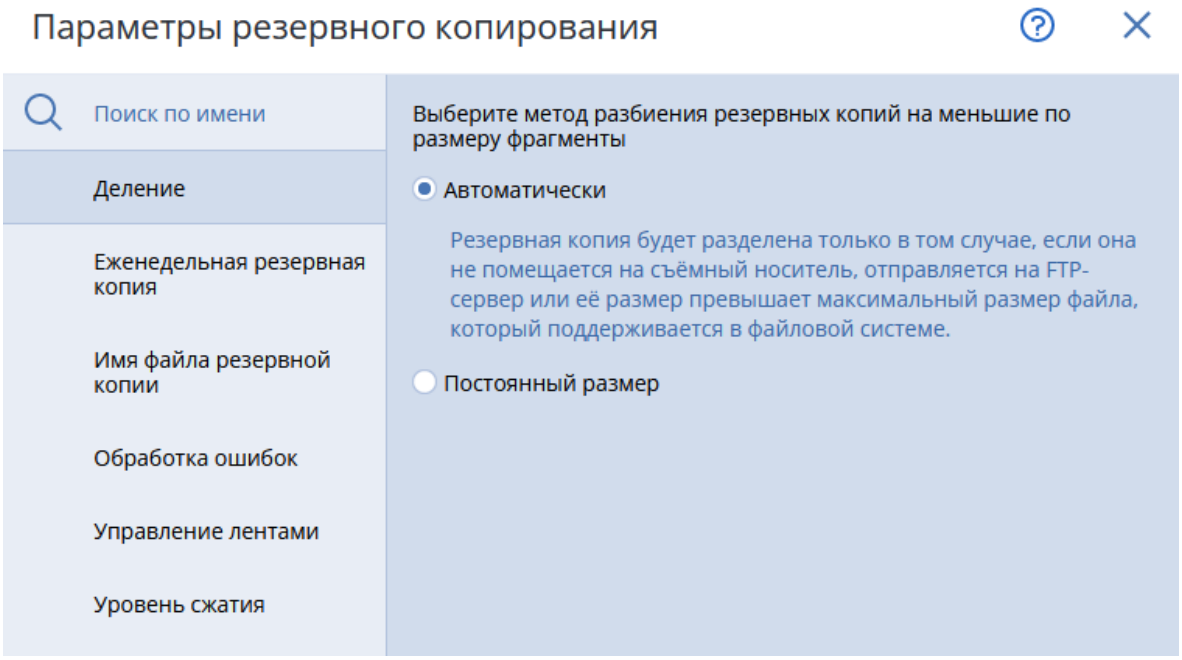


3. **Место сохранения**. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, узел хранения, Кибер Инфраструктура / Кибер Хранилище, папка NFS, SFTP.



Подробнее о выборе места хранения резервных копий см. в разделе *Выбор места сохранения*.

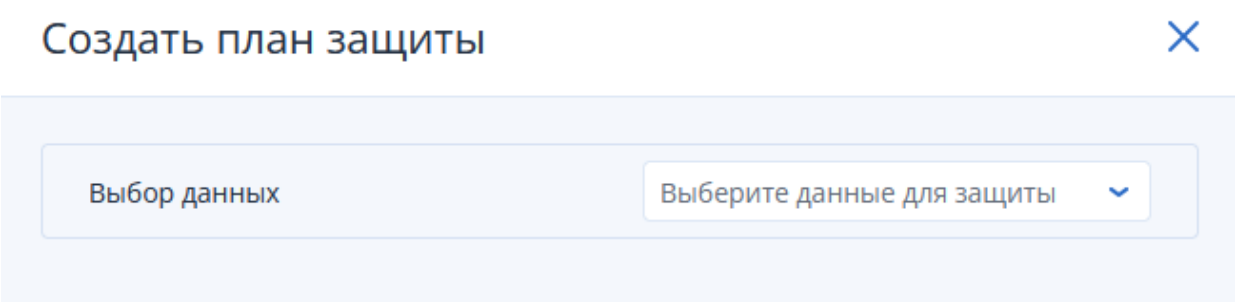
4. [Необязательно] **Расписание**. Задайте расписание резервного копирования.
5. [Необязательно] **Срок хранения**. Укажите срок хранения резервных копий.
6. [Необязательно] **Защита паролем**. Активируйте защиту паролем при необходимости.
7. [Необязательно] **Параметры резервного копирования**. Выберите параметры резервного копирования (см. также *Параметры резервного копирования*).



6. Нажмите **Применить**.

Создание плана через пункт веб-консоли "Планы"

1. В веб-консоли перейдите в раздел **Планы** → **Защита**.
2. Нажмите справа вверху **Создать план**.
3. В открывшемся окне в строке **Выбор данных** выберите из списка **Kubernetes**.



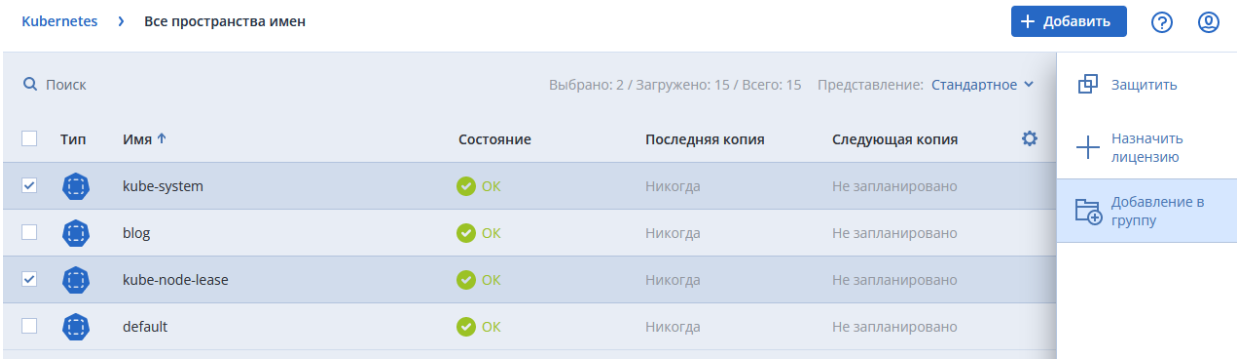
4. В окне создания плана настройте план нужным вам образом и нажмите **Создать**.

Создание групп

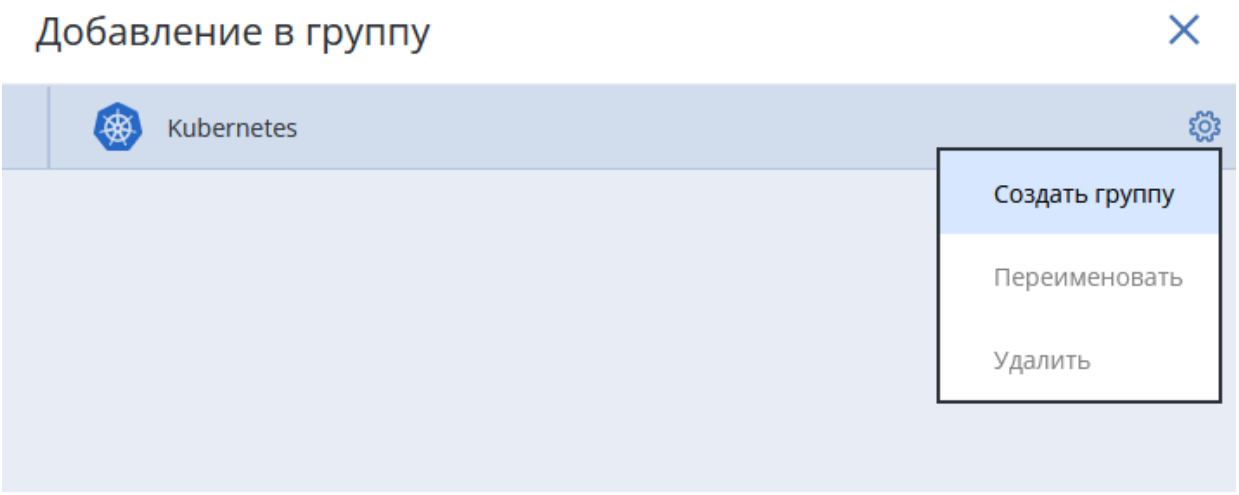
С Кибер Бэкап вы можете создавать и защищать не только отдельные пространства имен, но и группы пространств имен.

Для создания группы пространств имен выполните следующие действия:

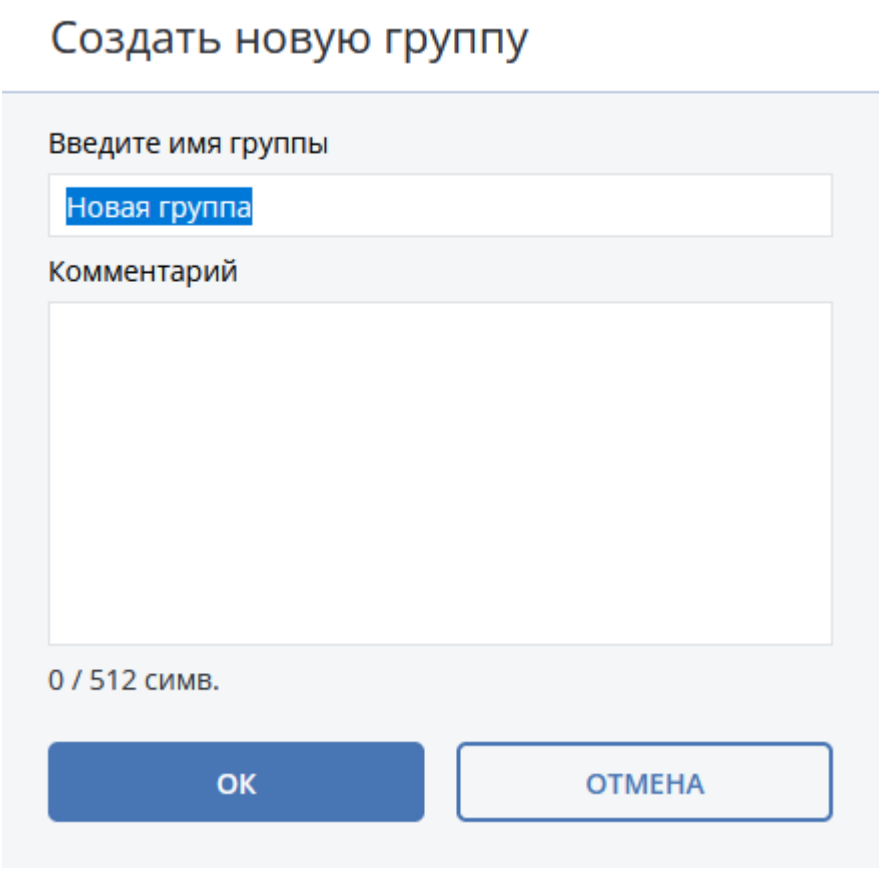
1. В веб-консоли перейдите в раздел **Устройства** → **Kubernetes**.
2. Отметьте в списке устройства, которые хотите добавить в группу, и щёлкните справа **Добавление в группу**.



3. Щёлкните значок шестеренки и выберите **Создать группу**.



4. Введите имя группы; если требуется, добавьте комментарий и нажмите **ОК**.



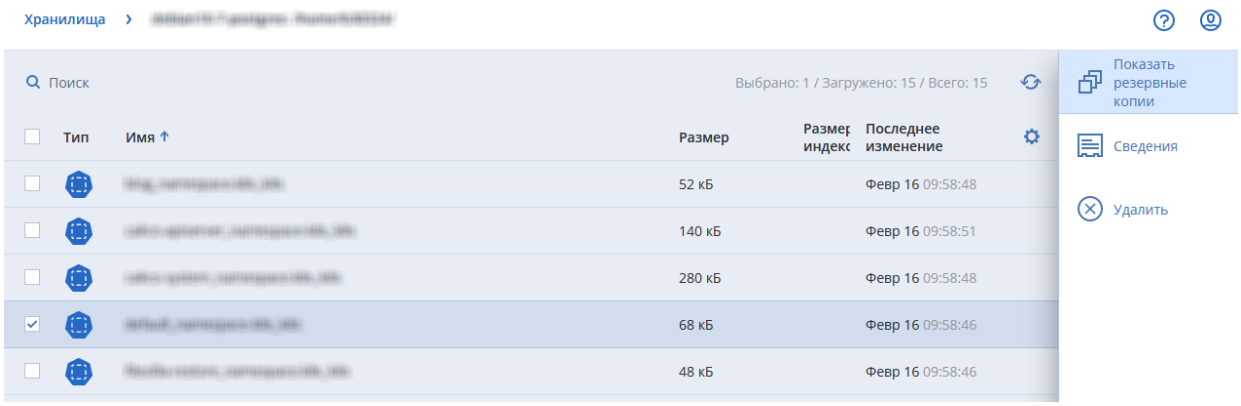
5. Нажмите **Готово**.

Восстановление Kubernetes

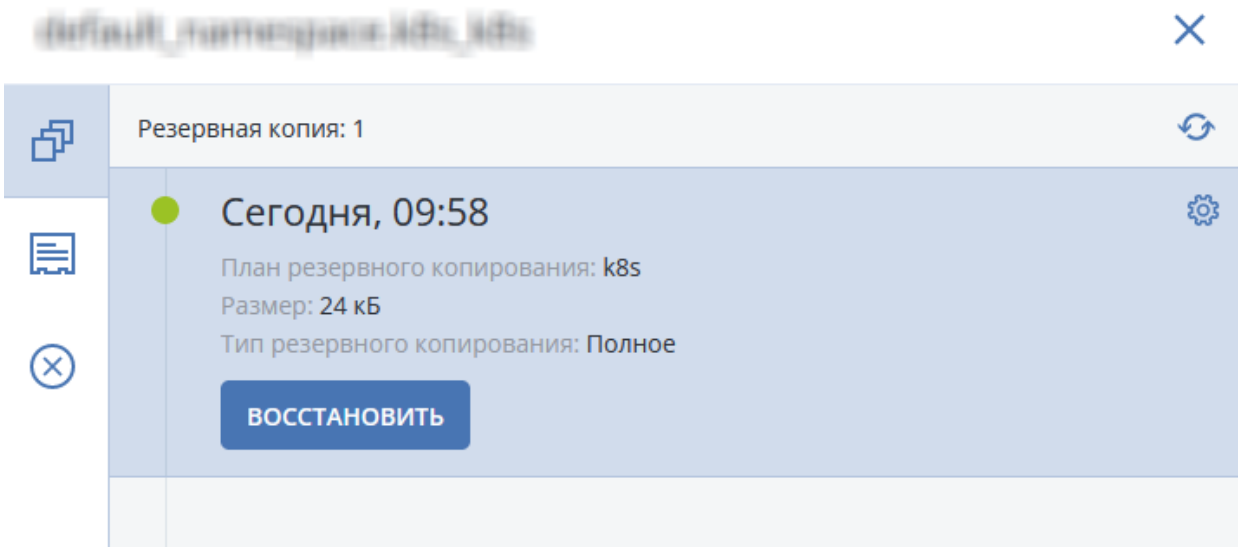
Перед восстановлением убедитесь, что место хранения резервных копий доступно, а резервные копии, из которых вы хотите выполнить восстановление, были созданы успешно.

Восстановление пространства имен и постоянных томов Kubernetes из меню ”Резервные копии”

1. В веб-консоли перейдите в раздел **Хранилища резервных копий** и выберите хранилище с резервными копиями Kubernetes.
2. В списке резервных копий Kubernetes отметьте нужную вам и нажмите справа вверху **Показать резервные копии**.



3. Выберите нужную резервную копию из списка и нажмите **Восстановить**.



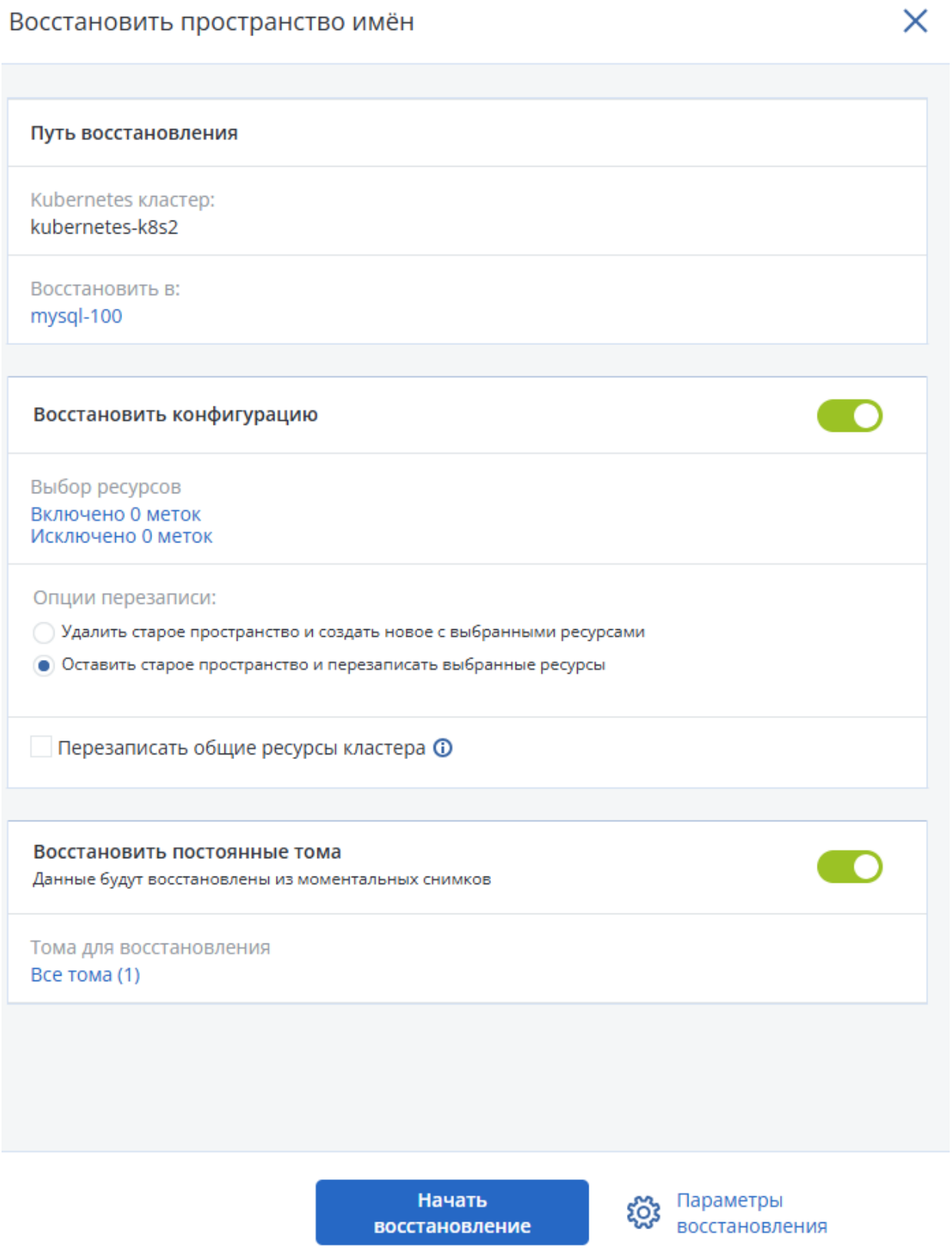
4. Для восстановления щёлкните **Восстановить все пространство**.

   Для просмотра списка постоянных томов щёлкните **Постоянные тома**.

   Для просмотра сведений о конфигурации:

1. щёлкните **Конфигурация**;
2. отметьте в списке необходимый элемент;
3. нажмите справа **Открыть YAML** для просмотра сведений или **Скачать** для сохранения файла со сведениями.

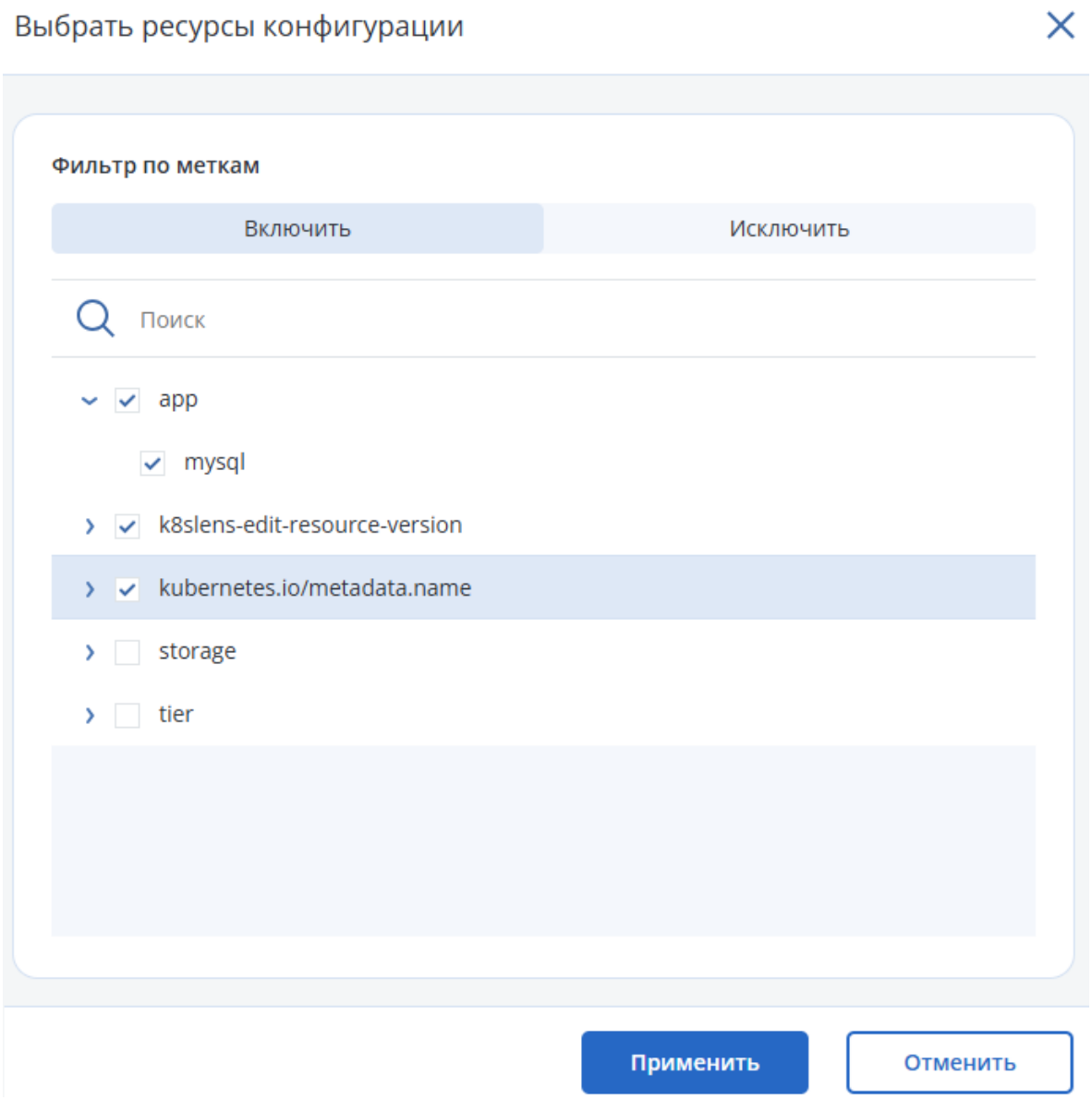
5. Укажите параметры восстановления.



- Укажите место для восстановления резервной копии. Выберите установленное по умолчанию место или укажите новое.
- Для восстановления конфигурации в области **Восстановить конфигурацию** укажите нужный

вариант и передвиньте ползунок.

- Для восстановления с фильтрацией по меткам щёлкните раздел **Выбор ресурсов**. Укажите метки ресурсов, которые необходимо восстановить:



Особенности восстановления с фильтраций по меткам:

- Восстанавливается не только ресурс с включающей меткой, но и вся цепочка связанных с ним ресурсов.

> **Примечание**
>
> Восстановление цепочек зависимостей ресурсов `Custom Resources` может работать некорректно.

- Ресурс, который имеет как включающую, так и исключающую метку, не будет восстановлен.
- Для восстановления постоянного тома должна присутствовать включающая метка самого тома (`Persistent Volume`) или запроса на хранилище тома (`Persistent Volume Claim`). При восстановлении постоянного тома всегда восстанавливаются ресурсы `Persistent Volume`, `Persistent Volume Claim` и `Storage Class` (так же восстанавливаются ресурсы `Volume Snapshot`, `Volume Snapshot Class` и `Volume Snapshot Content`, если они присутствуют в резервной копии).

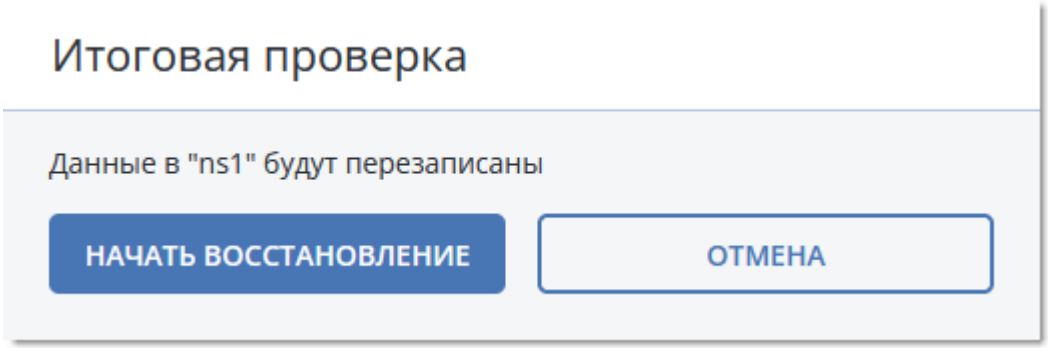
- Для восстановления всех постоянных томов передвиньте ползунок в области **Восстановить постоянные тома**. При необходимости измените параметры восстановления томов, такие как имя тома и класс хранения, нажав **Все тома**.

  > **Примечание**
  >
  > При восстановлении тома с новым именем исходный том не удаляется из кластера.

  Сведения о том, как восстановить только выбранные постоянные тома, не восстанавливая при этом пространство имен, см. в подразделе ”Восстановление постоянных томов из меню **Резервные копии**”.

- [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.

6. Нажмите **Начать восстановление**. Подтвердите еще раз восстановление в открывшемся окне и дождитесь его окончания.

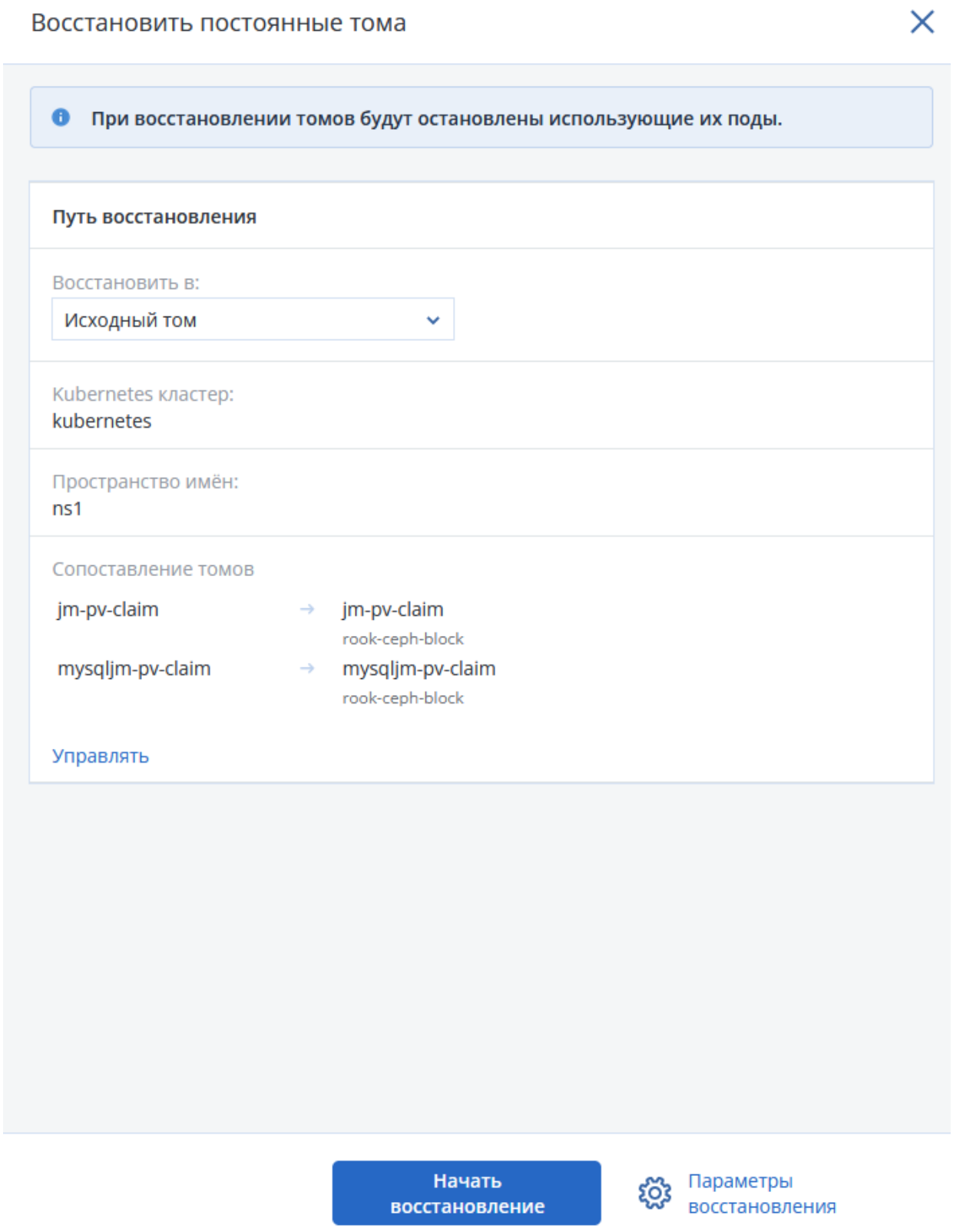


Восстановление постоянных томов из меню ”Резервные копии”

1. В веб-консоли перейдите в раздел **Хранилища резервных копий** и выберите хранилище с резервными копиями Kubernetes.
2. В списке резервных копий Kubernetes отметьте нужную вам и нажмите справа вверху **Показать**

резервные копии.

3. Выберите нужную резервную копию из списка и нажмите **Восстановить**.
4. Щёлкните **Постоянные тома** и выберите тома, которые необходимо восстановить.
5. Справа вверху щёлкните **Восстановить постоянные тома**.
6. Укажите параметры восстановления.



- Укажите место для восстановления резервной копии. Выберите установленное по умолчанию место или укажите новое.
- При необходимости измените имена и классы хранения восстанавливаемых томов, щёлкнув

Управлять в разделе **Сопоставление томов**.

> **Примечание**
>
> Автоматическое сопоставление томов возможно только в последовательном порядке при условии, что конфигурации целевой машины и машины-источника одинаковы. Если конфигурации машин различаются, сопоставить тома можно только в ручном режиме.

> **Примечание**
>
> При восстановлении тома с новым именем исходный том не удаляется из кластера.

- [Необязательно] Нажмите **Параметры восстановления** и укажите команды, которые должны выполняться перед восстановлением данных или после него.

7. Нажмите **Начать восстановление**. Подтвердите еще раз восстановление в открывшемся окне и дождитесь его окончания.

> **Примечание**
>
> Для корректного восстановления убедитесь, что конфигурационный файл `kubeconfig` подготовлен необходимым образом (подробнее см. *Подготовка файла kubeconfig*).

Резервное копирование постоянных томов в хранилище Кибер Бэкап

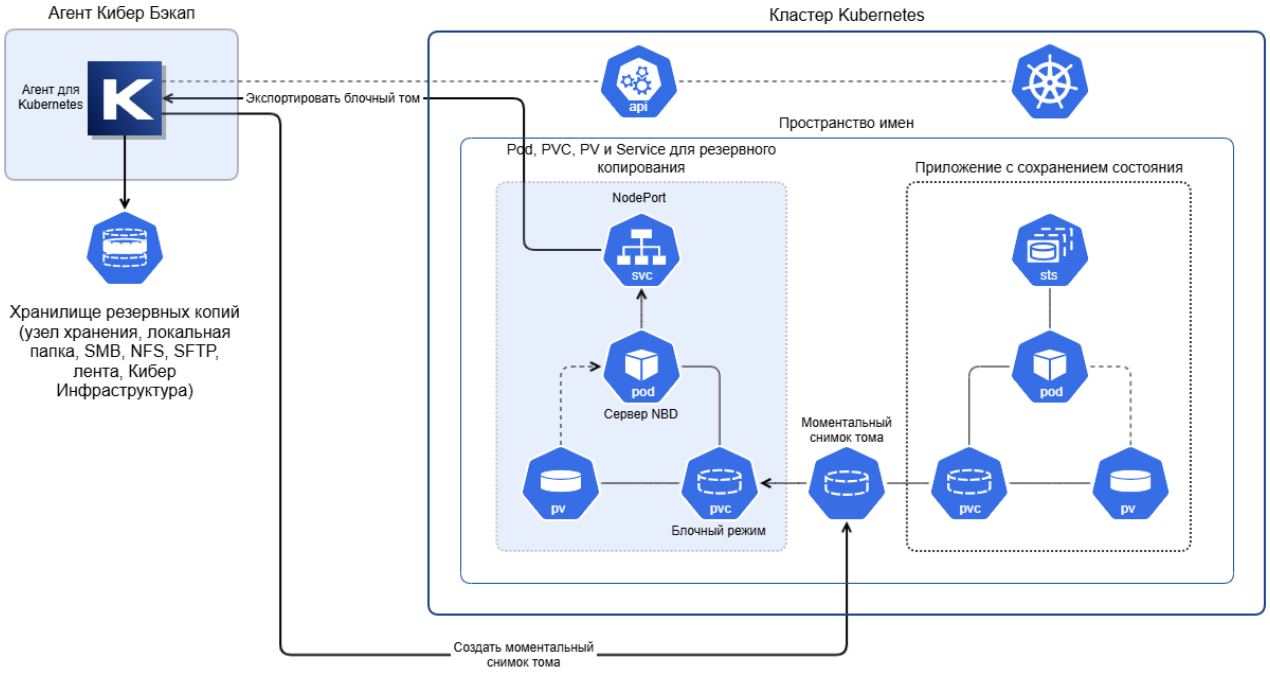
Резервное копирование

Резервное копирование постоянного тома (PersistentVolume) в хранилище Кибер Бэкап выполняется следующим образом:

1. Создается моментальный снимок исходного тома (VolumeSnapshotContent).
2. На основе моментального снимка создается временный том в блочном режиме или в режиме файловой системы (при наличии аннотации `cyberprotect.ru/convert-to-block-mode=false` в `VolumeSnapshotClass`).
3. В служебном пространстве имён `cyberprotect` создается временный под (Pod) с сервером NBD/NFS на основе Docker-образа `k8s-backup-and-restore`, к которому подключен временный том.
4. Создается сервис (Service) типа NodePort, посредством которого агент для Kubernetes может получить данные временного тома. В случае недоступности сервиса агент использует механизм

port forwarding.

5. Агент для Kubernetes получает данные временного тома, создается резервная копия тома в хранилище Кибер Бэкап.
6. По завершении создания резервной копии сервис, временные под и том удаляются. Моментальный снимок тома удаляется при использовании режима хранения моментальных снимков тома **В хранилище Кибер Бэкап** либо оставляется в кластере при использовании режима **Комбинированное**.



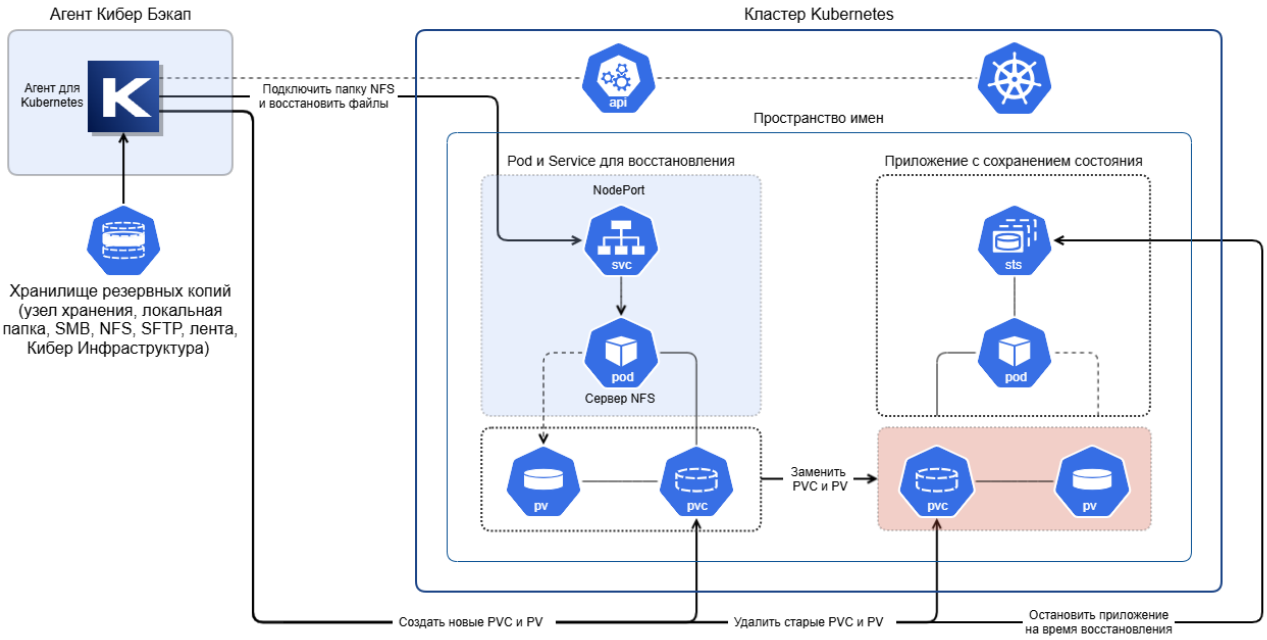
Восстановление из резервной копии

Восстановление тома из размещенной в хранилище Кибер Бэкап резервной копии происходит следующим образом:

1. Останавливаются использующие восстанавливаемый том приложения (число реплик устанавливается равным нулю или удаляются поды).
2. В служебном пространстве имён `cyberprotect` создаются новый том и временный под (Pod) с сервером NFS; при этом старый том удаляется, если его имя совпадает с именем нового тома.
3. Создается сервис типа NodePort, посредством которого агент для Kubernetes может записать данные из резервной копии на новый том. В случае недоступности сервиса агент использует механизм port forwarding.
4. Агент для Kubernetes монтирует папку NFS и записывает данные из резервной копии на новый том.
5. Сервис и временный под (Pod) удаляются. Объект PersistentVolumeClaim тома переносится в

целевое пространство имён.

6. Новый том подключается к требуемым подам, восстанавливается исходное число реплик приложений.



Требования

- Для создания моментальных снимков томов в кластере Kubernetes должен быть установлен CSI-драйвер с поддержкой функции Snapshot.

  Для резервного копирования томов в хранилище Кибер Бэкап CSI-драйвер должен поддерживать функцию Raw Block. Если ваш драйвер её не поддерживает, то следует добавить аннотацию в соответствующие ему объекты VolumeSnapshotClass:

  ```
  kubectl annotate volumesnapshotclass <volume_snapshot_class_name> cyberprotect.ru/convert-to-
  ↪block-mode=false
  ```

  Список CSI-драйверов и сведения о поддерживаемых ими функциях см. в документации разработчика Kubernetes.

- Из кластера должен быть доступен Docker-репозиторий, из которого можно получить Docker-образ `k8s-backup-and-restore`. По умолчанию используется публичный Docker-репозиторий компании Киберпротект `registry.cyberprotect.ru/registry`.

- Сервисная учетная запись `cyberprotect` должна обладать правами на запуск пода в привилегированном режиме в целевом пространстве имен.

Настройка доступа в Docker-репозиторий в закрытой среде

При отсутствии доступа в Docker-репозиторий по умолчанию (например, если Кибер Бэкап используется в среде без доступа в Интернет) можно загрузить из него Docker-образ `k8s-backup-and-restore` и разместить его в Docker-репозитории, который доступен в пределах закрытой среды. Например:

1. На машине, на которой есть доступ к Docker-репозиторию по умолчанию и на которой установлен Docker, получите Docker-образ и сохраните его в виде tar-архива:

```
CYBERPROTECT_REGISTRY=registry.cyberprotect.ru/registry
IMAGE_NAME=k8s-backup-and-restore
IMAGE_TAG=1.0

docker pull ${CYBERPROTECT_REGISTRY}/${IMAGE_NAME}:${IMAGE_TAG}
docker save -o ${IMAGE_NAME}_${IMAGE_TAG}.tar ${CYBERPROTECT_REGISTRY}/${IMAGE_NAME}:${IMAGE_
↪TAG}
```

2. Разместите tar-архив на машине, на которой есть доступ к внутреннему Docker-репозиторию и на которой установлен Docker.

3. Отправьте Docker-образ во внутренний Docker-репозиторий:

```
CYBERPROTECT_REGISTRY=registry.cyberprotect.ru/registry
IMAGE_NAME=k8s-backup-and-restore
IMAGE_TAG=1.0

INTERNAL_REGISTRY=<YOUR_INTERNAL_DOCKER_REGISTRY>
INTERNAL_IMAGE_NAME=${IMAGE_NAME}
INTERNAL_IMAGE_TAG=${IMAGE_TAG}

docker image load -i ${IMAGE_NAME}_${IMAGE_TAG}.tar
docker tag ${CYBERPROTECT_REGISTRY}/${IMAGE_NAME}:${IMAGE_TAG} ${INTERNAL_REGISTRY}/$
↪{INTERNAL_IMAGE_NAME}:${INTERNAL_IMAGE_TAG}
docker push ${INTERNAL_REGISTRY}/${INTERNAL_IMAGE_NAME}:${INTERNAL_IMAGE_TAG}
```

4. Укажите новое имя Docker-образа в конфигурационном файле агента для Kubernetes `/opt/acronis/etc/dsp.k8s/k8s-agent.json` в поле `cluster_config.docker_image`.

5. В конфигурационном файле агента для Kubernetes укажите учетные данные для доступа во внутренний Docker-репозиторий, использовав один из следующих способов:

   - **Base64-строка с учетными данными для доступа во внутренний Docker-репозиторий**

     1. Получите строку с учетными данными в формате Base64, выполнив команду:

```
kubectl create secret docker-registry regcred \
  --docker-server=<YOUR_INTERNAL_DOCKER_REGISTRY> \
  --docker-username=<YOUR_DOCKER_USER> \
  --docker-password=<YOUR_DOCKER_PASSWORD> \
  --docker-email=<YOUR_DOCKER_EMAIL> \
  --dry-run=server -o json | jq '.data.”.dockerconfigjson”' -r
```

2. Укажите строку из вывода команды в поле `cluster_config.docker_image_pull_secret` конфигурационного файла агента для Kubernetes `/opt/acronis/etc/dsp.k8s/k8s-agent.json`.

- **Файл с учетными данными для доступа во внутренний Docker-репозиторий**

1. Создайте файл с учетными данными, выполнив команду:

```
kubectl create secret docker-registry regcred \
  --docker-server=<YOUR_INTERNAL_DOCKER_REGISTRY> \
  --docker-username=<YOUR_DOCKER_USER> \
  --docker-password=<YOUR_DOCKER_PASSWORD> \
  --docker-email=<YOUR_DOCKER_EMAIL> \
  -dry-run=server -o json | jq '.data.”.dockerconfigjson”' -r | base64 -d > <YOUR_
↪DOCKER_CREDENTIALS_FILE.json>
```

2. Разместите полученный файл с учетными данными на машине с агентом для Kubernetes.
3. Укажите путь к файлу с учетными данными в поле `cluster_config.docker_image_pull_secret` конфигурационного файла агента для Kubernetes `/opt/acronis/etc/dsp.k8s/k8s-agent.json`.

6. Перезапустите агент для Kubernetes:

```
/opt/acronis/aakore restart --unit dsp.k8s
```

Защита SAP HANA

В этом разделе описывается решение для создания согласованных резервных копий серверов с SAP HANA. Это решение позволяет восстанавливать серверы SAP HANA до состояния bare-metal, на том же или другом оборудовании, переносить их с физической машины на виртуальную и наоборот.

Кибер Бэкап использует механизм подготовки моментальных снимков SAP HANA для создания согласованных с приложениями резервных копий всего сервера SAP HANA на уровне дисков. Это решение дает следующие преимущества:

- Восстановление на ”голое железо” на то же или другое оборудование с поддержкой LVM.
- Преобразование физического в виртуальное и виртуального в физическое, включая преобразование в виртуальную машину по расписанию.
- Практически мгновенное восстановление путем запуска виртуальной машины VMware ESXi из резервной копии сервера SAP HANA.

Поддерживаемые версии SAP HANA

Поддерживаемые версии SAP HANA указаны в разделе *Поддерживаемые СУБД*.

Поскольку SAP HANA не поддерживает восстановление контейнеров баз данных с несколькими арендаторами с использованием моментальных снимков хранилища, данное решение поддерживает контейнеры SAP HANA с базой данных только одного арендатора.

Резервное копирование физических серверов

Предварительные условия

- В вашей среде установлен сервер управления Кибер Бэкап. См. раздел *Установка сервера управления*.
- Вы можете войти на сервер управления с помощью поддерживаемого браузера. См. раздел *Доступ к веб-консоли Кибер Бэкап*.
- Агент Кибер Бэкап для Linux установлен на компьютере с SAP HANA и добавлен на сервер управления. См. раздел *Добавление машины с ОС Linux*.
- Компьютеру, на котором работает SAP HANA, назначена лицензия: Расширенная редакция для физического сервера.

Установка сценариев

1. Загрузите файл https://download.cyberprotect.ru/releases/AcronisDataProtection/SAP-HANA-modules.tar
2. Распакуйте файл:

```
tar -xvf SAP-HANA-modules.tar
```

3. Предоставьте права на исполняемый файл сценарию установки:

```
sudo chmod 777 setup.sh
```

4. Запустите сценарий установки:

```
setup.sh
```

Настройка доступа к базам данных

1. Перейдите в каталог:

```
cd /usr/lib/Acronis/SAPHANA/bash/
```

2. Укажите учетные данные доступа с помощью команд, приведенных ниже.

   Пользователь, чьи учетные данные вы указываете, должен иметь права Администратора резервного копирования и права чтения каталогов в соответствующем экземпляре.

   - Чтобы добавить данные учетной записи, указав имя пользователя и пароль:

     ```
     sudo ./config.sh ADD -i <instance_number> -d <database> -u <user> -p <password>
     ```

     Данные учетной записи, добавленные вами, будут сохранены в `/var/lib/Acronis/SAPHANA/Config/config.yaml` и будут доступны только пользователю root. Пароль будет закодирован в base64 и не зашифрован.

   - Чтобы добавить пользователя из безопасного хранилища пользователей:

     ```
     sudo ./config.sh ADD -i <instance_number> -d <database> -U <key>
     ```

   - Чтобы удалить учетные данные для определенной базы данных:

     ```
     ./config.sh REMOVE -i <instance_number> -d <database>
     ```

   - Чтобы просмотреть список добавленных учетных данных:

     ```
     sudo ./config.sh LIST
     ```

   - Чтобы просмотреть учетные данные для определенной базы данных:

     ```
     sudo ./config.sh GET -i <instance_number> -d <database>
     ```

3. Укажите путь установки SAP HANA:

```
sudo ./config.sh SET_INSTALL_PATH --install_path <path>
```

Здесь `<path>` — это путь к файлу `sapservices`, который используется в SAP HANA для отслеживания места установки баз данных. Путь по умолчанию — `/usr/sap`.

Создание плана резервного копирования

В соответствии с вашими требованиями к защите сервера создайте план резервного копирования для всего сервера SAP HANA, как описано в разделе *Резервное копирование*.

При создании плана:

1. Нажмите **Изменить** рядом с параметром **Параметры резервного копирования**, а затем выберите параметр **Команды до или после захвата данных**.
2. Активируйте переключатель **Выполнение команды до захвата данных**.
3. В поле **Команда или путь к файлу пакета на машине с агентом** введите путь к сценарию предварительного захвата данных:

   ```
   /usr/lib/Acronis/SAPHANA/bash/pre_freeze.sh
   ```

4. Активируйте переключатель **Выполнение команды после захвата данных**.
5. В поле **Команда или путь к файлу пакета на машине с агентом** введите путь к сценарию последующего захвата данных.

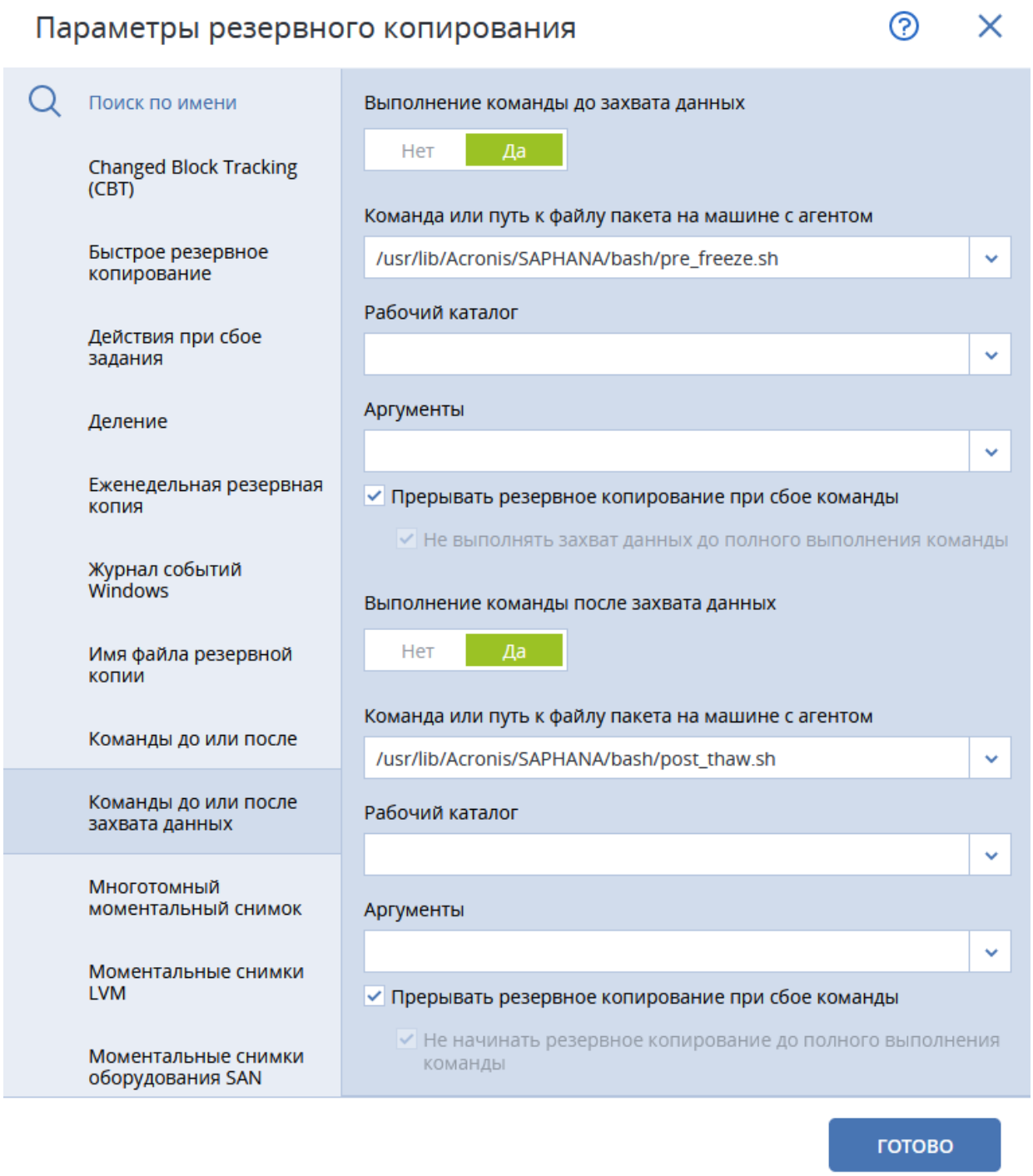
   - Если вы не хотите усекать журналы:

     ```
     /usr/lib/Acronis/SAPHANA/bash/post_thaw.sh
     ```

   - Если вы хотите усекать журналы после каждого резервного копирования.

     ```
     /usr/lib/Acronis/SAPHANA/bash/post_thaw_with_truncate_logs.sh
     ```

     Этот измененный сценарий удалит журналы повторов после успешного закрытия моментального снимка.



6. Выберите параметр **Многотомный моментальный снимок** и убедитесь, что он включен.
7. Нажмите **Готово**.
8. При необходимости укажите другие параметры плана резервного копирования, а затем нажмите **Создать**.

План резервного копирования будет создан и применен к вашему серверу SAP HANA. Резервные копии, созданные с помощью этого плана, будут содержать согласованную базу данных, при этом будут

использоваться мощные функциональные возможности, которые предусмотрены для всех резервных копий на уровне дисков.

Резервное копирование виртуальных серверов

Предварительные условия

- Виртуальная машина VMware ESXi работает под управлением SAP HANA и имеет установленные инструменты VMware.
- В вашей среде установлен сервер управления Кибер Бэкап. См. раздел *Установка сервера управления*.
- Вы можете войти на сервер управления с помощью поддерживаемого браузера. См. раздел *Доступ к веб-консоли Кибер Бэкап*.
- Агент Кибер Бэкап для VMware установлен в VMware vSphere или на компьютере с Windows и добавлен на сервер управления. См. раздел *Добавление vCenter или хоста ESXi*.
- ESXi, на котором размещена виртуальная машина под управлением SAP HANA, назначена лицензия: Расширенная редакция для физического сервера.

Дальнейшие шаги

Войдите в гостевую систему и выполните процедуры ”Установка сценариев” и ”Настройка доступа к базам данных”, описанные в разделе *Резервное копирование физических серверов*.

Создайте план резервного копирования для резервного копирования всего сервера SAP HANA в соответствии с вашими требованиями к защите сервера, как описано в разделе *Резервное копирование*. Для виртуальных машин не нужно указывать команды предварительного и последующего сбора данных. Сценарии будут автоматически вызываться инструментами VMware каждый раз, когда требуется моментальный снимок с остановкой. Однако убедитесь, что параметр **Многотомный моментальный снимок** включен.

Чтобы включить или отключить усечение журнала, отредактируйте файл `/usr/sbin/post-thaw-script`. По умолчанию этот сценарий вызывает `/usr/lib/Acronis/SAPHANA/bash/post_thaw.sh`, что означает, что журналы не усекаются. Чтобы включить усечение, измените строку `/usr/lib/Acronis/SAPHANA/bash/post_thaw.sh` на `/usr/lib/Acronis/SAPHANA/bash/post_thaw_with_truncate_logs.sh`.

Восстановление всего сервера

Восстановите физический или виртуальный сервер, как описано в разделе *Восстановление машины*.

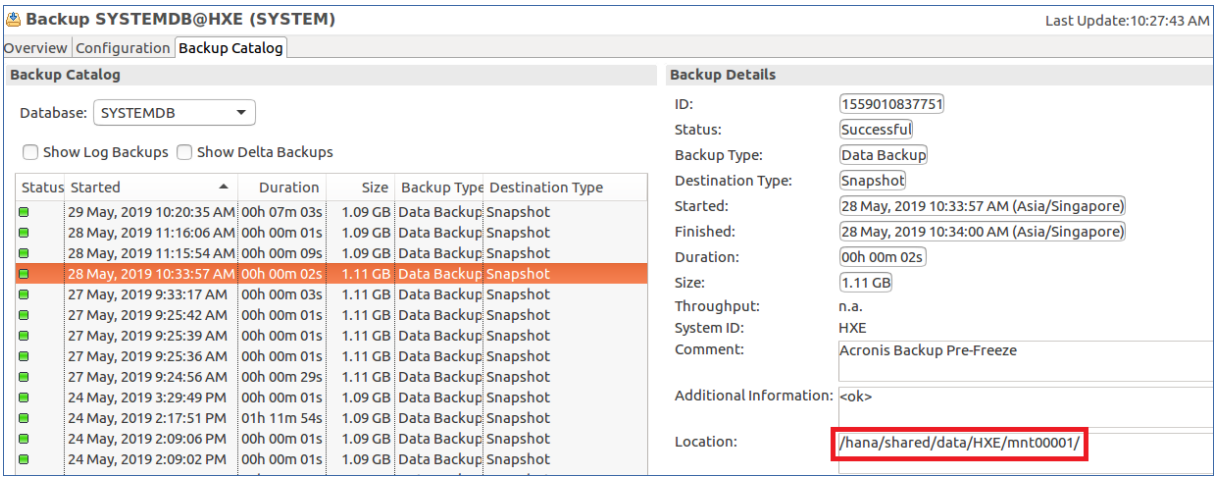
Если вы хотите запустить виртуальную машину VMware ESXi из резервной копии, действуйте, как описано в разделе *Запуск виртуальной машины из резервной копии (мгновенное восстановление)*.

Восстановление базы данных с помощью SAP HANA Studio

Если нет необходимости восстанавливать весь сервер, вы можете вернуть базу данных к моментальному снимку с помощью собственных инструментов SAP HANA. Ниже приведены примеры восстановления базы данных из моментальных снимков HANA, созданных во время выполнения команд предварительного сбора данных.

Эти моментальные снимки можно распознать по комментарию ”Pre-Freeze” (Предварительная заморозка) в сведениях о резервном копировании, например, в каталоге резервных копий SAP HANA.

Перед началом восстановления отметьте папку, в которой находятся моментальные снимки:



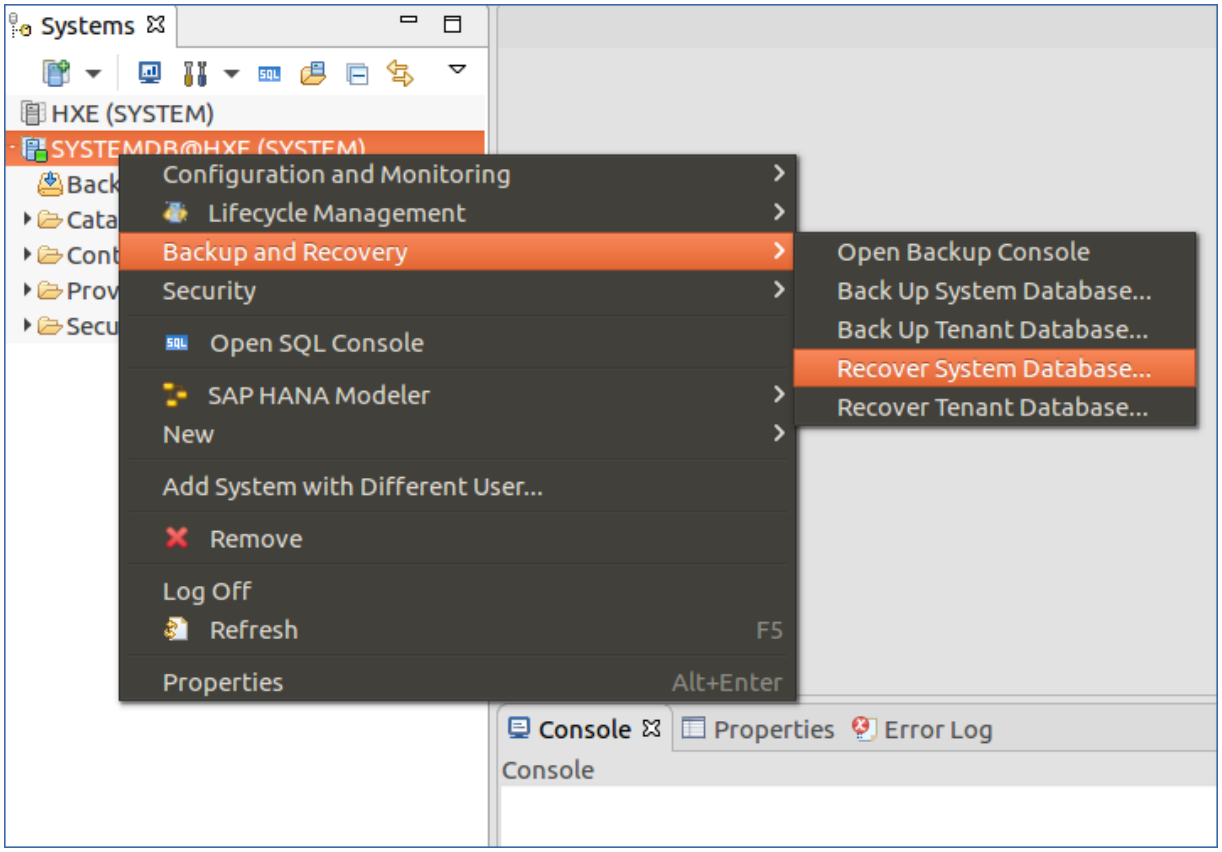
Во время восстановления мы сначала восстановим папку, содержащую моментальный снимок, а затем вернем базы данных к этому моментальному снимку с помощью SAP HANA Studio.

Восстановление из последней резервной копии

1. Остановите службы SAP.
    1. Откройте терминал и переключитесь на пользователя SAP HANA: `su <sid>adm`. Например, `su hxeadm`.
    2. Наберите `HDB stop`.
2. Восстановите папку, в которой находятся моментальные снимки из самой последней резервной копии, созданной Кибер Бэкап. Процедура восстановления описана в разделе *Восстановление*

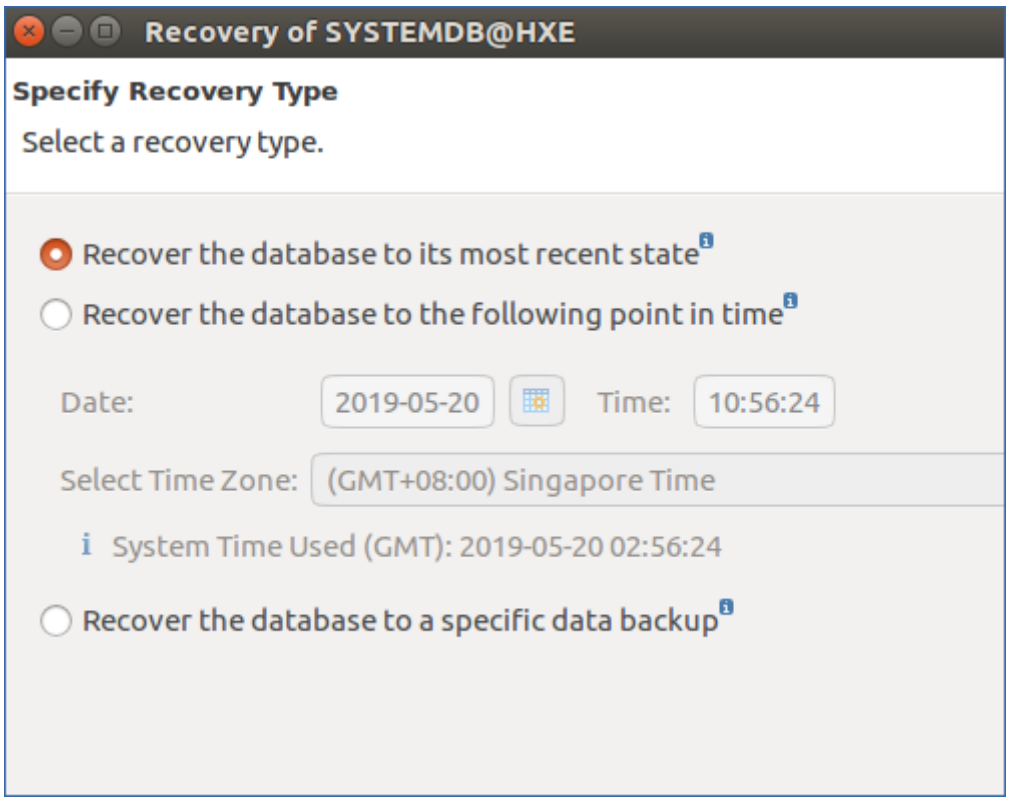
файлов с помощью веб-интерфейса.

3. Запустите SAP HANA Studio.
4. Щёлкните правой кнопкой мыши на системной базе данных, а затем выберите **Backup and Recovery (Резервное копирование и восстановление) → Recover System Database... (Восстановить системную базу данных)**.

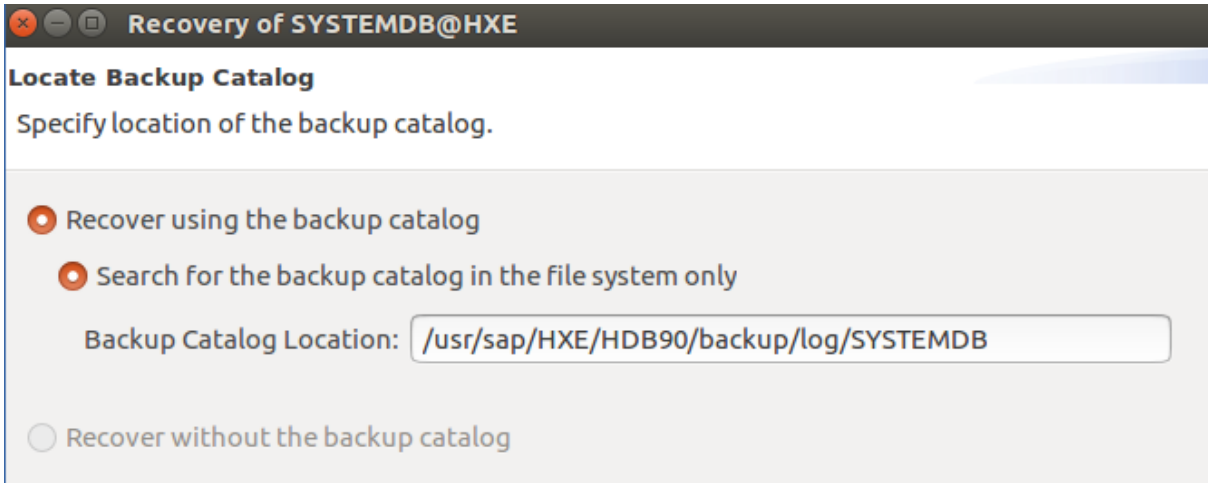


5. Выберите **Recover the database to its most recent state (Восстановить базу данных до ее последнего**

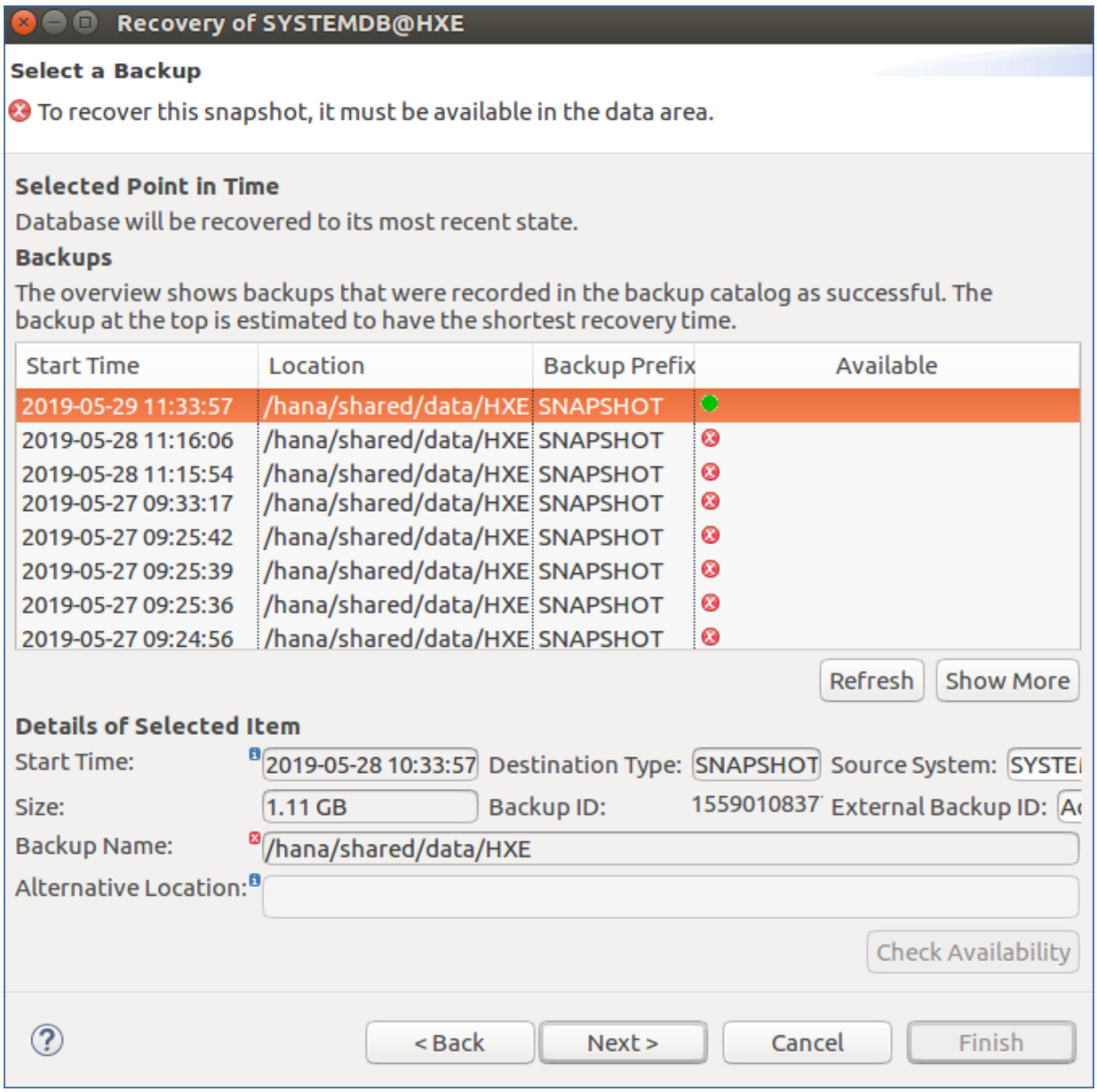
состояния).



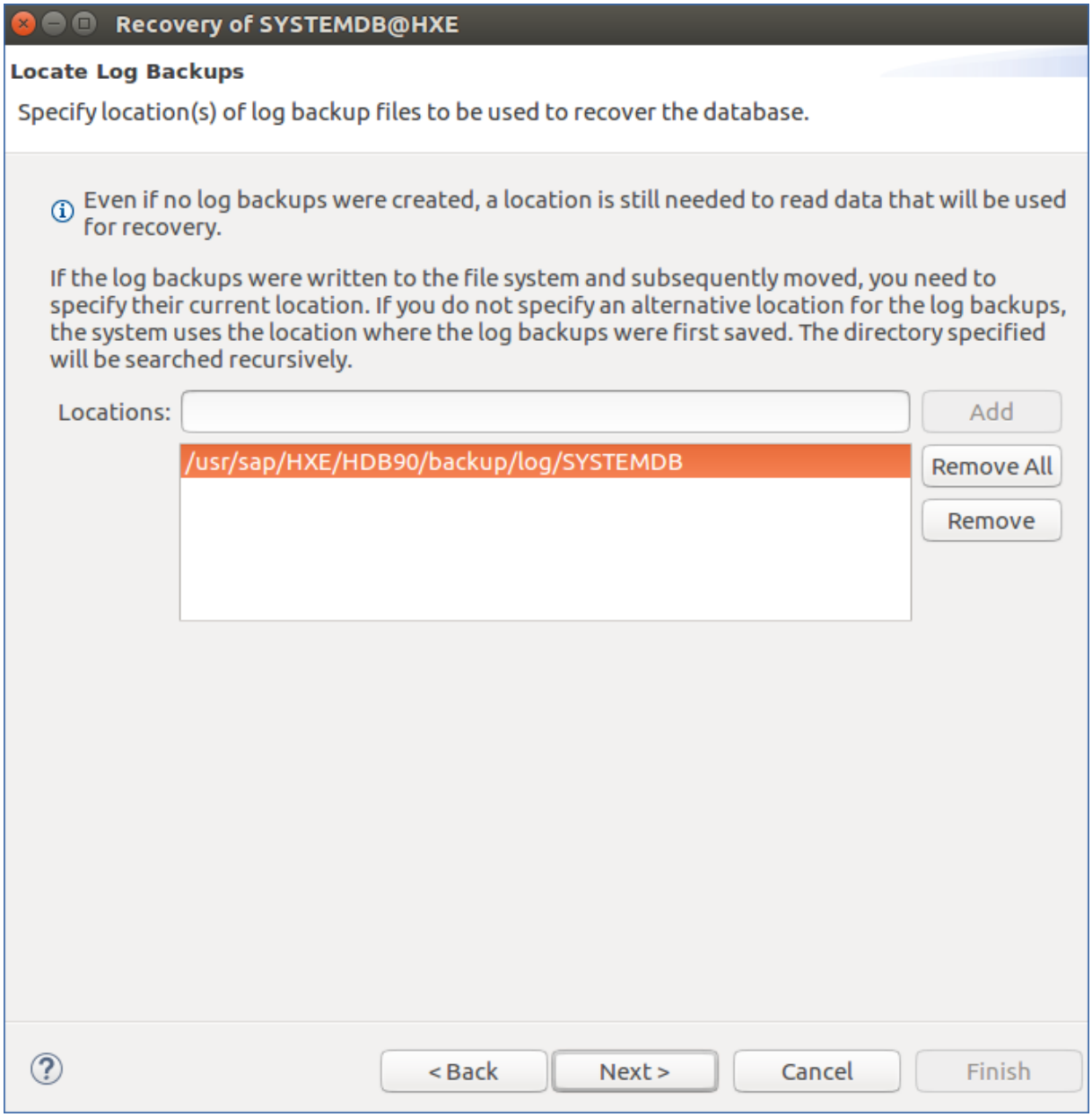
6. Проверьте путь к каталогу резервных копий и при необходимости измените его.



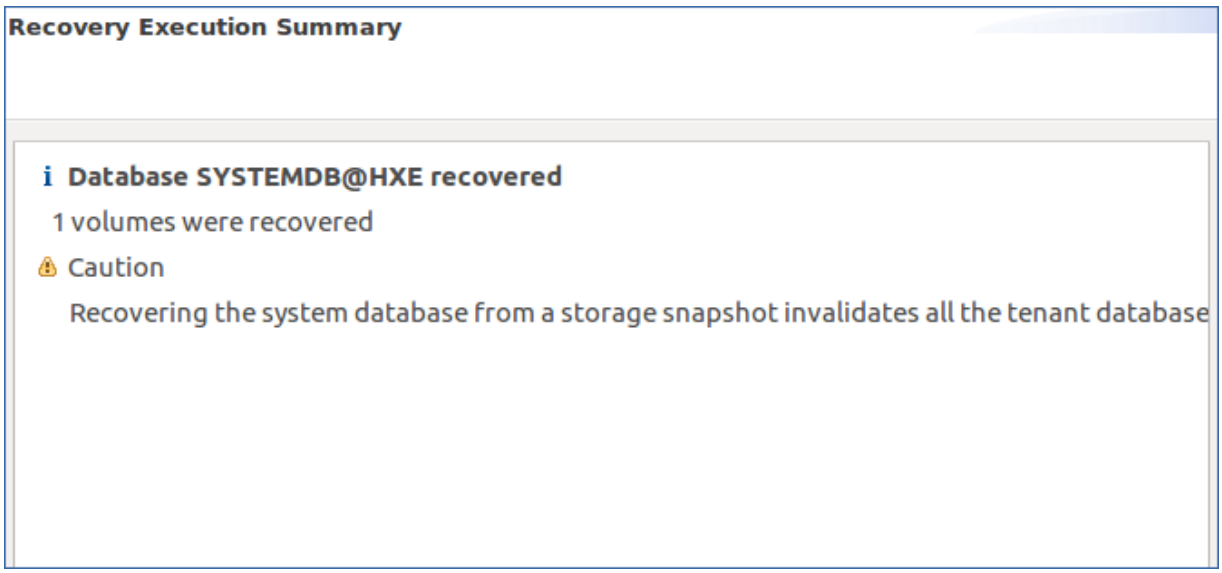
7. Последний снимок должен быть доступен, поскольку он был восстановлен на шаге 2. Если это не так, нажмите **Refresh (Обновить)**.



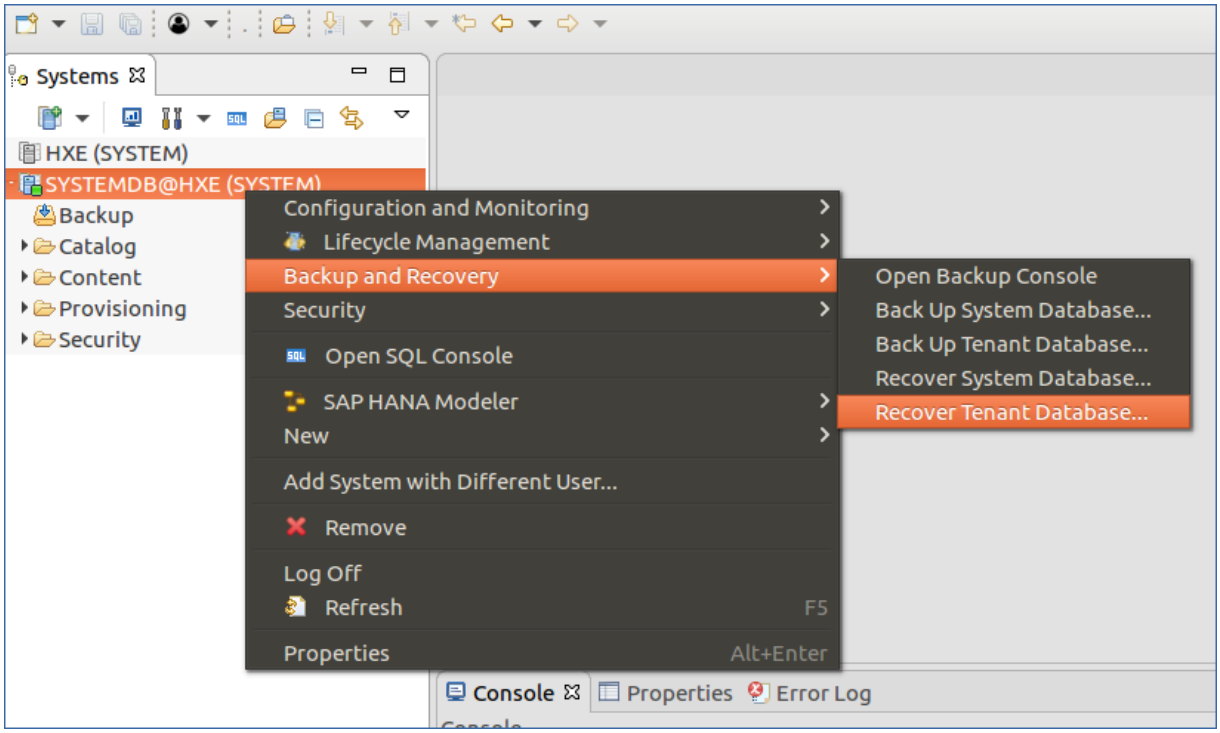
8. Проверьте путь к файлам журнала и при необходимости измените его.



9. На шаге **Other Settings (Прочие настройки)** оставьте настройки по умолчанию и нажмите **Next (Далее)**.
10. Проверьте параметры восстановления и нажмите **Finish (Завершить)**. После успешного восстановления будет отображено сообщение о базе данных клиента.



11. Щёлкните правой кнопкой мыши по системной базе данных, а затем выберите **Backup and Recovery (Резервное копирование и восстановление) → Recover Tenant Database... (Восстановить клиентскую базу данных)**.

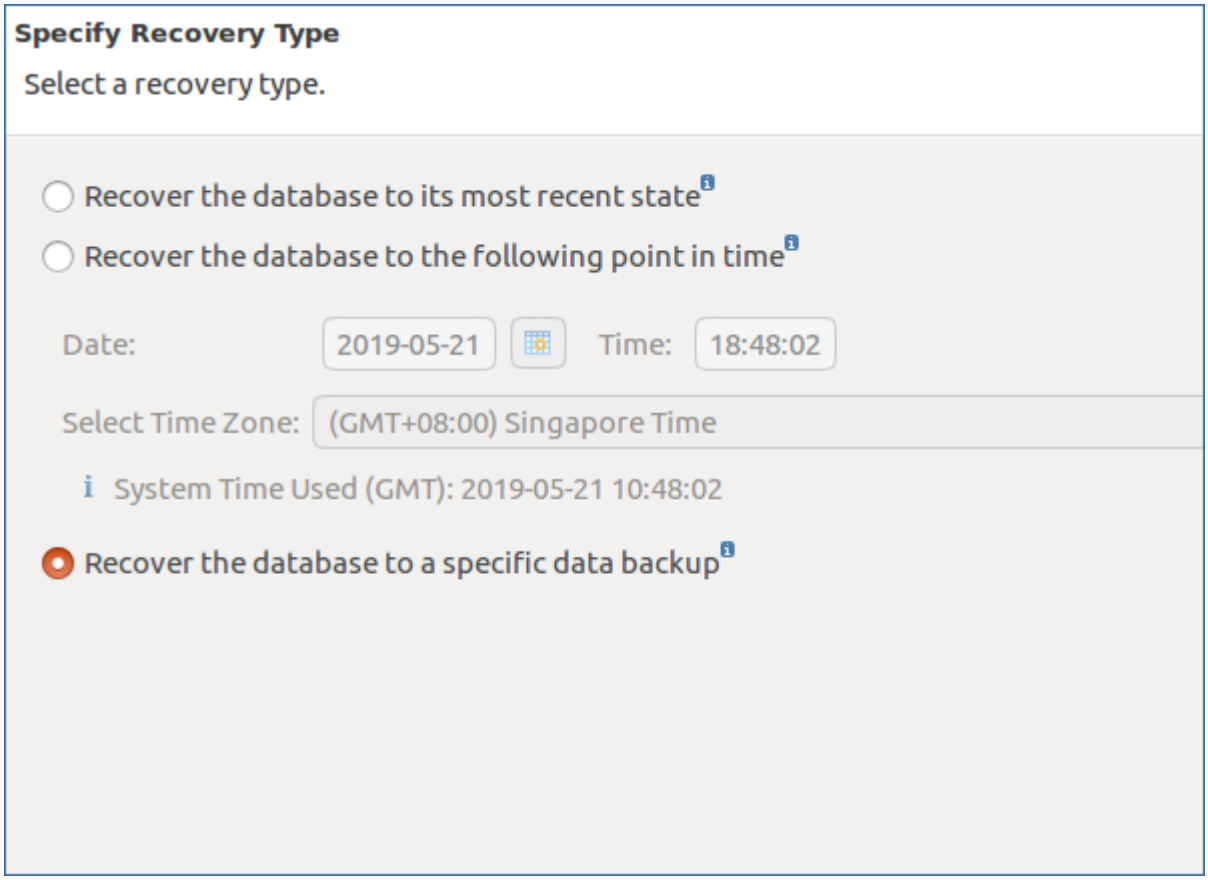


12. Повторите шаги 5-10 для клиентской базы данных.

13. После успешного восстановления откройте терминал, переключитесь на пользователя SAP HANA, а затем введите `HDB start`.

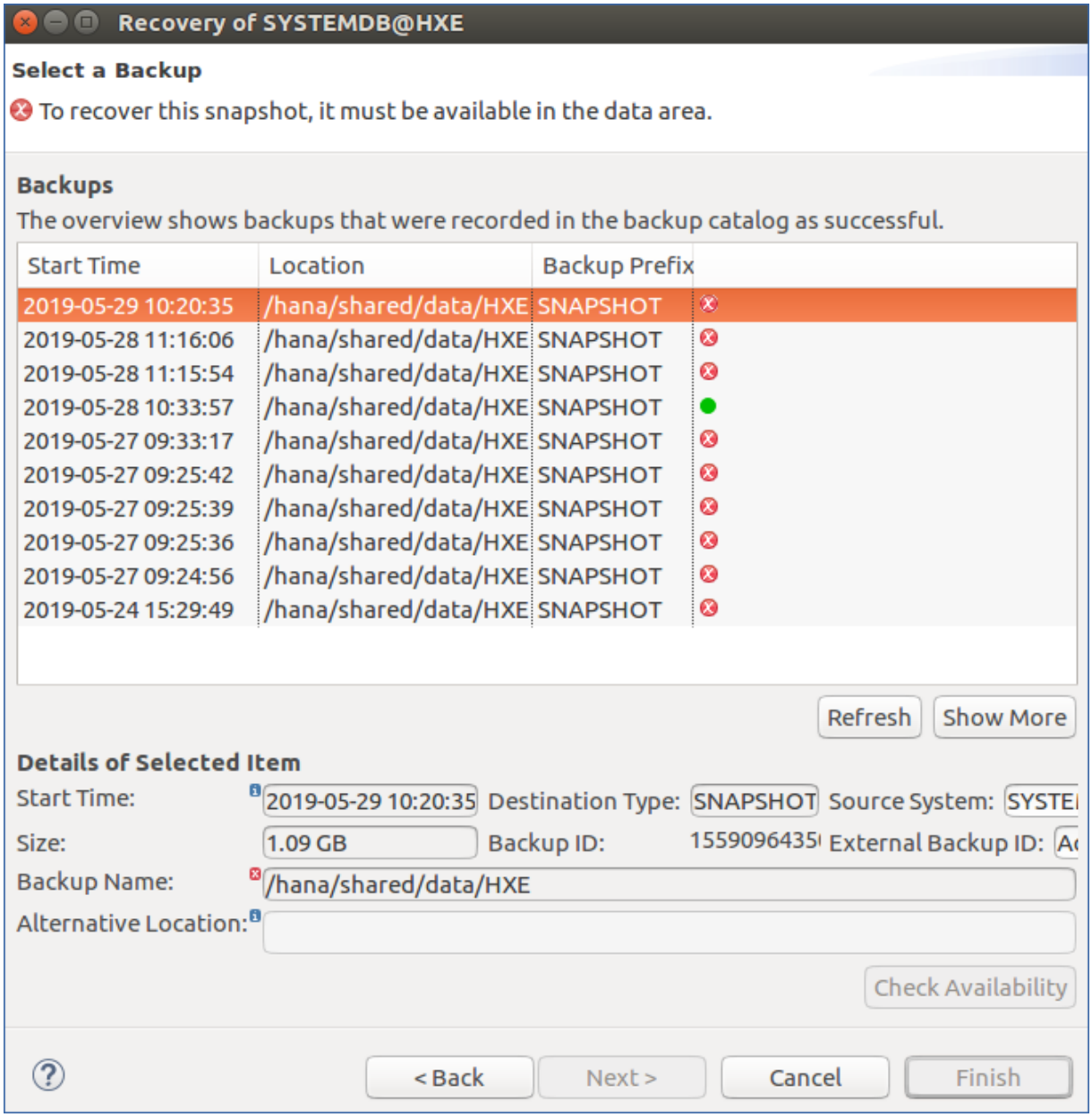
Восстановление из определенной резервной копии

1. Запустите SAP HANA studio и войдите в системную базу данных.
2. Щёлкните правой кнопкой мыши на системной базе данных, а затем выберите **Backup and Recovery (Резервное копирование и восстановление)** → **Recover System Database... (Восстановить системную базу данных)**.
3. Выберите **Recover the database to a specific data backup (Восстановить базу данных из определенной резервной копии)**, а затем щёлкните **Next (Далее)**.

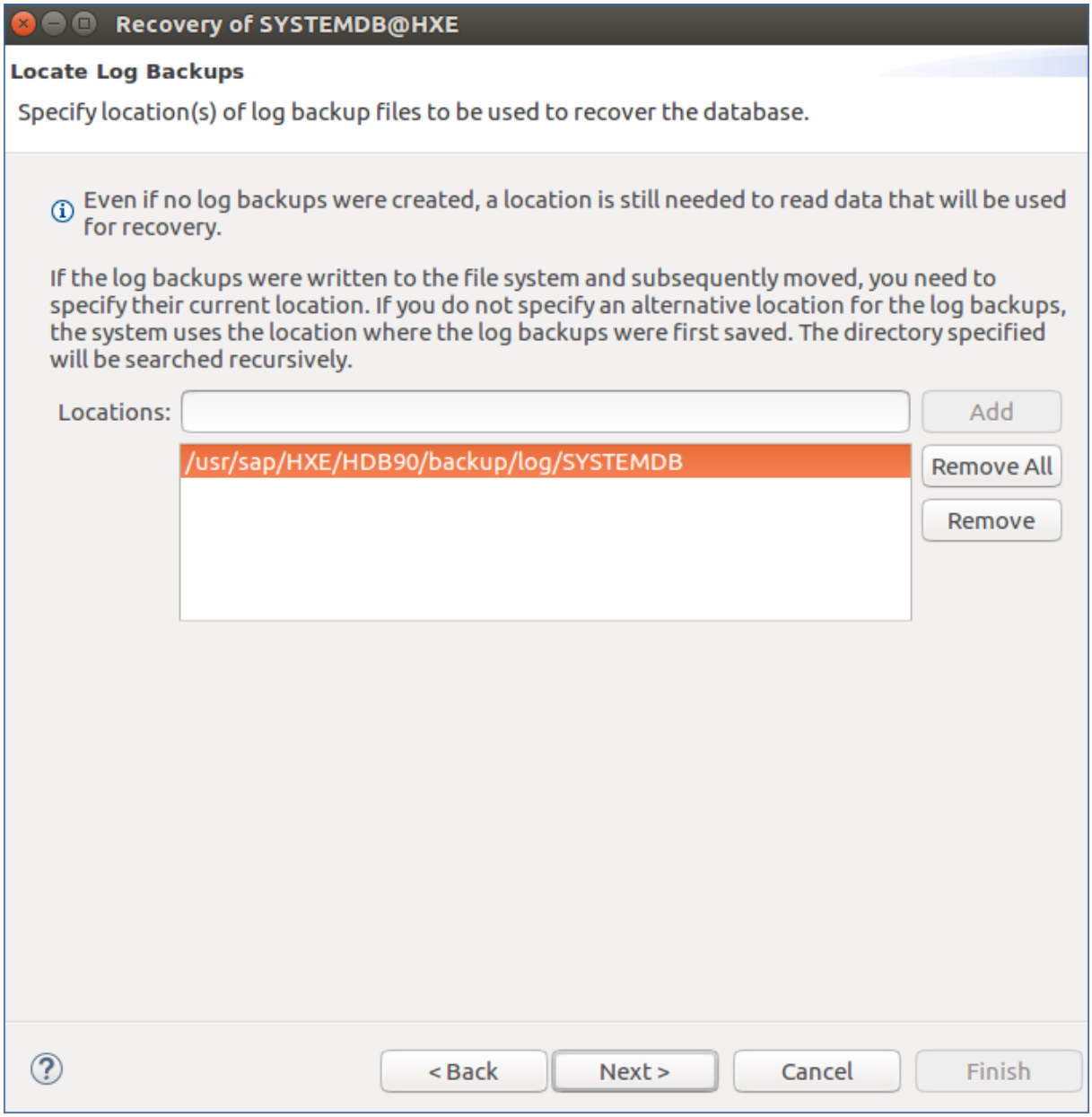


4. Выберите **Recover using the backup catalog (Восстановить с использованием каталога резервных копий)**. Проверьте путь к каталогу резервных копий и при необходимости измените его.
5. В каталоге резервных копий моментальные снимки отображаются как недоступные. Выберите моментальный снимок, к которому нужно вернуть базу данных, и отметьте **Start Time (Время начала)** моментального снимка.
6. Восстановите папку, в которой находятся снимки, из резервной копии, созданной в момент, соответствующий значению **Start Time (Время начала)**. Процедура восстановления описана в разделе *Восстановление файлов с помощью веб-интерфейса*.
7. Вернитесь в каталог резервных копий и нажмите **Refresh (Обновить)**. Выбранный снимок теперь

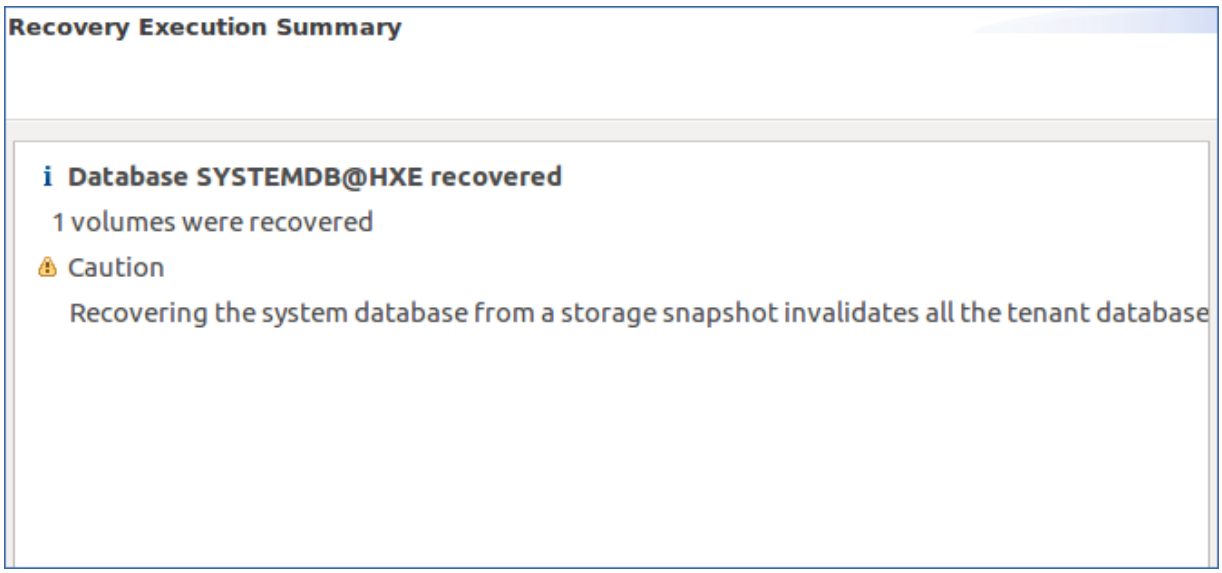
отображается как доступный. Выберите этот снимок и нажмите **Next (Далее)**.



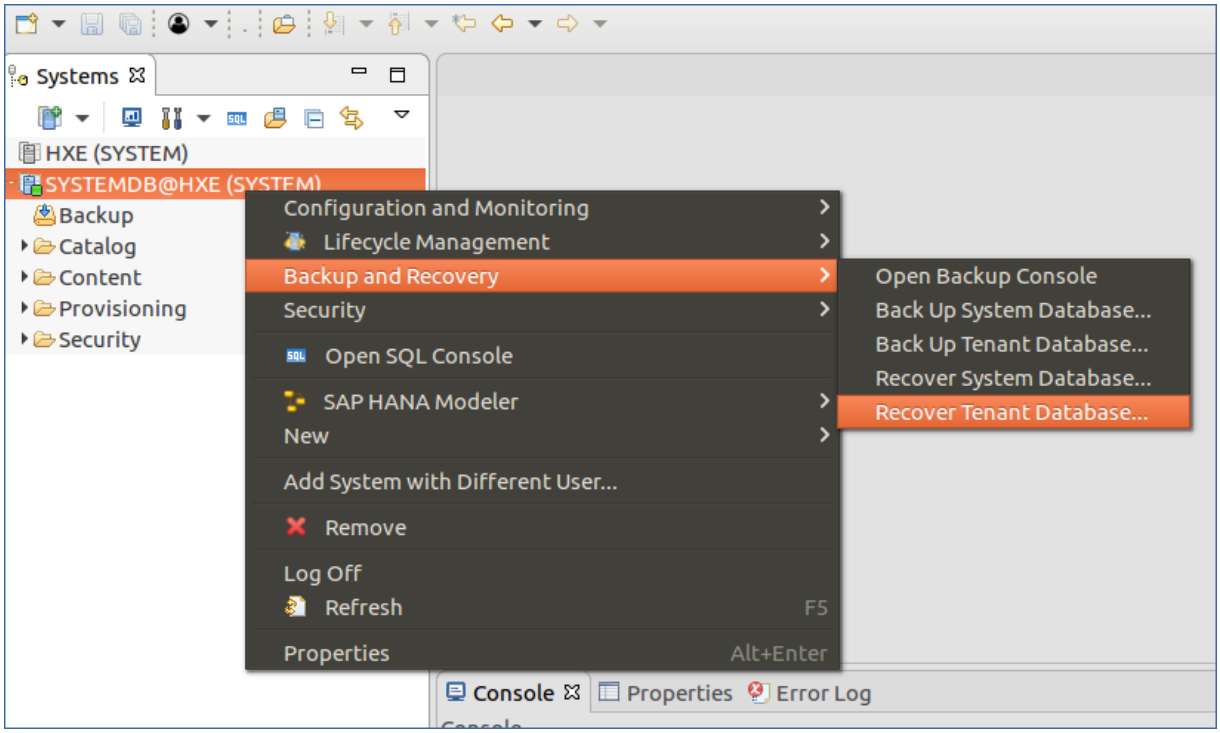
8. Проверьте путь к файлам журнала и при необходимости измените его.



9. На шаге **Other Settings (Прочие настройки)** оставьте настройки по умолчанию и нажмите **Next (Далее)**.
10. Проверьте параметры восстановления и нажмите **Finish (Завершить)**. После успешного восстановления будет отображено сообщение о базе данных клиента.



11. Щёлкните правой кнопкой мыши по системной базе данных, а затем выберите **Backup and Recovery (Резервное копирование и восстановление) → Recover Tenant Database... (Восстановить клиентскую базу данных)**.



12. Повторите шаги 3-4 и 7-10 для клиентской базы данных.

13. После успешного восстановления откройте терминал, переключитесь на пользователя SAP HANA, а затем введите `HDB start`.

Специальные операции с виртуальными машинами

Запуск виртуальной машины из резервной копии (мгновенное восстановление)

Можно запустить виртуальную машину с резервной копии на уровне дисков, которая содержит операционную систему. Эта операция, которая также известна как мгновенное восстановление, позволяет ускорить виртуальный сервер за считанные секунды. Виртуальные диски эмулируются непосредственно с резервной копии и поэтому не занимают место в хранилище данных. Место хранения требуется только для того, чтобы сохранить изменения в виртуальных дисках.

Рекомендуем запустить эту временную виртуальную машину на срок до трех дней. После этого можно полностью удалить ее или преобразовать в обычную виртуальную машину (финализировать) без простоя.

Пока существует временная виртуальная машина, правила хранения нельзя применить к резервной копии, которая используется этой машиной. Резервные копии исходной машины могут продолжать выполняться.

Примеры использования

- **Аварийное восстановление**

  Мгновенное восстановление виртуальной машины, на которой произошел сбой.

- **Тестирование резервного копирования**

  Запустите машину с резервной копии и убедитесь в том, что гостевая ОС и приложения работают правильно.

- **Доступ к данным приложения**

  Когда машина запущена, воспользуйтесь встроенными инструментами управления в приложении, чтобы получить доступ к требуемым данным и извлечь их.

Предварительные требования

- В службе Защиты Данных необходимо зарегистрировать хотя бы один агент для VMware или агент для Hyper-V.
- Резервная копия может храниться в сетевой папке, на узле хранения или в локальной папке машины, на которой установлен агент для VMware или агент для Hyper-V. Сетевая папка должна быть доступной с данной машины. Виртуальную машину невозможно запустить из резервной копии, хранящейся на сервере SFTP, на ленточном устройстве или в зоне безопасности.
- Резервная копия должна содержать всю машину или все тома, которые необходимы для запуска операционной системы.
- Могут использоваться резервные копии физических и виртуальных машин.
- Резервные копии с логическими томами Linux (LVM) должны создаваться агентом для VMware или агентом для Hyper-V. При этом тип виртуальной машины должен быть идентичен типу исходной машины (ESXi или Hyper-V).

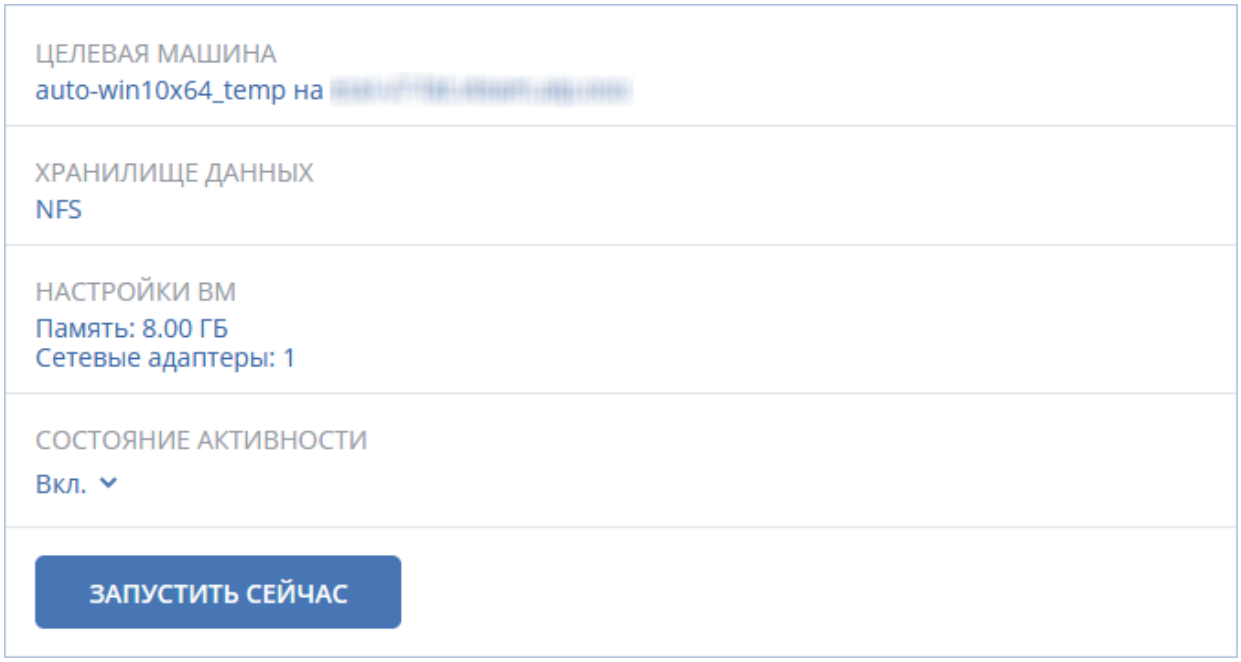
Примечание

Мгновенное восстановление из резервной копии физической Linux-машины с логическими томами (LVM) не поддерживается.

Запуск машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке *Хранилища резервных копий*.
2. Щёлкните **Запустить как ВМ**.

   Программа автоматически выберет хост и другие требуемые параметры.



3. [Необязательно] Щёлкните **Целевая машина**, затем измените тип виртуальной машины (ESXi или Hyper-V), хост или имя виртуальной машины.
4. [Необязательно] Щёлкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.

   Изменения, внесенные в виртуальные диски, накапливаются, пока машина запущена. Убедитесь, что в выбранном хранилище данных достаточно свободного пространства. Если вы намерены сохранить эти изменения, *сделав виртуальную машину постоянной*, выберите хранилище данных, подходящее для запуска машины в рабочей среде.
5. [Необязательно] Щёлкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.
6. [Необязательно] Выберите состояние активности ВМ (**Включено**/**Выключено**).
7. Щёлкните **Запустить сейчас**.

В результате этого машина появляется в веб-интерфейсе с одним из следующих значков:  или 

. Такие виртуальные машины невозможно выбрать для резервного копирования.

Удаление машины

Не рекомендуется удалять временную виртуальную машину непосредственно в vSphere/Hyper-V. Это может привести к возникновению артефактов в веб-интерфейсе. Кроме того, резервная копия, с которой запускалась машина, может быть заблокирована в течении некоторого времени (невозможно будет ее удалить согласно правилам хранения).

Порядок удаления виртуальной машины, которая запущена из резервной копии

1. На вкладке **Физические и виртуальные машины** выберите машину, которая запущена из резервной копии.
2. Щёлкните **Удалить**.

Машина будет удалена из веб-интерфейса. Она также удаляется из инвентаря и хранилища данных vSphere или Hyper-V. Все изменения данных, которые были внесены, когда машина была запущена, будут утрачены.

Финализация машины

Когда виртуальная машина запущена из резервной копии, содержимое виртуальных дисков берется непосредственно из этой резервной копии. Поэтому при утрате подключения к хранилищу резервных копий или агенту защиты машина становится недоступной или даже повреждается.

Эту машину можно сделать постоянной, то есть восстановить все ее виртуальные диски вместе с изменениями, внесенными при работе машины, в хранилище данных, в котором хранятся эти изменения. Этот процесс называется финализацией.

Финализация выполняется без простоя. При выполнении финализации виртуальная машина *не* выключается.

Расположение окончательных виртуальных жестких дисков определяется в параметрах операции *Запустить как ВМ* (**Хранилище данных** для ESXi или **Путь** для Hyper-V). Прежде чем запускать финализацию, убедитесь, что свободное место, возможности предоставления общего доступа и производительность этого хранилища данных позволяют запустить машину в рабочей среде.

Порядок финализации машины, которая запущена из резервной копии

1. На вкладке **Физические и виртуальные машины** выберите машину, которая запущена из резервной копии.
2. Щёлкните **Финализировать**.

3. [Необязательно] Укажите новое имя для данной машины.
4. [Необязательно] Измените режим распределения ресурсов диска. По умолчанию задана настройка **Экономное**.
5. Щёлкните **Финализировать**.

Имя машины сразу же меняется. Ход выполнения восстановления показан на вкладке **Действия**. После выполнения восстановления значок машины меняется на значок постоянной виртуальной машины.

Сравнение финализации и обычного восстановления

Процесс финализации выполняется медленнее обычного восстановления по указанным ниже причинам:

- При выполнении финализации агент в случайном порядке выбирает разные части резервной копии. При восстановлении всей машины агент считывает данные из резервной копии последовательно.
- Если при выполнении финализации запущена виртуальная машина, агент считывает данные из резервной копии более часто. Это необходимо для одновременной поддержки обоих процессов. При обычном восстановлении виртуальная машина останавливается.

Работа в VMware vSphere

В этом разделе описаны операции, характерные для среды VMware vSphere.

Репликация виртуальных машин

Репликация доступна только для виртуальных машин VMware ESXi.

Репликация — это процесс создания точной копии (реплики) виртуальной машины с последующей поддержкой реплики в синхронизированном состоянии с исходной машиной. Репликация критически важных машин позволяет всегда иметь копию этой машины в готовом к запуску состоянии.

Репликацию можно запустить вручную или по расписанию, которое определяется пользователем. Первая репликация является полной (выполняется копирование всей машины). Все последующие репликации являются инкрементными и выполняются с помощью функции *Changed Block Tracking*, если этот параметр не отключен.

Репликация и резервное копирование

В отличие от запланированных процессов резервного копирования, в реплику сохраняется только актуальное на момент создания реплики состояние. Для реплики необходимо пространство хранилища данных, а резервные копии могут храниться на более дешевых хранилищах данных.

Однако включение реплики выполняется гораздо быстрее, чем восстановление и запуск виртуальной машины из резервной копии. Включенная реплика работает быстрее виртуальной машины, запущенной из резервной копии и не загружает агент для VMware.

Примеры использования

- **Репликация виртуальных машин на удаленную площадку.**

  Репликация позволяет сохранить работоспособность при частичном или полном отказе центра обработки данных. Это возможно за счет клонирования виртуальных машин с основной площадки на вторичную площадку. Эта вторичная площадка обычно располагается на удаленном оборудовании, которое не подвергается воздействию тех факторов окружающей среды, инфраструктурных или иных факторов, которые могли привести к отказу основной площадки.

- **Репликация виртуальных машин в рамках одной площадки (с одного хоста/хранилища данных на другой хост/другое хранилище данных).**

  Репликацию на месте можно использовать в сценариях High Availability и аварийного восстановления.

Действия, которые можно выполнить с репликой

- *Проверка реплики*

  Реплика будет включена для тестирования. Чтобы проверить правильность работы реплики, воспользуйтесь клиентом vSphere или другими инструментами. При выполнении тестирования репликация приостанавливается.

- *Переход к реплике*

  Перенос рабочей нагрузки с исходной виртуальной машины на ее реплику. При выполнении перехода к реплике репликация приостанавливается.

- Резервное копирование реплики

  Как для резервного копирования, так и для репликации необходим доступ к виртуальным дискам. Это влияет на производительность работы хоста, на котором запущена виртуальная машина. Если необходимо иметь и реплику, и резервные копии виртуальной машины, то, чтобы не создавать дополнительную нагрузку для рабочего хоста, реплицируйте машину на другой хост и задайте

резервные копии данной реплики.

Ограничения

Невозможно выполнить репликацию указанных ниже типов виртуальных машин:

- Машины, которые запущены из резервных копий.
- Реплики виртуальных машин.

Создание плана репликации

План репликации необходимо создать отдельно для каждой машины. Невозможно применить существующий план к другим машинам.

Порядок создания плана репликации:

1. Выберите виртуальную машину для репликации.
2. Щёлкните **Репликация**.

   В программе отображается новый шаблон плана репликации.
3. [Необязательно] Чтобы изменить имя плана репликации, щёлкните имя по умолчанию.
4. Щёлкните **Целевая машина** и выполните указанные ниже действия:
   1. Выберите, создавать ли новую или использовать уже существующую реплику исходной машины.
   2. Выберите хост ESXi и укажите имя новой реплики или выберите существующую реплику.

      Новая реплика будет иметь имя по умолчанию **[Имя первоначальной машины]_replica**.
   3. Нажмите кнопку **ОК**.
5. [Только при репликации на новую машину] Щёлкните **Хранилище данных** и выберите хранилище данных для виртуальной машины.
6. [Необязательно] Щёлкните **Расписание**, чтобы изменить расписание репликации.

   По умолчанию репликация выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска репликации.

   Чтобы изменить частоту выполнения репликации, перетащите ползунок и задайте расписание.

   Можно также выполнить следующие действия:

   - Задать интервал дат, в течение которого будет использоваться указанное расписание. Установите флажок **Выполнять план в диапазоне дат** и укажите диапазон дат.

- Отключить расписание. В этом случае репликацию можно запустить вручную.

7. [Необязательно] Щёлкните значок шестерни, чтобы изменить *параметры репликации*.
8. Нажмите кнопку **Применить**.
9. [Необязательно] Чтобы запустить план вручную, щёлкните **Запустить сейчас** на панели плана.

В результате выполнения плана репликации реплика виртуальной машины появляется в списке **Физические и виртуальные машины** с указанным ниже значком:



Тестирование реплики

Порядок подготовки реплики к тестированию

1. Выберите реплику для тестирования.
2. Щёлкните **Тестировать реплику**.
3. Щёлкните **Начать тестирование**.
4. Выберите, подключить ли включённую реплику к сети. По умолчанию реплика не подключена к сети.

   Для возможности остановки тестирования реплики в блоке **Сетевое подключение** выберите **Подключить при включённом питании**. В противном случае кнопка **Остановить тестирование** будет неактивна.
5. [Необязательно] Если выбрано подключение реплики к сети, установите флажок **Остановить исходную виртуальную машину**, чтобы остановить исходную виртуальную машину до включения реплики.
6. Нажмите кнопку **Запустить**.

Порядок остановки тестирования реплики

1. Выберите реплику, для которой выполняется тестирование.
2. Щёлкните **Тестировать реплику**.
3. Щёлкните **Остановить тестирование**.
4. Подтвердите операцию.

Переход к реплике

Переход с машины к реплике

1. Выберите реплику, к которой необходимо перейти.
2. Щёлкните **Действия с репликой**.
3. Щёлкните **Переход к реплике**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика будет подключена к той же сети, что и исходная машина.
5. [Необязательно] Если выбрано подключение реплики к сети, снимите флажок **Остановить исходную виртуальную машину**, чтобы не выключать исходную виртуальную машину.
6. Нажмите кнопку **Запустить**.

При выполнении перехода к реплике можно выбрать одно из указанных ниже действий:

- *Остановить переход к реплике*

  Остановите переход к реплике, если исходная машина исправлена. Реплика будет выключена. Репликация будет продолжена.

- *Выполнить окончательный переход на реплику*

  Эта мгновенная операция позволяет удалить флаг ”реплика” из виртуальной машины, чтобы сделать репликацию невозможной. Чтобы продолжить репликацию, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.

- *Возврат из реплики*

  Выполните возврат из реплики, если выполнен переход на площадку, которая не предназначена для непрерывных операций. Реплика будет восстановлена на исходную или новую виртуальную машину. По окончании восстановления на исходную машину она включается и репликация продолжается. Если выбрано восстановление на новую машину, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.

Остановка перехода к реплике

Порядок остановки перехода к реплике:

1. Выберите реплику, к которой выполняется переход.
2. Щёлкните **Действия с репликой**.
3. Щёлкните **Остановить переход к реплике**.

4. Подтвердите операцию.

Выполнение окончательного перехода на реплику

1. Выберите реплику, к которой выполняется переход.
2. Щёлкните **Действия с репликой**.
3. Щёлкните **Окончательный переход на реплику**.
4. Подтвердите операцию.
5. [Необязательно] Измените имя виртуальной машины.
6. [Необязательно] Установите флажок **Остановить исходную виртуальную машину**.
7. Нажмите кнопку **Запустить**.

Возврат из реплики

Порядок выполнения возврата из реплики

1. Выберите реплику, к которой выполняется переход.
2. Щёлкните **Действия с репликой**.
3. Щёлкните **Возврат из реплики**.

   Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.
4. [Необязательно] Щёлкните **Целевая машина** и выполните следующие действия:
   1. Выберите новую или существующую машину для возврата из реплики.
   2. Выберите хост ESXi и укажите имя новой машины или выберите существующую машину.
   3. Нажмите кнопку **ОК**.
5. [Необязательно] При возврате из реплики на новую машину также можно выполнить следующие действия:
   - Щёлкните **Хранилище данных**, чтобы выбрать хранилище данных для виртуальной машины.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щёлкните **Настройки ВМ**.
6. [Необязательно] Щёлкните **Параметры восстановления**, чтобы изменить *параметры возврата из реплики*.
7. Щёлкните **Начать восстановление**.

8. Подтвердите операцию.

Параметры репликации

Чтобы изменить параметры репликации, щёлкните значок шестерни рядом с именем плана репликации и нажмите **Параметры репликации**.

Функция Changed Block Tracking (CBT)

Этот параметр подобен параметру резервного копирования *Changed Block Tracking (CBT)*.

Распределение ресурсов диска

Этот параметр определяет настройки распределения ресурсов диска для реплики.

Значение по умолчанию: **Экономное распределение**.

Доступны следующие значения: **Экономное распределение**, **Неэкономное распределение**, **Сохранить первоначальную настройку**.

> **Примечание**
>
> Для виртуальных машин, диски которых расположены в NFS-хранилищах, диск для реплики всегда создаётся в режиме **Экономное распределение**.

Обработка ошибок

Этот параметр подобен параметру резервного копирования *Обработка ошибок*.

Команды до и после процедуры

Этот параметр подобен параметру резервного копирования *Команды до и после процедуры*.

Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр подобен параметру резервного копирования *Служба теневого копирования томов (VSS) для виртуальных машин*.

Параметры возврата из реплики

Чтобы изменить параметры возврата из реплики, щёлкните **Параметры восстановления** при настройке возврата из реплики.

Обработка ошибок

Этот параметр подобен параметру восстановления *Обработка ошибок*.

Производительность

Этот параметр подобен параметру восстановления *Производительность*.

Команды до и после процедуры

Этот параметр подобен параметру восстановления *Команды до и после процедуры*.

Управление питанием ВМ

Этот параметр подобен параметру восстановления *Управление питанием ВМ*.

Сохранение первоначальной реплики

Чтобы ускорить репликацию в удаленное расположение и сэкономить пропускную способность сети, можно выполнить сохранение реплики.

Важно

Для сохранения реплики агент для VMware (виртуальное устройство) должен работать на целевом хосте ESXi.

Сохранение первоначальной реплики

1. Выполните одно из следующих действий:
   - Если исходную виртуальную машину можно выключить, сделайте это, а затем перейдите к шагу 4.
   - Если исходную виртуальную машину нельзя выключить, перейдите к следующему шагу.
2. *Создайте план репликации*.

   При создании плана в разделе **Целевая машина** выберите пункт **Создать реплику** и хост ESXi, на котором размещена первоначальная машина.
3. Запустите план однократно.

   На исходном хосте ESXi будет создана реплика.
4. Экспортируйте файлы виртуальной машины (или реплики) на внешний жесткий диск.
   1. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.

2. Подключите клиент vSphere к исходному хосту vCenter\ESXi.
3. Выберите только что созданную реплику в списке.
4. Щёлкните **Файл** → **Экспорт** → **Экспорт шаблона OVF**.
5. В поле **Папка** укажите папку на внешнем жестком диске.
6. Нажмите кнопку **ОК**.

5. Перенесите жесткий диск в удаленное расположение.
6. Импортируйте реплику на целевой хост ESXi.
   1. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   2. Подключите клиент vSphere к целевому хосту vCenter\ESXi.
   3. Щёлкните **Файл** → **Развернуть шаблон OVF**.
   4. В поле **Развернуть из файла или URL-адреса** укажите шаблон, экспортированный на шаге 4.
   5. Завершите процедуру импорта.
7. Измените план репликации, созданный на шаге 2. В поле **Целевая машина** выберите **Существующая реплика**, а затем выберите импортированную реплику.

В результате программа продолжит обновлять реплику. Все репликации будут инкрементными.

Использование локально присоединенного хранилища

К агенту для виртуального устройства VMware можно подключить дополнительный диск, чтобы агент мог создавать резервные копии в этом локальном хранилище. Этот подход устраняет сетевой трафик между агентом и хранилищем резервных копий.

Виртуальное устройство, которое выполняется на одном хосте или в одном кластере с виртуальными машинами, для которых созданы резервные копии, имеет прямой доступ к хранилищам данных, в которых расположены эти машины. Это означает, что устройство может присоединить диски, для которых созданы резервные копии, используя транспорт HotAdd. В этом случае трафик резервного копирования направляется от одного локального диска к другому. Если хранилище данных подключено как диск/логическое устройство (LUN), а не как NFS, резервная копия будет работать без использования локальной сети. В случае хранилища данных NFS, будет иметь место сетевой трафик между хранилищем данных и хостом.

При использовании локально присоединенного хранилища предполагается, что агент всегда создает резервную копию для одних и тех же машин. Если несколько агентов работают в рамках vSphere и один или несколько из них используют локально присоединенные хранилища, необходимо *вручную привязать* каждый агент ко всем машинам, для которых он должен создавать резервные копии. В

противном случае, если сервер управления произведет перераспределение машин среди агентов, резервные копии машин могут оказаться рассредоточенными по нескольким хранилищам.

Можно добавить хранилище к уже работающему агенту или сделать это при развертывании агента *из шаблона OVF*.

Как прикрепить хранилище к уже работающему агенту

1. В списке VMware vSphere щёлкните правой кнопкой мыши агент для виртуального устройства VMware.
2. Добавьте диск путем внесения изменений в параметры виртуальной машины. Размер диска должен составлять по меньшей мере 10 ГБ.

   > **Предупреждение**
   >
   > Необходимо соблюдать осторожность при добавлении уже существующего диска. После создания хранилища все данные, содержавшиеся ранее на этом диске, будут потеряны.

3. Перейдите на консоль виртуального устройства. Ссылка **Создать хранилище** доступна в нижней части экрана. Если этого не происходит, нажмите **Обновить**.
4. Нажмите ссылку **Создать хранилище**, выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.

Как выбрать локально присоединенное хранилище в качестве места сохранения резервной копии

При *создании плана защиты* в области **Место сохранения резервной копии** выберите **Локальные папки** и введите букву диска, соответствующую локально присоединенному хранилищу, например **D:**.

Привязка виртуальной машины

В этом разделе показано, как сервер управления организует работу нескольких агентов в VMware vCenter.

Нижеуказанный алгоритм распределения работает как для виртуальных устройств, так и для агентов, установленных в Windows.

Алгоритм распределения

Виртуальные машины автоматически равномерно распределяются между агентами для VMware. Под равномерностью имеется в виду, что все агенты управляют равным количеством машин. Объем пространства, занимаемого в хранилище виртуальной машиной, не учитывается.

При выборе агента для машины программное обеспечение пытается оптимизировать общую производительность системы. В частности, программное обеспечение учитывает расположение агента и виртуальной машины. Предпочтительным является агент, размещенный на том же хосте. Если на том же хосте агента нет, по возможности выбирается агент из того же кластера.

Когда виртуальная машина назначается агенту, все централизованные резервные копии этой машины делегируются этому агенту.

Перераспределение

Перераспределение происходит каждый раз, когда нарушается этот баланс, или, точнее, когда дисбаланс нагрузки между агентами достигает 20 процентов. Это может произойти при добавлении или удалении машины или агента, при переносе машины на другой хост или в другой кластер или если машина привязывается к агенту вручную. В этом случае сервер управления перераспределяет машины с помощью того же алгоритма.

Например, вы понимаете, что для необходимой пропускной способности требуется больше агентов, и развертываете в кластере дополнительное виртуальное устройство. Сервер управления назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится.

Если агент удаляется с сервера управления, то машины, назначенные этому агенту, распределяются между оставшимися агентами. Однако этого не произойдет, если агент поврежден или вручную удален из vSphere. Перераспределение начнется только после удаления такого агента из веб-интерфейса.

Просмотр результата распределения

Можно просмотреть результат автоматического распределения:

- в столбце **Агент** для каждой виртуальной машины в разделе **Физические и виртуальные машины**;
- в разделе **Назначенные виртуальные машины** на панели **Сведения** при выборе агента в разделе **Настройки** → **Агенты**.

Привязка вручную

Привязка агента для VMware позволяет исключить виртуальную машину из этого процесса распределения, указав агент, который должен всегда выполнять резервное копирование этой машины. Общий баланс будет поддерживаться, но конкретная машина может быть передана другому агенту только в случае удаления исходного агента.

Порядок привязки машины к агенту

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе **Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Вручную**.
5. Выберите агент, к которому вы хотите привязать машину.
6. Нажмите кнопку **Сохранить**.

Как отвязать машину от агента

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе **Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Автоматически**.
5. Нажмите кнопку **Сохранить**.

Отключение автоматического назначения для агента

Для отключения автоматического назначения для агента VMware, чтобы исключить его из процесса распределения, укажите список машин, для которых этот агент должен выполнять резервное копирование. Прочие агенты будут поддерживать общий баланс.

Невозможно отключить автоматическое назначение для агента при отсутствии прочих зарегистрированных агентов или при отключенном автоматическом назначении для прочих агентов.

Отключение автоматического назначения для агента

1. Щёлкните **Настройки** → **Агенты**.
2. Выберите агент для VMware, для которого вы хотите отключить автоматическое назначение.
3. Нажмите **Сведения**.
4. Отключите **Автоматическое назначение**, нажав на переключатель.

Примеры использования

- Привязка вручную может быть удобна, если необходимо, чтобы агент для VMware (Windows) создал резервную копию конкретной (очень большой) машины через оптоволоконный канал, тогда как резервные копии других машин создаются виртуальными устройствами.
- Привязка вручную необходима при использовании *моментальных снимков оборудования SAN*. Привяжите агент для VMware (Windows), для которого сконфигурированы моментальные снимки оборудования SAN, к машинам, расположенным в хранилище данных SAN.
- Виртуальные машины необходимо привязать к агенту, если к агенту *локально прикреплено хранилище*.
- Отключение автоматического назначения дает возможность убедиться в том, что резервное копирование конкретной машины гарантировано будет проходить по указанному вами расписанию. Агент, отвечающий за резервное копирование только одной машины, не может быть привлечен к резервному копированию других машин в запланированное время.
- Отключение автоматического назначения полезно при наличии нескольких географически разделенных хостов ESXi. При отключении автоматического назначения и последующей привязке виртуальных машин на каждом хосте к агенту, запущенному на том же хосте вы можете быть уверены, что агент не будет выполнять резервное копирование машин, запущенных на удаленных хостах ESXi, что позволит сэкономить сетевой трафик.

Поддержка миграции VM

В этом разделе рассказывается об особенностях миграции виртуальных машин в среде vSphere, включая перемещение виртуальных машин между узлами ESXi, входящими в кластер vSphere.

vMotion

vMotion перемещает состояние и конфигурацию виртуальной машины на другой хост. При этом диски машины остаются в той же папке общего хранилища данных.

- Функциональная возможность vMotion агента для VMware (виртуальное устройство) не

поддерживается и отключена.

- Функциональная возможность vMotion виртуальной машины отключена при выполнении резервного копирования. Выполнение резервного копирования будет продолжено после завершения миграции.

Storage vMotion

Storage vMotion перемещает диски виртуальной машины из одного хранилища данных в другое.

- Функциональная возможность Storage vMotion агента для VMware (виртуальное устройство) не поддерживается и отключена.
- Функциональная возможность Storage vMotion виртуальной машины отключена при выполнении резервного копирования. Процессы резервного копирования продолжат выполняться после миграции.

Управление средами виртуализации

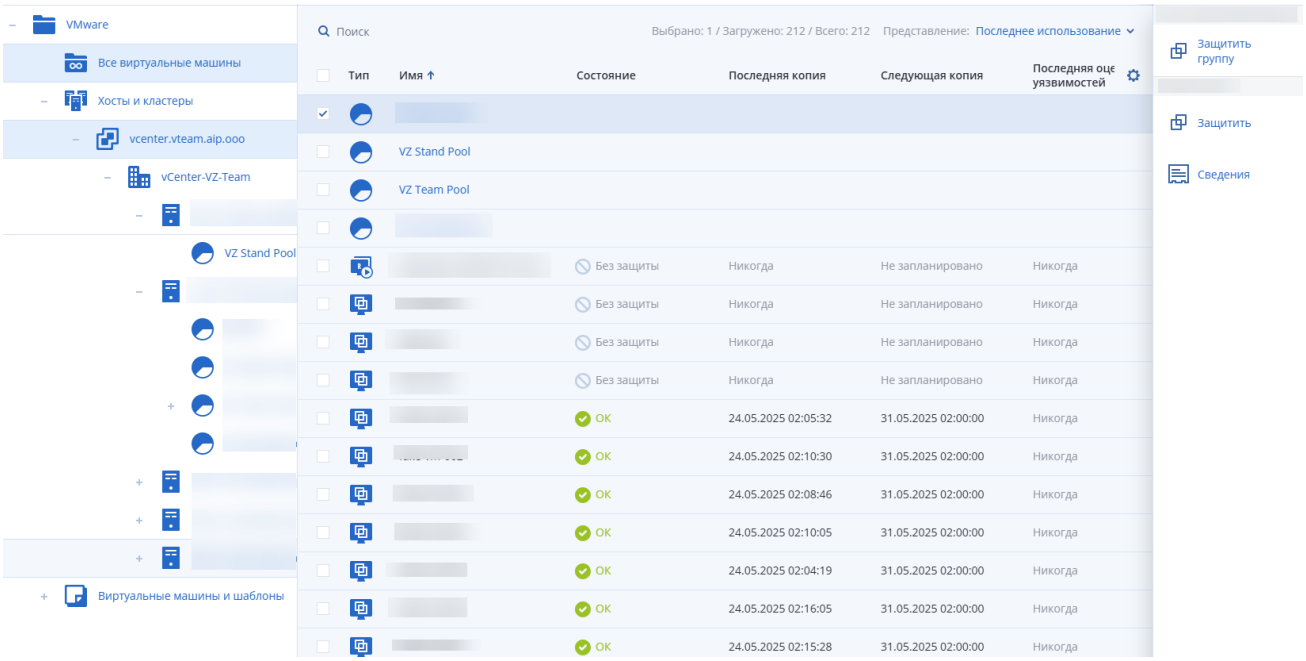
Можно просмотреть среды vSphere и Hyper-V в их собственном представлении. После установки и регистрации соответствующего агента в разделе **Устройства** появляются вкладки **VMware** или **Hyper-V**.

На вкладке **VMware** выполните резервное копирование следующих объектов инфраструктуры vSphere:

- Центр обработки данных
- Папка
- Кластер
- Хост ESXi
- Пул ресурсов

Каждый из этих объектов инфраструктуры работает как группа объектов для виртуальных машин. При применении плана защиты к любому из этих объектов группы создается резервная копия для всех виртуальных машин, которые входят в этот план. Можно создать резервную копию выбранных машин группы, щёлкнув **Защитить**, или машин родительской группы, в которую входит выбранная группа, щёлкнув **Защитить группу**.

Например, вы выбрали кластер, а затем — пул ресурсов в нем. Если щёлкнуть **Защитить**, будет создана резервная копия для всех виртуальных машин в выбранном пуле ресурсов. Если щёлкнуть **Защитить группу**, будет создана резервная копия для всех виртуальных машин в кластере.



Можно изменить учетные данные доступа vCenter Server или автономного хоста ESXi без переустановки агента.

Изменение учетных данных доступа vCenter Server или хоста ESXi

1. В разделе **Устройства** выберите **VMware**.
2. Выберите **Хосты и кластеры**.
3. В списке **Хосты и кластеры** (справа от дерева **Хосты и кластеры**) выберите vCenter Server или автономный хост ESXi, который был указан при установке агента для VMware.
4. Нажмите **Сведения**.
5. В области **Учетные данные** выберите имя пользователя.
6. Укажите новые учетные данные для доступа, а затем щёлкните **ОК**.

Просмотр статуса резервного копирования в клиенте vSphere

Можно просмотреть статус резервного копирования и время создания последней резервной копии виртуальной машины в клиенте vSphere.

Эти сведения появляются в сводке по виртуальной машине (**Сводка** → **Настраиваемые атрибуты/Аннотации/Примечания** в зависимости от типа клиента и версии vSphere). Можно также включить столбцы **Последняя резервная копия** и **Состояние резервного копирования** на вкладке **Виртуальные машины** для любого хоста, ЦОД, папки, пула ресурсов или для всего экземпляра vCenter Server.

Для предоставления этих атрибутов, помимо прав, описанных в разделе *Агент для VMware: необходимые привилегии*, агенту для VMware должны быть предоставлены следующие права:

- Глобальные > Управление настраиваемыми атрибутами,
- Глобальные > Настройка настраиваемых атрибутов.

Агент для VMware: необходимые привилегии

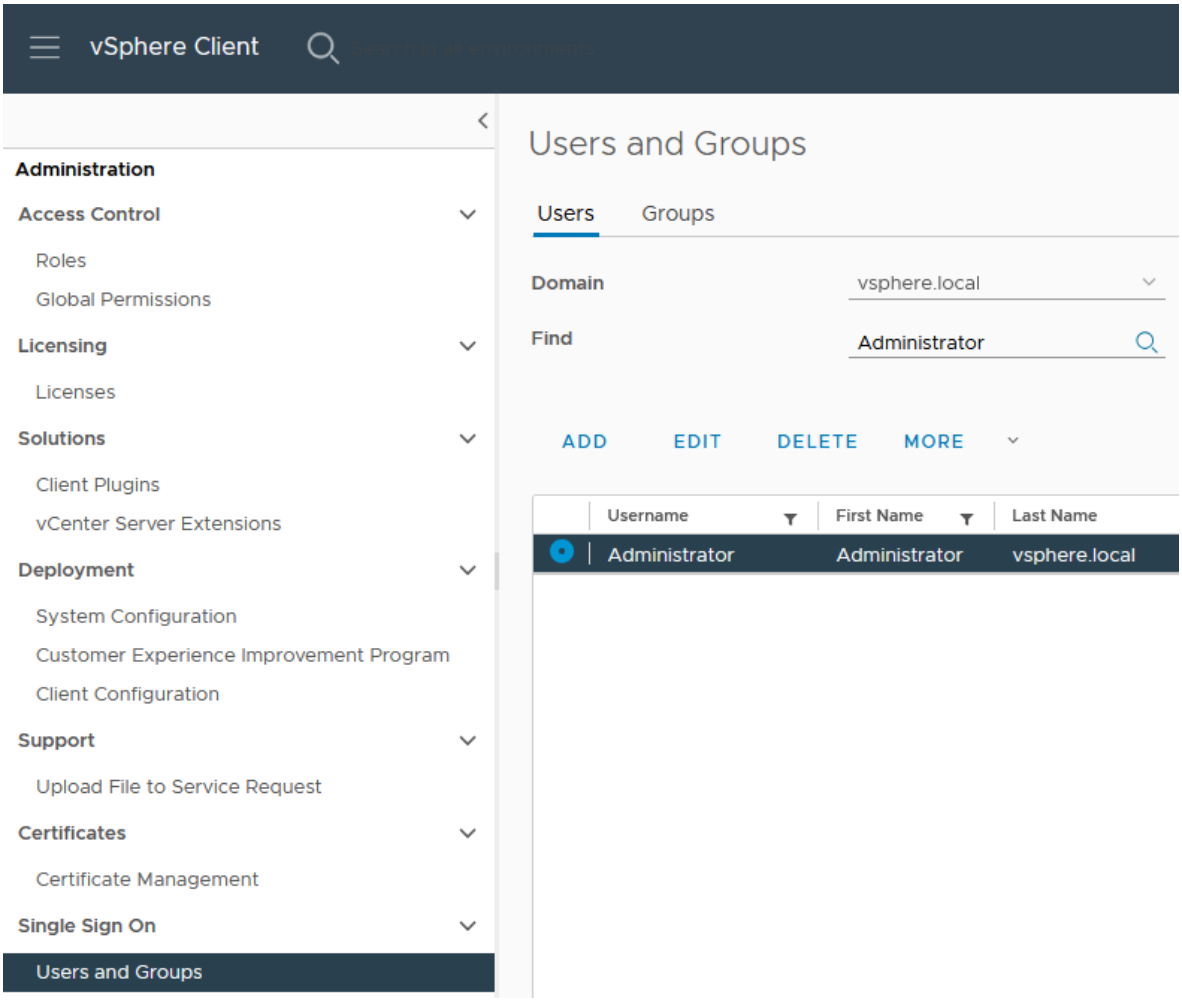
В этом разделе описаны права, необходимые для операций с виртуальными машинами ESXi, а также для развертывания виртуальных устройств.

Для выполнения любой операции с объектами vCenter (например, виртуальными машинами, хостами ESXi, кластерами, хостами vCenter и т. д.) агент для VMware выполняет аутентификацию на хосте vCenter или ESXi с учетными данными vSphere, которые указаны пользователем. Учетная запись vSphere, которая используется агентом для VMware для подключения к vSphere, должна иметь необходимые права на всех уровнях инфраструктуры vSphere, начиная с уровня vCenter.

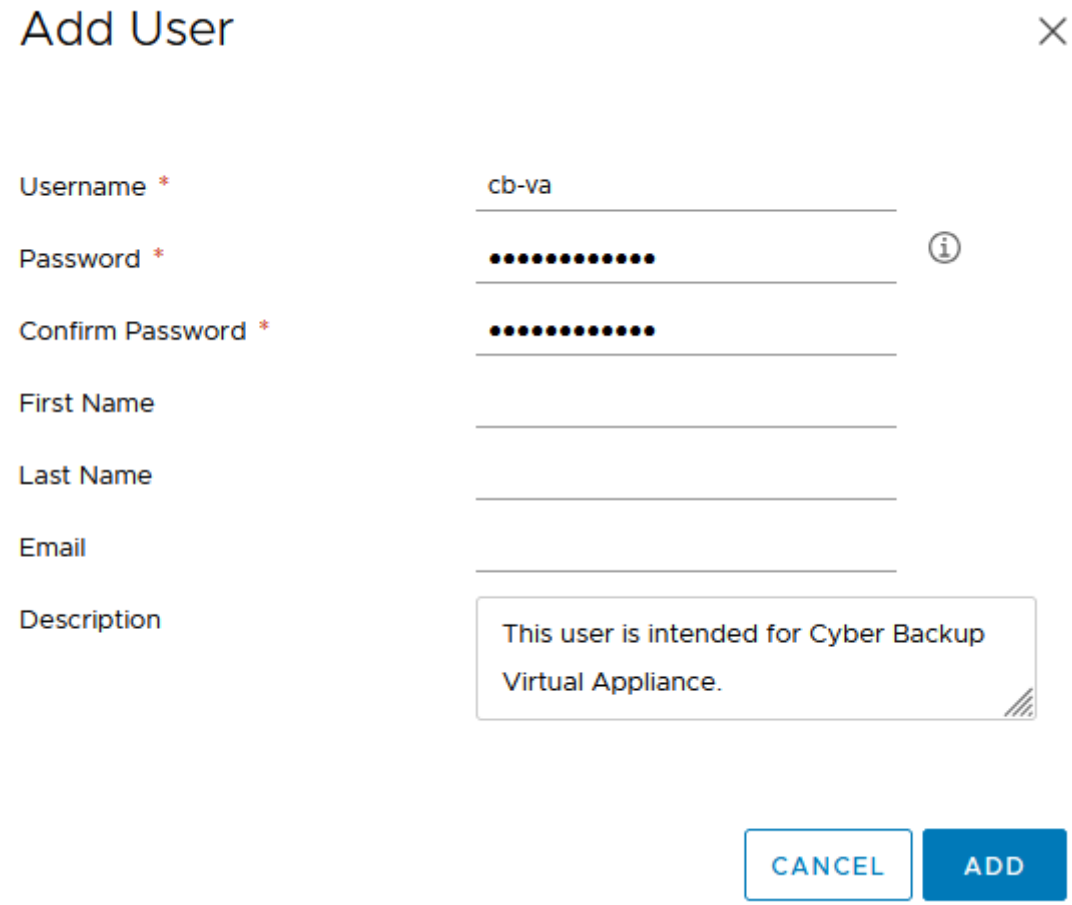
Укажите учетную запись vSphere с необходимыми правами при установке или настройке агента для VMware. Чтобы изменить учетную запись позже, см. информацию в разделе *Управление средами виртуализации*.

Порядок подготовки пользователя vSphere с необходимыми правами:

1. Подключитесь к vCenter с помощью веб-клиента vSphere, использовав учетные данные администратора.
2. Создайте пользователя:
    1. Перейдите в раздел **Administration (Администрирование)** → **Single Sign On (Единый вход)** → **Users and Groups (Пользователи и группы)**, выберите вкладку **Users (Пользователи)** и нажмите **ADD (ДОБАВИТЬ)**.

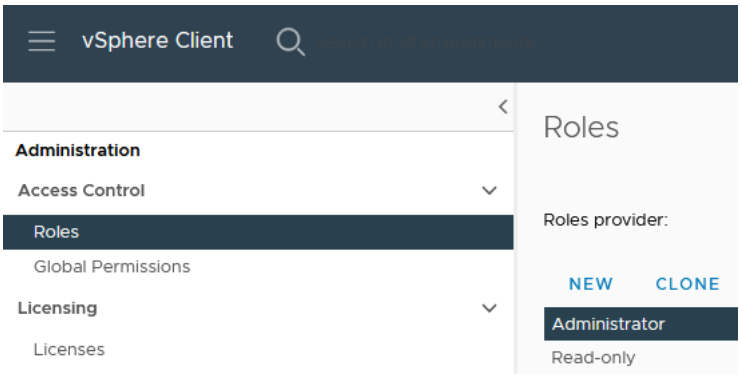


2. В окне **Add User (Добавление пользователя)** укажите имя пользователя и пароль, затем нажмите **ADD (ДОБАВИТЬ)**.



3. Создайте роль:

   1. Перейдите в раздел **Administration (Администрирование)** → **Access Control (Контроль доступа)** → **Roles (Роли)** и нажмите **NEW (НОВАЯ)**.



   2. Укажите имя роли и выберите следующие привилегии:

      - Cryptographic operations > Add disk (Операции шифрования > Добавить диск (доступно, начиная с vSphere 6.5)),
      - Cryptographic operations > Direct Access (Операции шифрования > Прямой доступ

(доступно, начиная с vSphere 6.5)),

- Datastore > Allocate space (Хранилище данных > Распределение пространства),
- Datastore > Browse datastore (Хранилище данных > Обзор хранилища данных),
- Datastore > Configure datastore (Хранилище данных > Настройка хранилища данных),
- Datastore > Low level file operations (Хранилище данных > Низкоуровневые файловые операции),
- Global > Disable methods (Глобальные > Методы отключения),
- Global > Enable methods (Глобальные > Методы включения),
- Global > Licenses (Глобальные > Лицензии),
- Global > Manage custom attributes (Глобальные > Управление настраиваемыми атрибутами),
- Global > Set custom attribute (Глобальные > Задание настраиваемых атрибутов),
- Host > Configuration > Storage partition configuration (Хост > Конфигурация > Конфигурация раздела хранения данных),
- Host > Configuration > Virtual machine autostart configuration (Хост > Конфигурация > Конфигурация автозапуска ВМ),
- Host > Configuration > Advanced settings (Хост > Конфигурация > Расширенные настройки),
- Host > Configuration > Connection (Хост > Конфигурация > Подключение),
- Host > Configuration > System management (Хост > Конфигурация > Управление системой),
- Host > Inventory > Modify cluster (Хост > Инвентарь > Изменение кластера),
- Host > Local operations > Create virtual machine (Хост > Локальные операции > Создание ВМ),
- Host > Local operations > Delete virtual machine (Хост > Локальные операции > Удаление ВМ),
- Host > Local operations > Reconfigure virtual machine (Хост > Локальные операции > Перенастройка ВМ),
- Network > Assign network (Сеть > Назначение сети),
- Resource > Assign virtual machine to resource pool (Ресурс > Назначение ВМ пулу ресурсов),
- vApp > Add virtual machine (vApp > Добавление виртуальной машины),

- vApp > Import (vApp > Импорт),
- Virtual machine > Change configuration > Acquire disk lease (Виртуальная машина > Изменение конфигурации > Аренда диска),
- Virtual machine > Change configuration > Add existing disk (Виртуальная машина > Изменение конфигурации > Добавление существующего диска),
- Virtual machine > Change configuration > Add new disk (Виртуальная машина > Изменение конфигурации > Добавление нового диска),
- Virtual machine > Change configuration > Add or remove device (Виртуальная машина > Изменение конфигурации > Добавление или удаление устройства),
- Virtual machine > Change configuration > Advanced configuration (Виртуальная машина > Изменение конфигурации > Дополнительная конфигурация),
- Virtual machine > Change configuration > Change CPU count (Виртуальная машина > Изменение конфигурации > Изменение числа ЦП),
- Virtual machine > Change configuration > Change Memory (Виртуальная машина > Изменение конфигурации > Управление ОЗУ),
- Virtual machine > Change configuration > Change Settings (Виртуальная машина > Изменение конфигурации > Изменение настроек),
- Virtual machine > Change configuration > Remove disk (Виртуальная машина > Изменение конфигурации > Удаление диска),
- Virtual machine > Change configuration > Rename (Виртуальная машина > Изменение конфигурации > Переименование),
- Virtual machine > Change configuration > Set annotation (Виртуальная машина > Изменение конфигурации > Настройка аннотации),
- Virtual machine > Change configuration > Toggle disk change tracking (Виртуальная машина > Изменение конфигурации > Включение/выключение отслеживания изменений диска),
- Virtual machine > Edit Inventory > Create from existing (Виртуальная машина > Редактирование инвентаря > Создание из существующей),
- Virtual machine > Edit Inventory > Create new (Виртуальная машина > Редактирование инвентаря > Создание новой),
- Virtual machine > Edit Inventory > Move (Виртуальная машина > Редактирование инвентаря > Перемещение),
- Virtual machine > Edit Inventory > Register (Виртуальная машина > Редактирование

инвентаря > Регистрация),

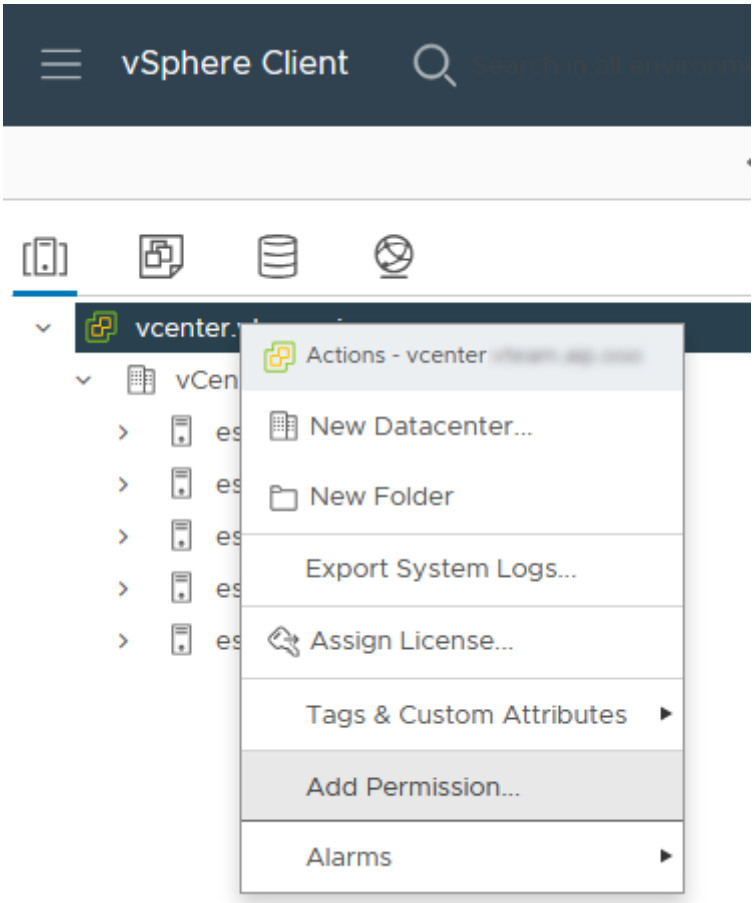
- Virtual machine > Edit Inventory > Remove (Виртуальная машина > Редактирование инвентаря > Удаление),
- Virtual machine > Edit Inventory > Unregister (Виртуальная машина > Редактирование инвентаря > Отмена регистрации),
- Virtual machine > Guest operations > Guest operation modifications (Виртуальная машина > Гостевые операции > Изменения гостевых операций),
- Virtual machine > Guest operations > Guest operation program execution (Виртуальная машина > Гостевые операции > Выполнение программы гостевой операции),
- Virtual machine > Guest operations > Guest operation queries (Виртуальная машина > Гостевые операции > Запросы гостевой операции),
- Virtual machine > Interaction > Configure CD media (Виртуальная машина > Взаимодействие > Настройка носителя CD),
- Virtual machine > Interaction > Connect devices (Виртуальная машина > Взаимодействие > Подключение устройств),
- Virtual machine > Interaction > Console interaction (Виртуальная машина > Взаимодействие > Взаимодействие с консолью),
- Virtual machine > Interaction > Guest operating system management by VIX API (Виртуальная машина > Взаимодействие > Управление гостевой операционной системой с помощью API VIX),
- Virtual machine > Interaction > Power off (Виртуальная машина > Взаимодействие > Отключение),
- Virtual machine > Interaction > Power on (Виртуальная машина > Взаимодействие > Включение),
- Virtual machine > Provisioning > Allow disk access (Виртуальная машина > Распределение > Разрешение доступа к диску),
- Virtual machine > Provisioning > Allow read-only disk access (Виртуальная машина > Распределение > Разрешение доступа к диску только для чтения),
- Virtual machine > Provisioning > Allow virtual machine download (Виртуальная машина > Распределение > Разрешение загрузки ВМ),
- Virtual machine > Snapshot management > Create snapshot (Виртуальная машина > Управление моментальными снимками > Создание моментального снимка),

- Virtual machine > Snapshot management > Remove snapshot (Виртуальная машина > Управление моментальными снимками > Удаление моментального снимка).

3. Нажмите **CREATE (СОЗДАТЬ)** для завершения создания роли.

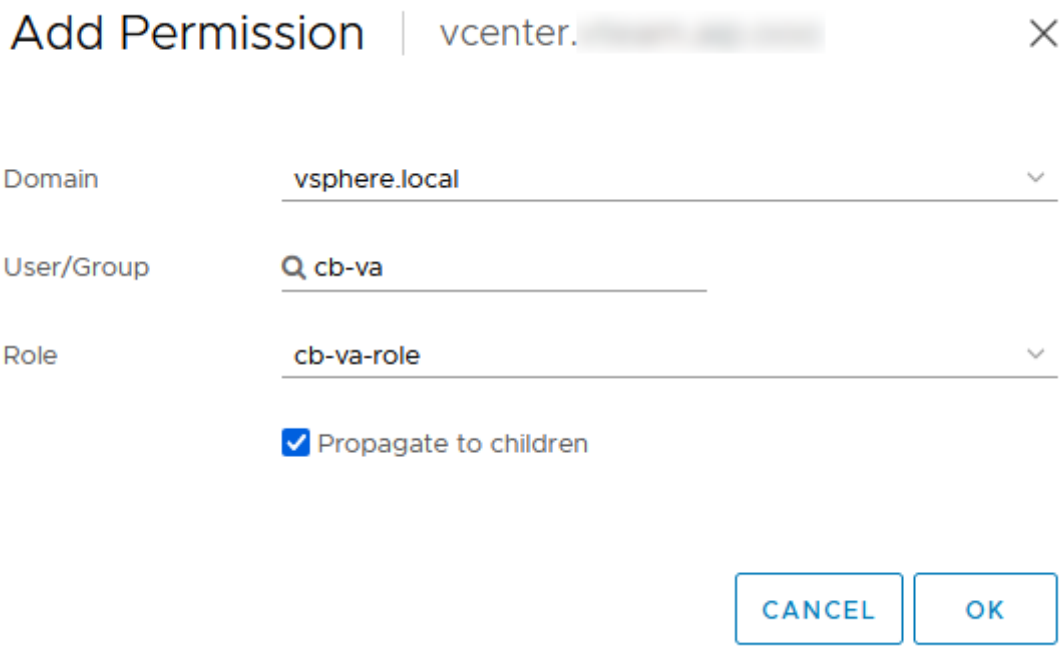
4. Назначьте пользователю роль на уровне vCenter:

   1. Перейдите в раздел **Inventory (Инвентарь)** → **Hosts and Clusters (Хосты и кластеры)** и щёлкните правой кнопкой мыши vCenter.



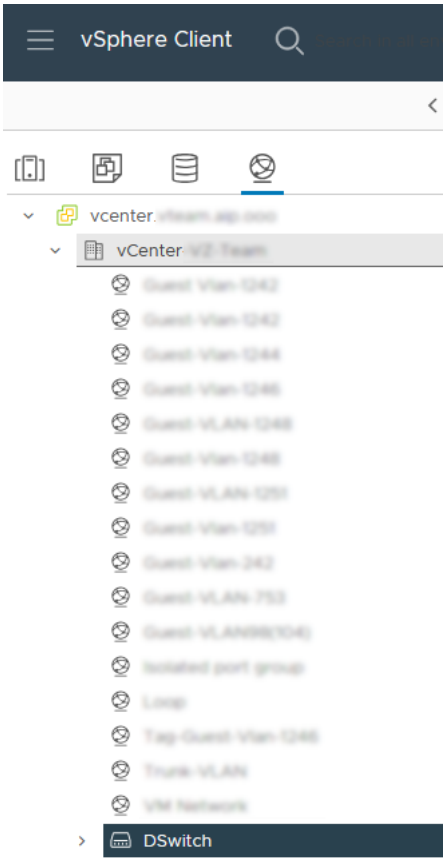
   2. В меню выберите **Add Permission (Добавить право)**.

   3. В окне **Add Permission (Добавить право)** выберите пользователя и роль, которые были созданы на предыдущих шагах, затем установите флажок **Propagate to children (Распространить на дочерние элементы)** и нажмите **OK**.

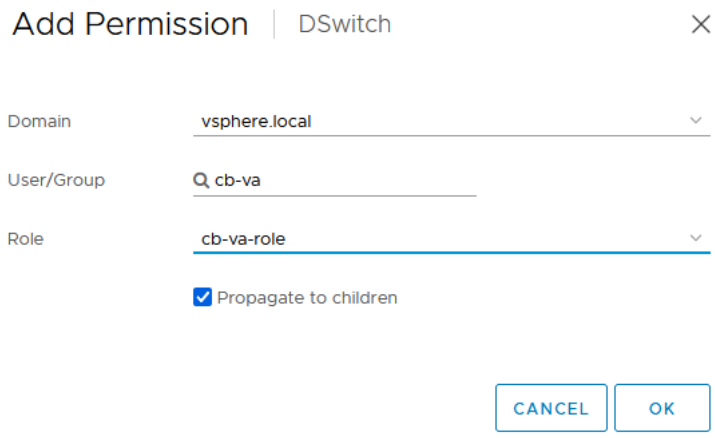


5. Назначьте пользователю роль на уровне распределенного виртуального коммутатора (dvSwitch):

    1. Перейдите в раздел **Inventory (Инвентарь)** → **Networking (Сеть)** и щёлкните правой кнопкой мыши распределенный виртуальный коммутатор, который будет использоваться при восстановлении в новую ВМ, затем щёлкните **Add Permission (Добавить право)**.



2. В окне **Add Permission (Добавить право)** выберите пользователя и роль, которые были созданы на предыдущих шагах, затем установите флажок **Propagate to children (Распространить на дочерние элементы)** и нажмите **OK**.



В таблице перечислены необходимые привилегии и приведены сведения о том, как они используются.

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Cryptographic operations (Операции шифрования (доступно начиная с vSphere 6.5))	Add disk (Добавить диск)	+[1]				
	Direct Access (Прямой доступ)	+[с. 812, 1]				
Datastore (Хранилище данных)	Allocate space (Распределение пространства)		+	+	+	+
	Browse datastore (Обзор хранилища данных)				+	+
	Configure datastore (Настройка хранилища данных)	+	+	+	+	+
	Low level file operations (Низкоуровневые файловые операции)				+	+
Global (Глобальные)	Licenses (Лицензии)	+	+	+	+	
	Disable methods (Методы отключения)	+	+	+		
	Enable methods (Методы включения)	+	+	+		
	Manage custom attributes (Управление настраиваемыми атрибутами)	+	+	+		
	Set custom attribute (Задание настраиваемых атрибутов)	+	+	+		

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Host > Configuration (Хост > Конфигурация)	VM autostart configuration (Конфигурация автозапуска ВМ)					+
	Storage partition configuration (Конфигурация раздела хранения данных)				+	
	Advanced settings (Расширенные настройки)					+
	Connection (Подключение)					+
	System management (Управление системой)					+
Host > Inventory (Хост > Инвентарь)	Modify cluster (Изменение кластера)					+
Host > Local operations (Хост > Локальные операции)	Create VM (Создание ВМ)				+	+
	Delete VM (Удаление ВМ)				+	+
	Reconfigure VM (Перенастройка ВМ)				+	+
Network (Сеть)	Assign network (Назначение сети)		+	+	+	+
Resource (Ресурс)	Assign VM to resource pool (Назначение ВМ пулу ресурсов)		+	+	+	+
Virtual machine > Change configuration (Виртуальная машина > Изменение конфигурации)	Add existing disk (Добавление существующего диска)	+	+		+	

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
	Add new disk (Добавление нового диска)		+	+	+	+
	Add or remove device (Добавление или удаление устройства)		+		+	+
	Advanced configuration (Дополнительная конфигурация)	+	+	+		+
	Change CPU count (Изменение числа ЦП)		+			
	Toggle disk change tracking (Включение/выключение отслеживания изменений диска)	+		+		
	Acquire disk lease (Аренда диска)	+		+		
	Change memory (Управление ОЗУ)		+			
	Remove disk (Удаление диска)	+	+	+	+	
	Rename (Переименование)		+			
	Set annotation (Настройка аннотации)				+	
	Change settings (Изменение настроек)		+	+	+	

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
Virtual machine > Guest Operations (Виртуальная машина > Гостевые операции)	Guest Operation Program Execution (Выполнение программы гостевой операции)	+[2]				+
	Guest Operation Queries (Запросы гостевой операции)	+[с. 812, 2]				+
	Guest Operation Modifications (Изменения гостевых операций)	+[с. 812, 2]				
Virtual machine > Interaction (Виртуальная машина > Взаимодействие)	Acquire guest control ticket (Получение контрольного билета гостя (для vSphere 5.0))				+	+
	Configure CD media (Настройка носителя CD)		+	+		
	Connect devices (Подключение устройств)		+	+		
	Console interaction (Взаимодействие с консолью)					+
	Guest operating system management by VIX API (Управление гостевой операционной системой с помощью API VIX (доступно начиная с vSphere 5.1))				+	+

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
	Power off (Отключение)			+	+	+
	Power on (Включение)		+	+	+	+
Virtual machine > Edit Inventory (Виртуальная машина > Редактирование инвентаря)	Create from existing (Создание из существующей)		+	+	+	
	Create new (Создание новой)		+	+	+	+
	Move (Перемещение)					+
	Register (Регистрация)				+	
	Remove (Удаление)		+	+	+	+
	Unregister (Отмена регистрации)				+	
Virtual machine > Provisioning (Виртуальная машина > Распределение)	Allow disk access (Разрешение доступа к диску)		+	+	+	
	Allow read-only disk access (Разрешение доступа к диску только для чтения)	+		+		
	Allow virtual machine download (Разрешение загрузки ВМ)	+	+	+	+	
Virtual machine > Snapshot management (Виртуальная машина > Управление моментальными снимками)	Create snapshot (Создание моментального снимка)	+		+	+	+
	Remove snapshot (Удаление моментального снимка)	+		+	+	+
vApp	Add virtual machine (Добавление ВМ)				+	
	Import (Импорт)					+

Предельное количество виртуальных машин для резервного копирования

Кибер Бэкап позволяет защитить до 20 000 виртуальных машин в одной конфигурации VMware vSphere.

Для этого необходимо соблюдать следующие условия:

- Иметь особую лицензию для резервного копирования больших объемов данных.
- Установить сервер управления на машину с ОС Linux, использующую СУБД PostgreSQL (см. раздел *Сервер управления на машине с ОС Linux, использующий СУБД PostgreSQL*).
- Производить резервное копирование с помощью *Группы устройств*. В каждой группе должно быть не более 500 виртуальных машин.
- Агент для VMware (виртуальное устройство) должен иметь как минимум 6 центральных процессоров и 16 ГБ ОЗУ.
- Использовать один агент на кластер VMware vSphere.
- Агент должен подключаться к vCenter Server с правами доступа только на свой кластер (видеть объекты только своего кластера). Подробнее см. в статье базы знаний.
- При резервном копировании на ленты использовать не более 5 потоков для одного агента (см. раздел *Управление лентами*).
- Производить одновременное резервное копирование не более 50 виртуальных машин (см. раздел *Ограничение общего количества виртуальных машин*).
- Использовать для хранения резервных копий Кибер Инфраструктуру. Кроме того, при количестве резервных копий до 150 000, можно использовать сетевую папку.

Наибольшая производительность резервного копирования достигается при следующих конфигурациях VMware vSphere:

- не более 2 000 виртуальных машин в одном кластере;
- не более 10 кластеров;
- пропускная способность сети не менее 300 Мбит/с.

[1] Эта привилегия требуется только для резервного копирования зашифрованных машин.
[2] Эта привилегия требуется только для резервных копий с поддержкой приложений.

Одновременное восстановление

Один агент может выполнять восстановление нескольких виртуальных машин параллельно, что является реализацией многозадачности агента Кибер Бэкап (см. раздел *Агент*). Одновременное восстановление позволяет повысить суммарную скорость восстановления одним агентом.

Для выполнения одновременного восстановления воспользуйтесь разделами *Виртуальная машина* или *Восстановление физической машины в виртуальную* и по очереди запускайте восстановление требуемых виртуальных машин. Каждый последующий запуск можно выполнять, не дожидаясь завершения предыдущего действия.

При выполнении одновременного восстановления необходимо следить за использованием агентом вычислительных ресурсов. При необходимости увеличьте количество виртуальных процессоров и памяти для агента (виртуального устройства). Нехватка вычислительных ресурсов может привести к деградации функциональности резервного копирования и восстановления (вплоть до сбоев).

Использование моментальных снимков оборудования SAN

Кибер Бэкап позволяет использовать моментальные снимки оборудования SAN при резервном копировании виртуальных машин платформ виртуализации VMware и oVirt (zVirt).

Для платформы виртуализации VMware поддерживаются следующие системы хранения данных:

- YADRO TATLIN.UNIFIED,
- NetApp,
- Huawei OceanStor (Dorado).

Для платформы виртуализации oVirt (zVirt) поддерживается система хранения данных YADRO TATLIN.UNIFIED.

Причины использования моментальных снимков оборудования SAN

Агенту требуются моментальные снимки виртуальных машин для выполнения согласованного резервного копирования. Агент считывает содержимое виртуального диска с моментального снимка диска, поэтому моментальный снимок должен храниться в течение всего процесса резервного копирования.

По умолчанию агент использует встроенные моментальные снимки приложения VMware, созданные хостом ESXi. Во время хранения снимка файлы виртуального диска находятся в режиме ”только чтение” и хост записывает все внесенные на диск изменения в отдельные разностные файлы. После

завершения процесса резервного копирования хост удаляет моментальные снимки, то есть, объединяет разностные файлы с файлами виртуального диска.

Хранение и удаление моментальных снимков влияет на производительность виртуальной машины. На виртуальных дисках большого объема с быстрым изменением данных эти операции занимают много времени и приводят к падению производительности. В исключительных случаях при одновременном проведении резервного копирования нескольких машин, возрастающий объем разностных файлов может привести к чрезмерному заполнению хранилища данных и привести к отключению всех виртуальных машин.

Вы можете снизить использование ресурсов гипервизором разгрузкой моментальных снимков в SAN. В данном случае последовательность операций будет следующей.

1. ESXi выполняет моментальный снимок VMware в начале процесса резервного копирования для согласования виртуальных дисков.
2. SAN создает моментальный снимок оборудования тома или LUN, содержащих виртуальную машину, и моментальный снимок VMware. Эта операция, как правило, займет несколько секунд.
3. ESXi удаляет моментальный снимок VMware. Агент для VMware считывает содержимое виртуального диска с моментального снимка оборудования SAN.

Моментальный снимок VMware сохраняется в течение нескольких секунд, поэтому снижение производительности виртуальной машины минимально.

Условия для использования моментальных снимков оборудования SAN

Для использования моментальных снимков оборудования SAN при резервном копировании виртуальных машин VMware убедитесь в выполнении следующих условий.

- Установлена расширенная редакция лицензии Кибер Бэкап.
- Выполнена настройка в соответствии с описанием в разделе *Настройка хранилища данных YADRO TATLIN.UNIFIED*.
- Хранилище SAN NetApp соответствует требованиям, описанным в разделе *Требования для хранилища данных NetApp SAN*.
- Выполнена настройка в соответствии с описанием в разделе *Настройка сервера управления для Huawei OceanStor (Dorado)*.
- Машина, на которой запущен агент для VMware (Windows), сконфигурирована в соответствии с описанием в разделе *Настройка машины с агентом для VMware*.
- Выполнена регистрация хранилища SAN в соответствии с описанием в разделе *Регистрация хранилища данных SAN на сервере управления*.

- [При наличии агентов для VMware, не принимавших участие в вышеуказанной регистрации] Виртуальные машины в хранилище SAN назначены агентам с подключенным SAN, как описано в разделе *Привязка виртуальной машины*.
- Параметр резервного копирования *Моментальные снимки оборудования SAN* включен в плане резервного копирования.

Для использования моментальных снимков оборудования SAN при резервном копировании виртуальных машин oVirt убедитесь в выполнении следующих условий.

- Установлена расширенная редакция лицензии Кибер Бэкап.
- Выполнена настройка в соответствии с описанием в разделе *Настройка хранилища данных YADRO TATLIN.UNIFIED*.
- Произведена настройка машины, на которой запущен агент для oVirt, в соответствии с описанием в разделе *Настройка машины с агентом для oVirt*.
- Параметр резервного копирования *Моментальные снимки оборудования SAN* включен в плане резервного копирования.

Настройка хранилища данных YADRO TATLIN.UNIFIED

Кибер Бэкап поддерживает системы хранения YADRO TATLIN.UNIFIED. В этом разделе описана настройка и подключение этих устройств к Кибер Бэкап для выполнения резервного копирования виртуальных машин в среде VMware и zVirt (oVirt) с использованием аппаратных моментальных снимков.

Поддерживаемые конфигурации

Поддерживается оборудование, имеющее интерфейс подключения с iSCSI-протоколом.

Ограничения

- Не поддерживается создание аппаратных моментальных снимков для ресурсов, включенных в группу ресурсов.
- Недоступно восстановление виртуальных машин локальным агентом для oVirt (Linux); для этого используйте агент, предоставляемый в виде виртуального устройства.

Следующие ограничения приведены из расчета на одну систему хранения или из расчета на одновременное выполнение резервного копирования виртуальных машин:

- Количество виртуальных машин, для которых выполняется резервное копирование, не должно превышать 40.

- Суммарное количество дисков виртуальных машин, для которых выполняется резервное копирование, не должно превышать 40.
- Число аппаратных моментальных снимков не должно превышать 40, если для одной виртуальной машины предполагается наличие нескольких аппаратных моментальных снимков.

Следующие ограничения приведены из расчета на одного агента или из расчета на одновременное выполнение резервного копирования виртуальных машин:

- Количество виртуальных машин, для которых выполняется резервное копирование, не должно превышать 10.
- Число аппаратных моментальных снимков не должно превышать 10, если для одной виртуальной машины предполагается наличие нескольких аппаратных моментальных снимков.

Настройка

Настройка хранилища данных состоит из следующих этапов:

1. Установка агента для VMware или локального агента для oVirt (Linux).
2. Настройка машины с агентом.
3. Подключение LUN к хостам виртуализации.
4. Подготовка пользователя.
5. Подключение к серверу управления.

Установка агента

Примечание

Для резервного копирования моментальных снимков на уровне СХД необходимо устанавливать агенты для VMware или oVirt посредством установщика Кибер Бэкап.

Установка агента для VMware

Для установки агента для VMware обратитесь к разделу *Установка агентов в ОС Windows вручную*.

Установка локального агента для oVirt (Linux)

Для установки локального агента для oVirt (Linux) выполните следующие действия:

1. Запустите установщик Кибер Бэкап.
2. Примите лицензионное соглашение.

3. В списке компонентов для установки отметьте флажком **Agent for Linux** (**Агент для Linux**) и **Agent for oVirt** (**Агент для oVirt**).

   Отметьте в списке **Management Server** (**Сервер управления**), если установка сервера управления выполняется на локальную машину.

4. Нажмите **Далее**.
5. Укажите при необходимости свои параметры для подключения. Если вы выбрали установку сервера управления на локальную машину, укажите порты для подключения или оставьте имеющиеся по умолчанию (рекомендуется). Если у вас уже установлен сервер управления, укажите имя или IP-адрес машины с сервером управления.
6. Нажмите **Далее**.
7. Дождитесь окончания установки.

Настройка машины с агентом

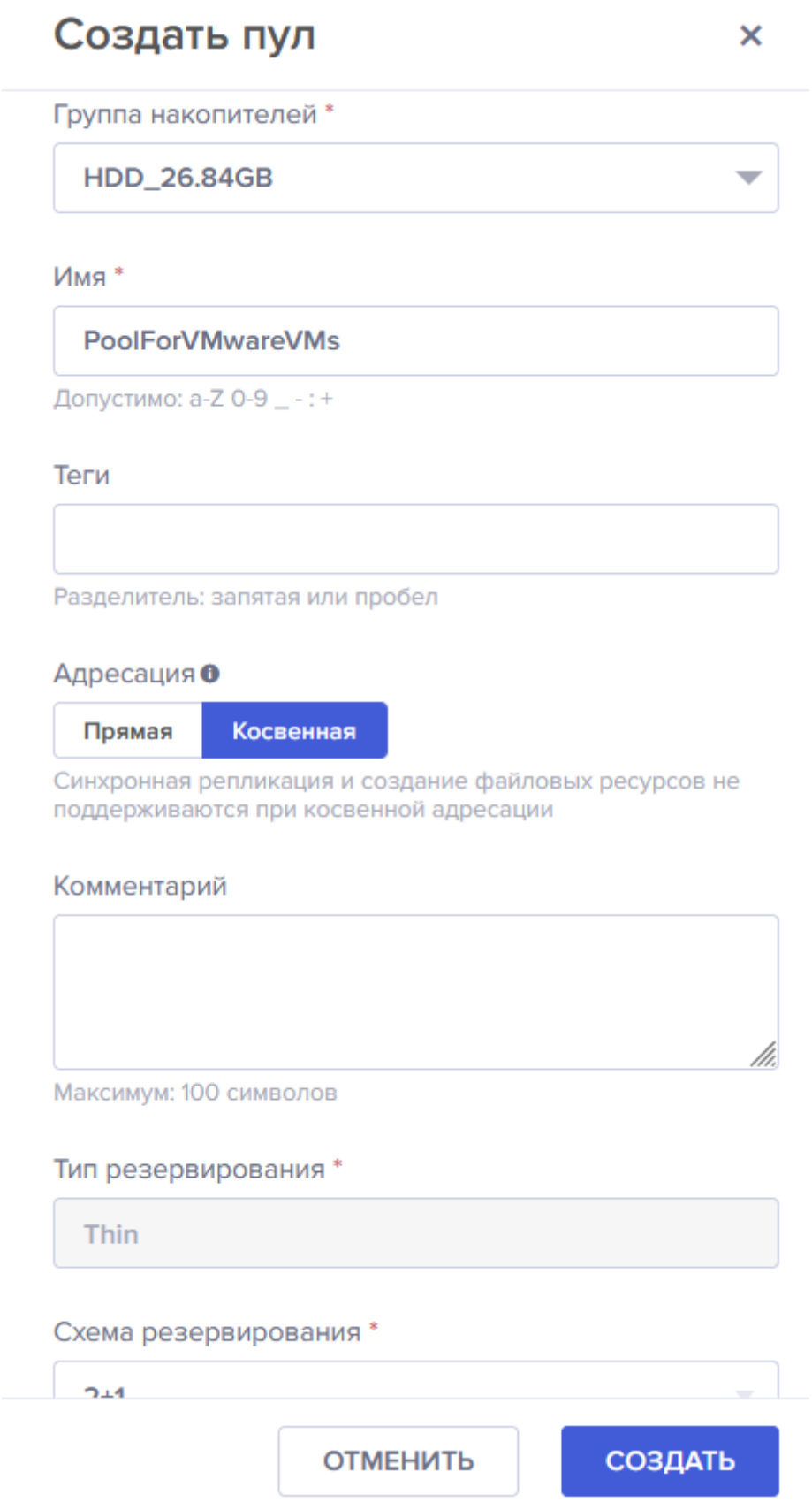
Для настройки машины с агентом для VMware выполните шаги из раздела *Настройка машины с агентом для VMware (Windows)*.

Для настройки машины с локальным агентом для oVirt (Linux) выполните шаги из раздела *Настройка машины с агентом для oVirt*.

В случае успешной установки и настройки в разделе **Устройства** появится подраздел **oVirt**.

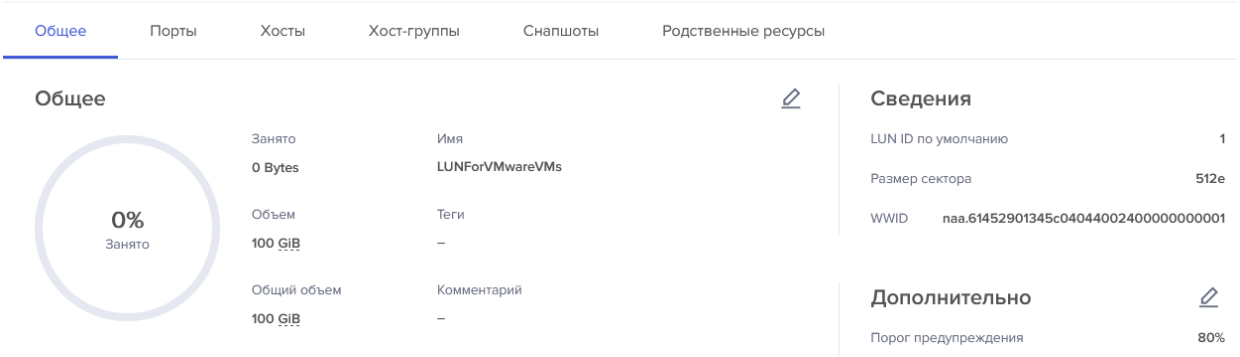
Создание и подключение к хостам виртуализации ресурса (LUN) для размещения дисков виртуальных машин

1. В хранилище данных YADRO TATLIN.UNIFIED создайте пул с косвенной адресацией.



2. В пуле создайте блочный ресурс (LUN) необходимого размера для размещения дисков виртуальных машин. При создании ресурса выберите размер сектора **512e** (рекомендовано для

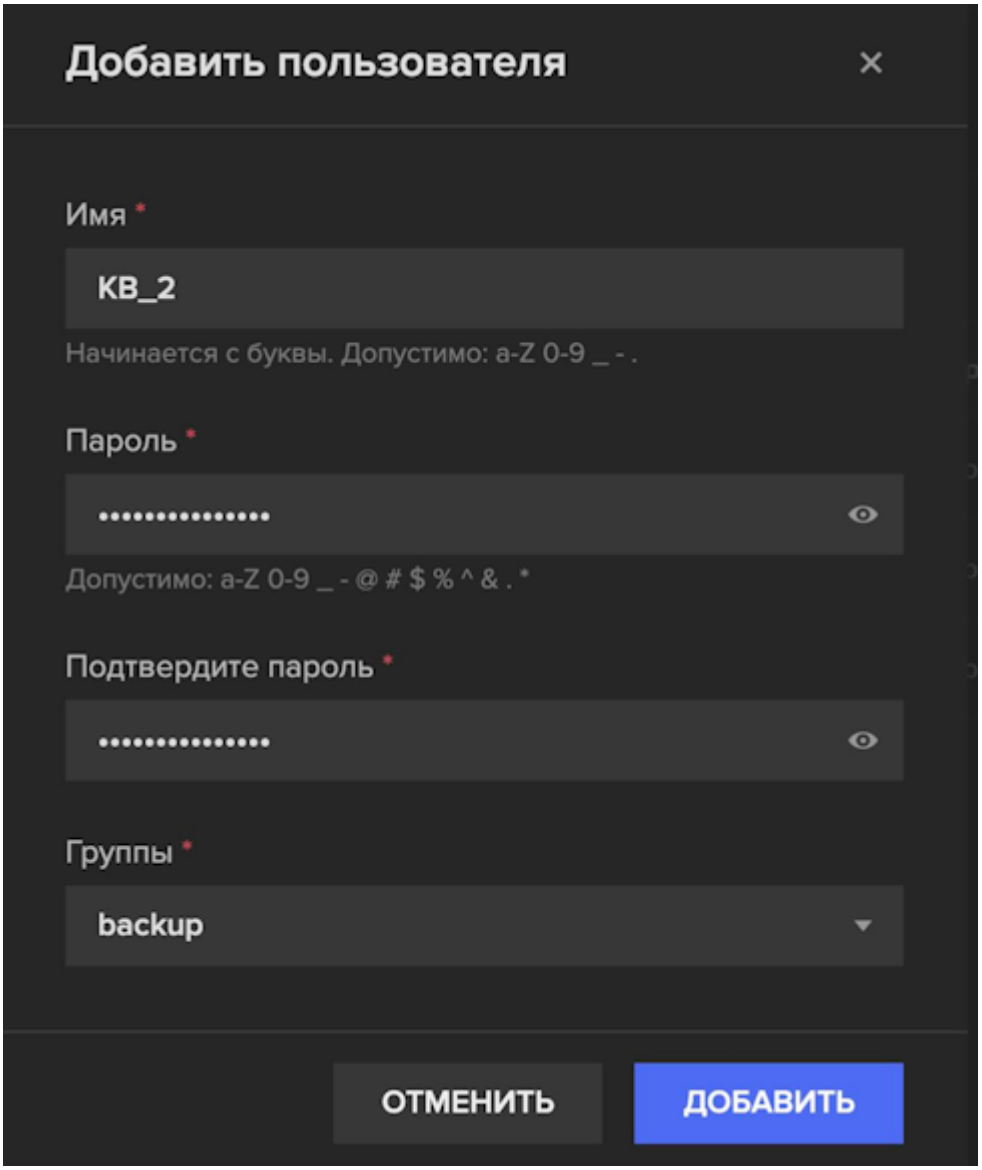
VMware).



3. Подключите ресурс (LUN) по протоколу iSCSI к хостам виртуализации в качестве хранилища виртуальных дисков. Сведения о том, как выполнить подключение, см. в документации системы хранения.

Подготовка пользователя для подключения к API системы хранения данных

В системе хранения данных YADRO TATLIN.UNIFIED создайте пользователя, добавьте его в группу **backup** и сохраните его учетные данные. Эти учетные данные будут использоваться сервером управления Кибер Бэкап для подключения к API системы хранения данных.

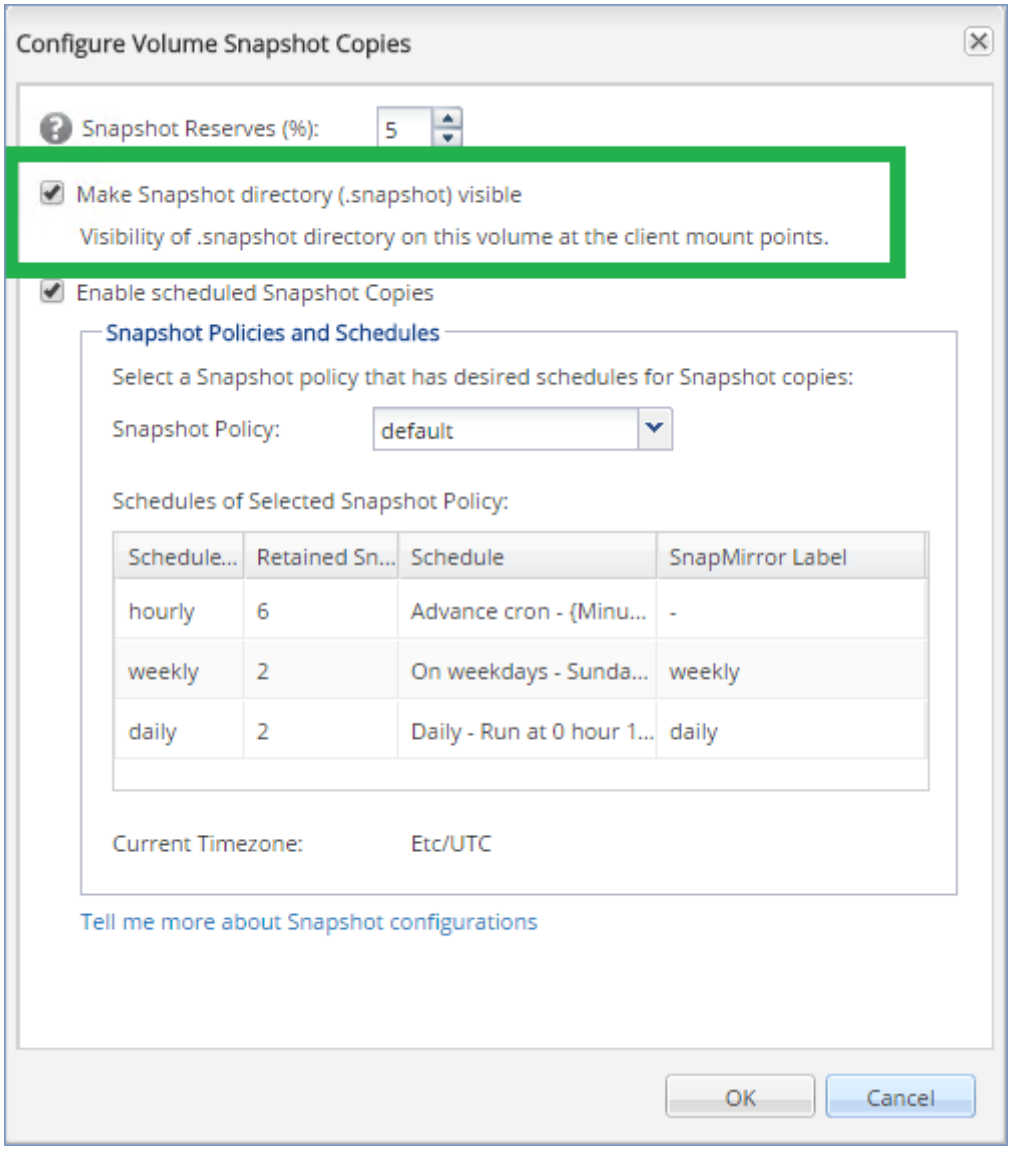


Подключение к серверу управления

Подключите систему хранения данных YADRO TATLIN.UNIFIED к серверу управления Кибер Бэкап согласно описанию в разделе *Регистрация хранилища данных SAN на сервере управления*.

Требования для хранилища данных NetApp SAN

- Хранилище SAN должно использовать хранилище данных NFS или iSCSI.
- SAN должен работать с ПО Data ONTAP версии 8.1 или более новой в режиме **Clustered Data ONTAP (cDOT)**. Режим **7-mode** не поддерживается.
- В менеджере системы NetApp OnCommand System Manager должен быть установлен флажок **Моментальные копии → Конфигурирование → Сделать видимой папку моментальных копий (.snapshot)** для тома, в котором находится хранилище данных.

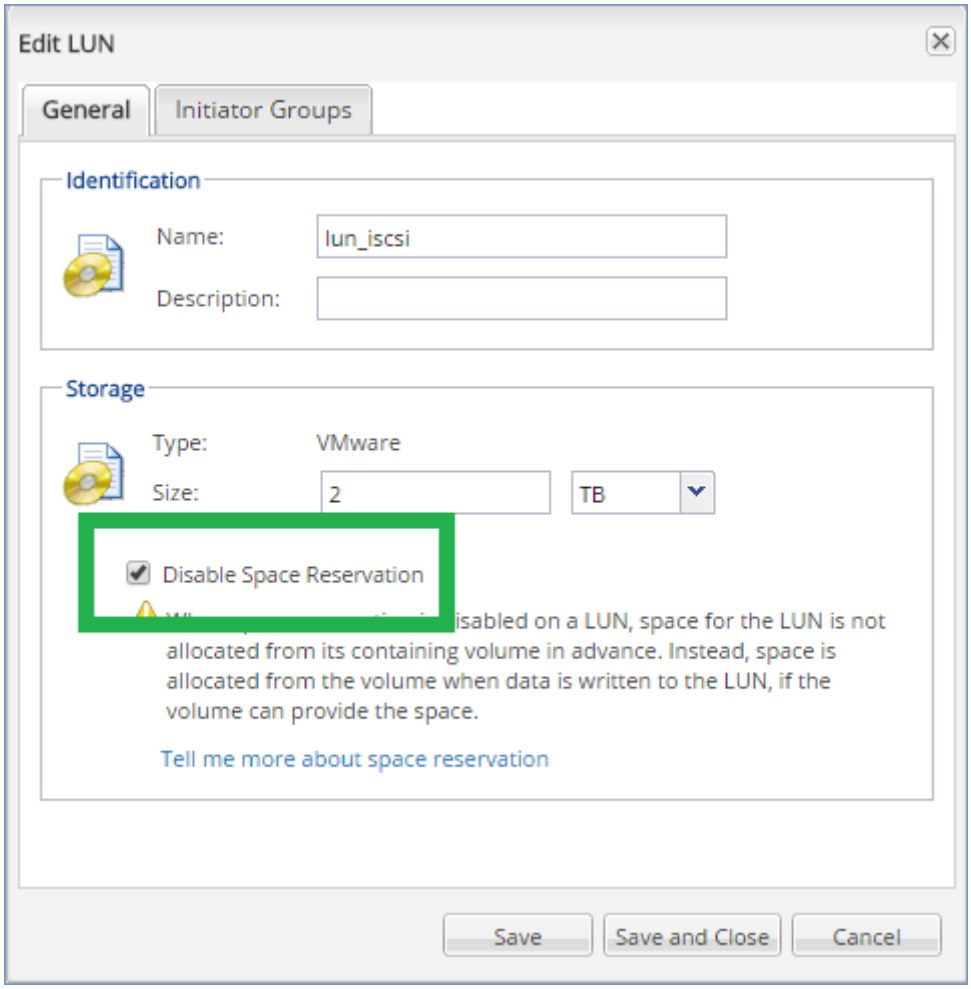


- [Для хранилищ данных NFS] На указанной при создании хранилища данных виртуальной машине должен быть разрешен доступ к общим папкам NFS для клиентов Windows NFSv3. Доступ можно разрешить посредством следующей команды:

```
vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
```

  Дополнительные сведения см. в документе с рекомендациями NetApp.

- [Для хранилищ данных iSCSI] В менеджере системы NetApp OnCommand должен быть установлен флажок **Отключить резервирование пространства** для iSCSI LUN, в котором находится хранилище данных.



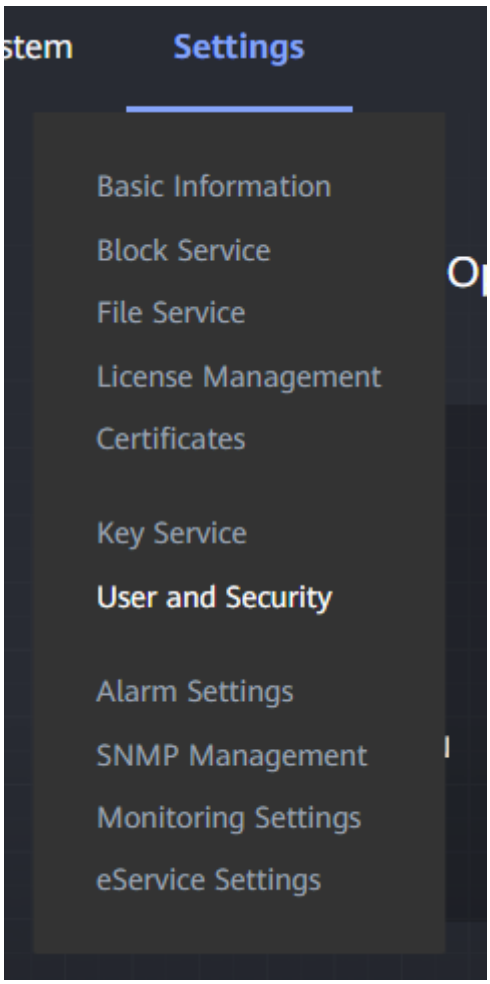
Настройка Huawei OceanStor (Dorado)

Кибер Бэкап поддерживает системы хранения семейства Huawei OceanStor (Dorado). В этом разделе описана настройка и подключение этих устройств к Кибер Бэкап для создания аппаратных моментальных снимков в среде VMware.

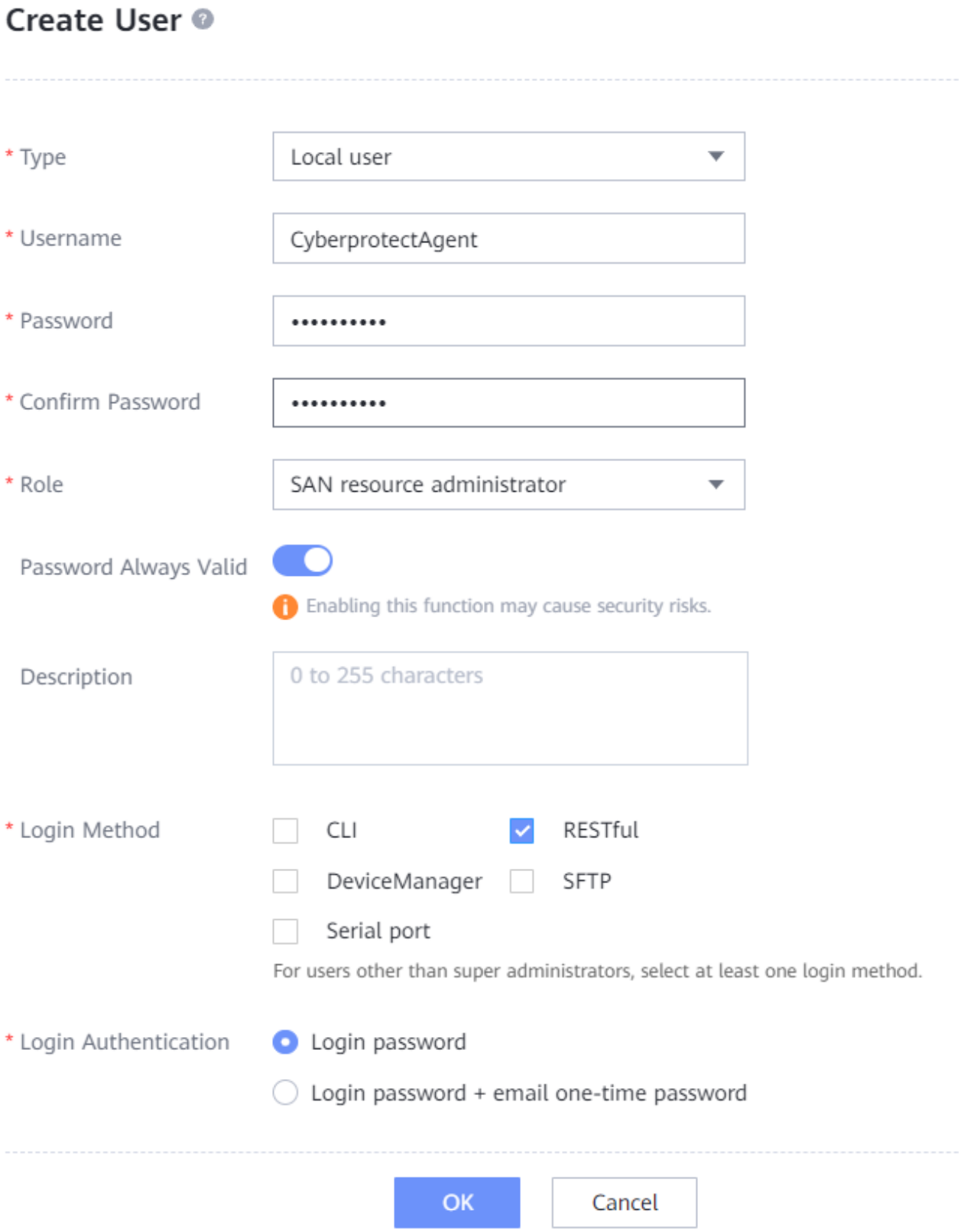
Настройка пользователя в Dorado

Для настройки пользователя в Dorado выполните следующие действия:

- В настройках **План резервного копирования** укажите параметр **SAN hardware snapshot**: **yes**.
- На вкладке **Settings** перейдите в раздел **User and Security** и нажмите **Create User**.

- 

- Заполните поля как показано далее:



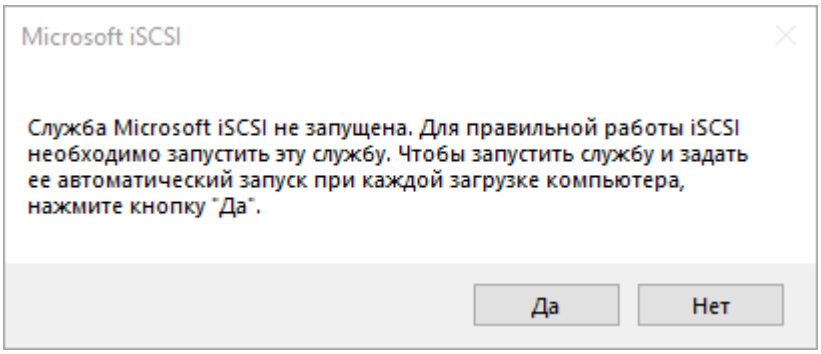
- В поле **Role** укажите одну из двух следующих ролей (встроенных групп):
  - Administrator

    - Super administrator
- По окончании ввода данных нажмите **OK**.

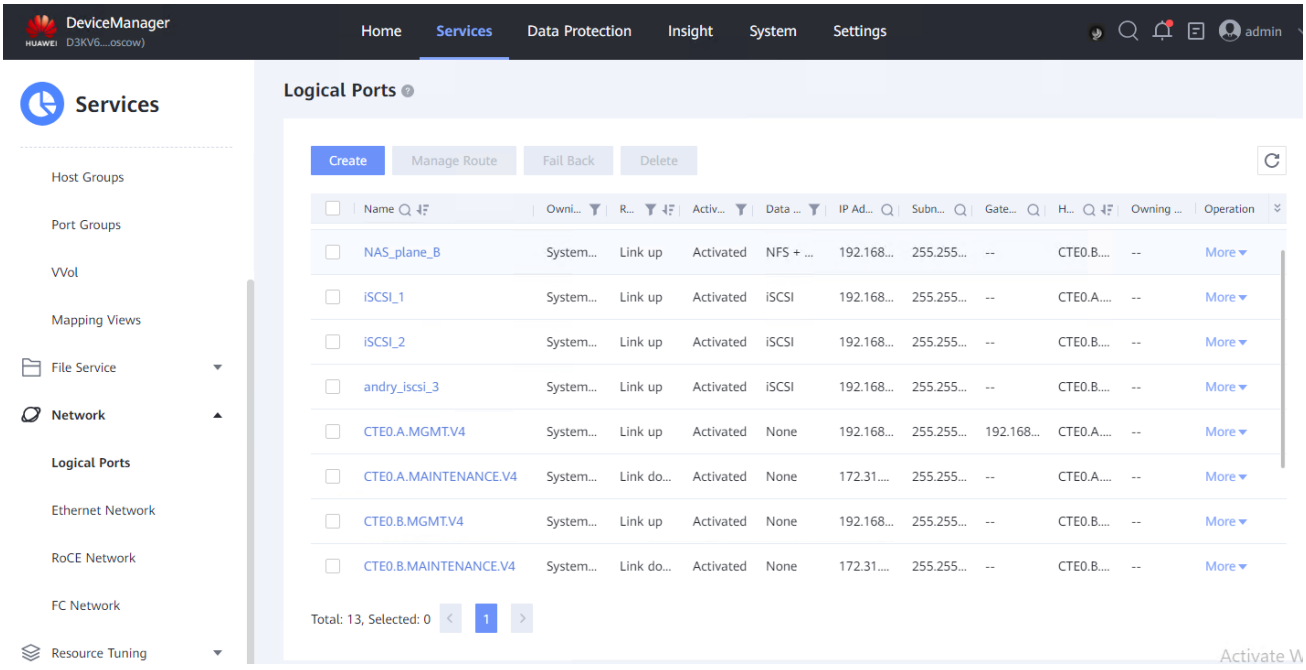
Настройка iSCSI-доступа

Нажмите **Пуск** → **Средства администрирования Windows** → **iSCSI Initiator**. Или в меню **Пуск** выберите **Выполнить** (или нажмите `Win+R`) и наберите `iscsicpl.exe`, а затем нажмите **OK** или `Ввод`.

Если служба не была запущена, появится предложение запустить службу, выберите **Да**.



Убедитесь, что у устройства Dorado есть доступ хотя бы к одному из портов Logical Ports iSCSI. При этом порт в Logical Ports может быть отличен от порта, который используется в ESXi.



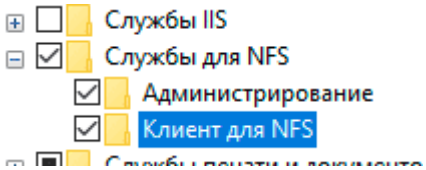
Убедитесь, что IQN инициатора уникально. Это актуально в случае, если машины были клонированы.

Настройка NFS

Убедитесь, что хотя бы одна сетевая карта (подсеть) имеет доступ к NFS устройства Dorado. NFS Dorado должна располагаться в той же подсети, в которой находится ESXi.

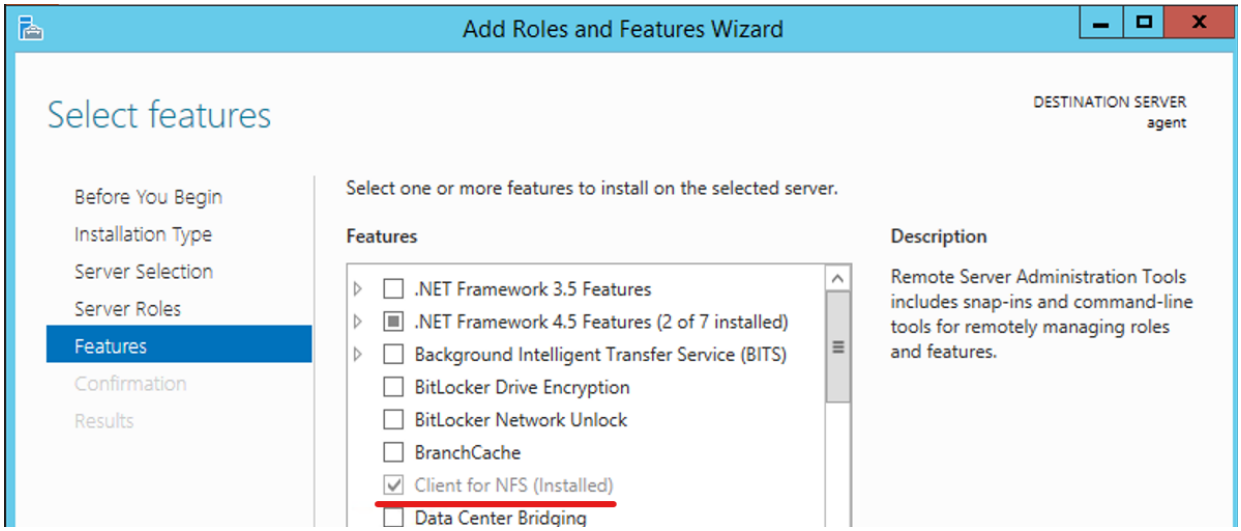
На клиентском компьютере под управлением Windows выполните следующие действия:

1. Нажмите **Пуск** → **Выполнить** (или нажмите `Win+R`).
2. Наберите `optionalfeatures.exe` и нажмите **OK** или `Ввод`.
3. Отметьте пункт **Клиент для NFS** и нажмите **OK**.



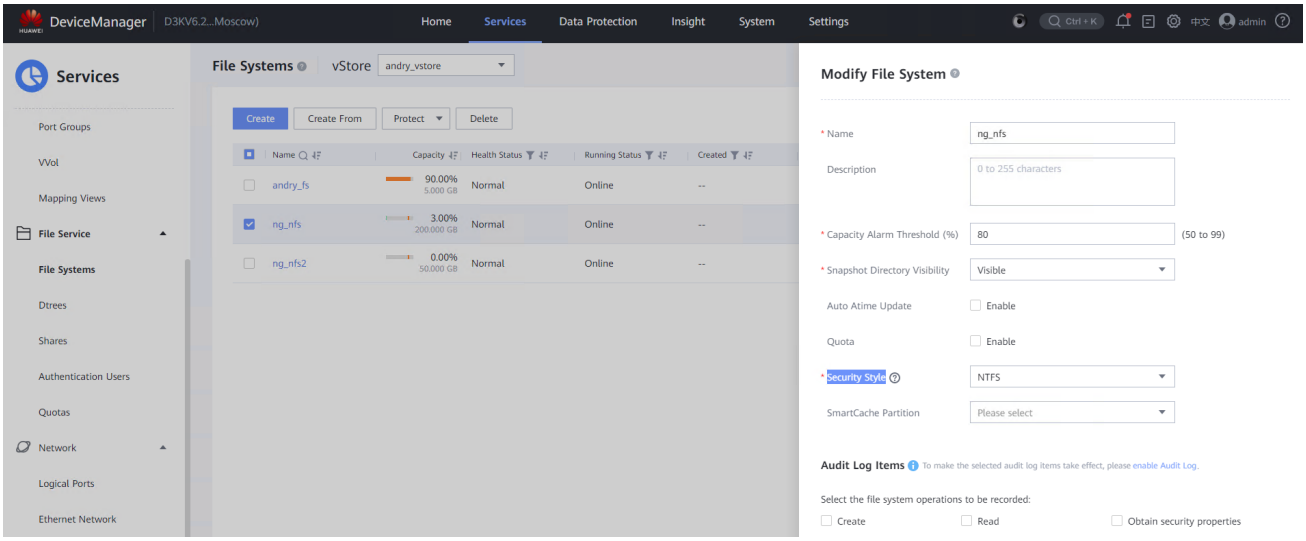
Для сервера под управлением Windows выполните следующие действия:

1. Нажмите **Пуск** → **Выполнить** (или нажмите `Win+R`).
2. Наберите `optionalfeatures.exe` и нажмите **OK** или `Ввод`.
3. Убедитесь, что на сервере установлен компонент **Клиент для NFS**. Иначе отметьте пункт **Клиент для NFS** и установите компонент (инструкции по установке см. в документации Microsoft).



Настройка CIFS

При создании общей папки SMB в секции **File Systems** в панели управления Dorado в поле **Security Style** выберите пункт **NTFS**.



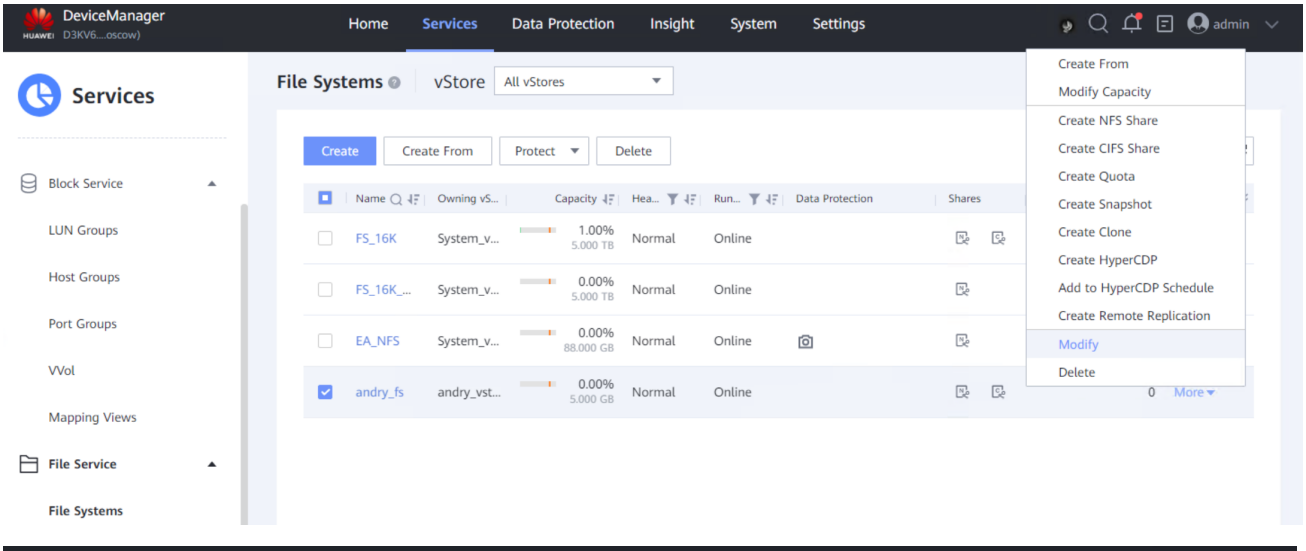
Рекомендуется в настройках общей папки прописывать доступ к машине с агентом. Убедитесь, что общая папка SMB доступна для чтения/записи штатными средствами.

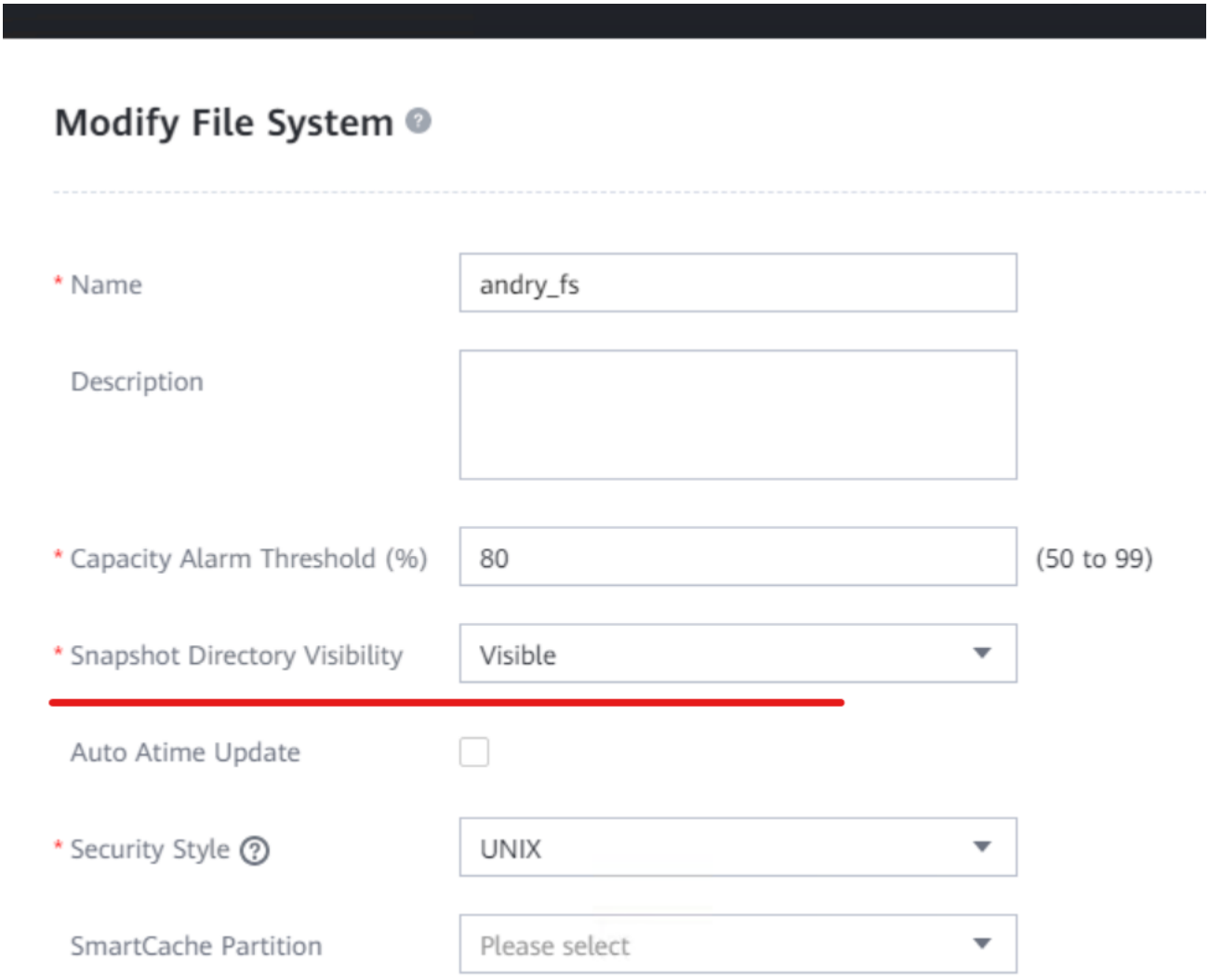
Настройка анонимного UID и анонимного GID

1. На компьютере, где находится агент для VMware (Windows) откройте реестр Windows: нажмите `Win+R`, а затем наберите `regedit.exe` и нажмите **OK** или `Ввод`).
2. Откройте `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default`
3. Создайте новый элемент `DWORD` с названием `AnonymousUID` и установите его значение на `0` (или другое значение UID для пользователя Unix).
4. Создайте новый элемент `DWORD` с названием `AnonymousGID` и установите его значение на `0` (или другое значение GID для пользователя Unix).
5. Перезагрузите компьютер.

Убедитесь, что IP-адрес агента находится в списке разрешенных для раздела ресурсов и у него есть права read-write.

Убедитесь, что **Snapshot Directory Visibility** файловой системы включен.


DeviceManager
Home
Services
Data Protection
Insight
System
Settings
admin
Services
File Systems
vStore
All vStores
Block Service
LUN Groups
Host Groups
Port Groups
VVol
Mapping Views
File Service
File Systems
Create
Create From
Protect
Delete
Name
Owning vS...
Capacity
Hea...
Run...
Data Protection
Shares
FS_16K
System_v...
1.00%
5.000 TB
Normal
Online
FS_16K_...
System_v...
0.00%
5.000 TB
Normal
Online
EA_NFS
System_v...
0.00%
88.000 GB
Normal
Online
andry_fs
andry_vst...
0.00%
5.000 GB
Normal
Online
0
More
Create From
Modify Capacity
Create NFS Share
Create CIFS Share
Create Quota
Create Snapshot
Create Clone
Create HyperCDP
Add to HyperCDP Schedule
Create Remote Replication
Modify
Delete


Modify File System
* Name
andry_fs
Description
* Capacity Alarm Threshold (%)
80
(50 to 99)
* Snapshot Directory Visibility
Visible
Auto Atime Update
* Security Style
UNIX
SmartCache Partition
Please select

Подключение к серверу управления

Для подключения к серверу управления выполните шаги по настройке Dorado из раздела *Регистрация хранилища данных SAN на сервере управления*.

Известные проблемы и ограничения

1. Возможность резервного копирования через NFS существует лишь для компьютеров под управлением Windows 10.
2. Аппаратные моментальные снимки поддерживаются только для VMware.
3. Проверяется наличие NFS-клиента, если в хранилище находится хотя бы одна файловая система NFS.
4. Проверяется наличие iSCSI-инициатора, если в хранилище находится хотя бы одно логическое устройство (LUN).
5. Не удается выполнить резервное копирование виртуальной машины с пустым диском.
6. Не удается выполнить резервное копирование, если диск виртуальной машины находится не в аппаратном хранилище.

Настройка машины с агентом для VMware (Windows)

В зависимости от использования хранилища SAN в качестве хранилища данных NFS или iSCSI см. соответствующий раздел ниже.

Настройка инициатора iSCSI

Убедитесь, что выполнены все последующие условия:

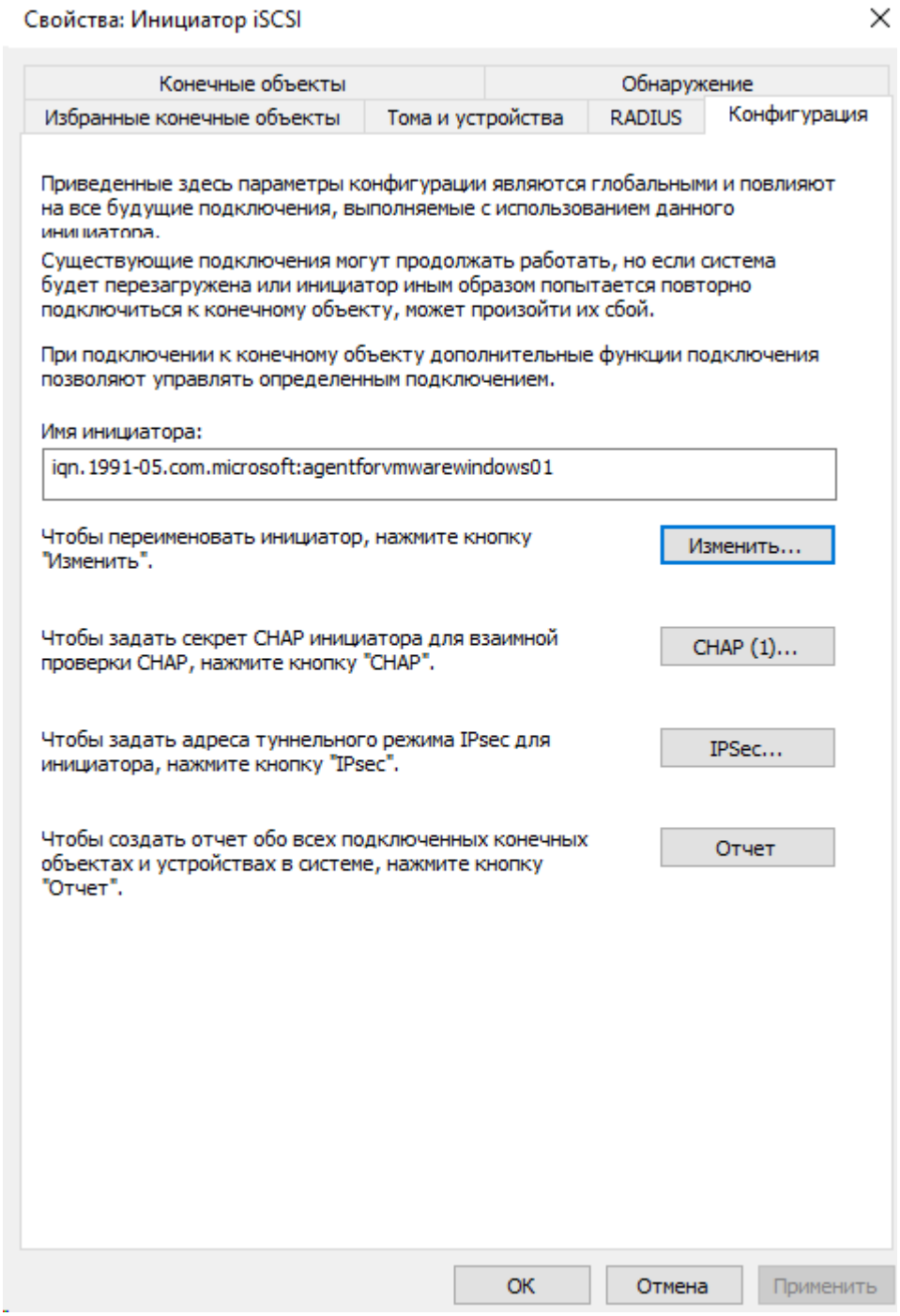
- Инициатор iSCSI установлен.
- Тип запуска службы инициатора iSCSI (Microsoft) имеет значение **Автоматически** или **Вручную**. Это можно сделать в оснастке **Службы**.
- Инициатор iSCSI настроен как описано в примере раздела *Резервное копирование без использования локальной сети посредством Windows-агента для VMware*.

Настройка iSCSI-инициатора для СХД YADRO TATLIN.UNIFIED

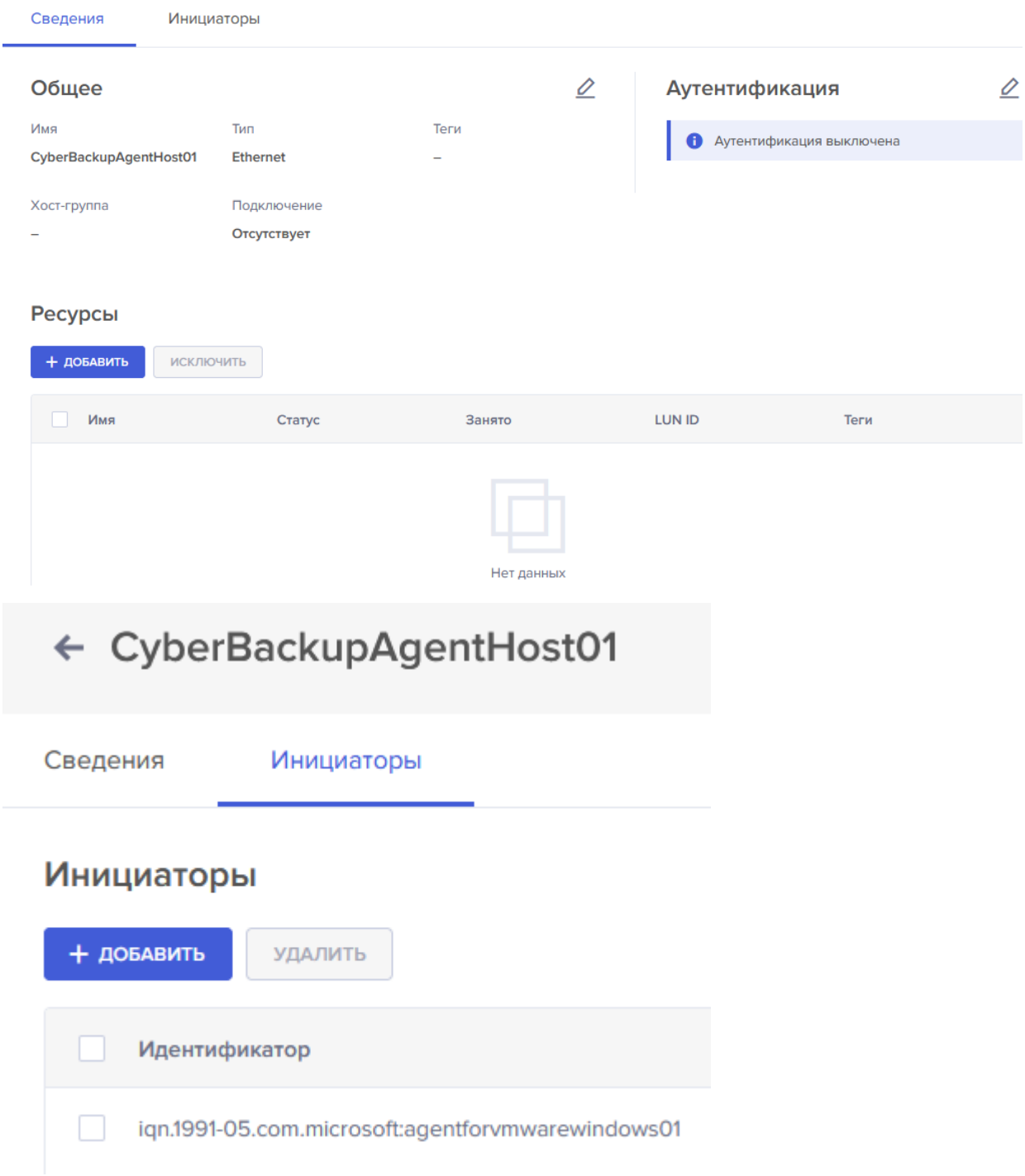
Выполните следующие действия для каждой машины с агентом:

1. В консоли управления службами укажите тип запуска **Автоматически** или **Вручную** для службы инициатора Майкрософт iSCSI.

2. Запустите приложение **Инициатор iSCSI** и на вкладке **Конфигурация** получите IQN-имя iSCSI-инициатора машины.



3. В хранилище данных YADRO TATLIN.UNIFIED создайте хост с именем **CyberBackupAgentHost<уникальный_суффикс>** и добавьте для него IQN-имя iSCSI-инициатора машины. Ресурсы добавлять не нужно.



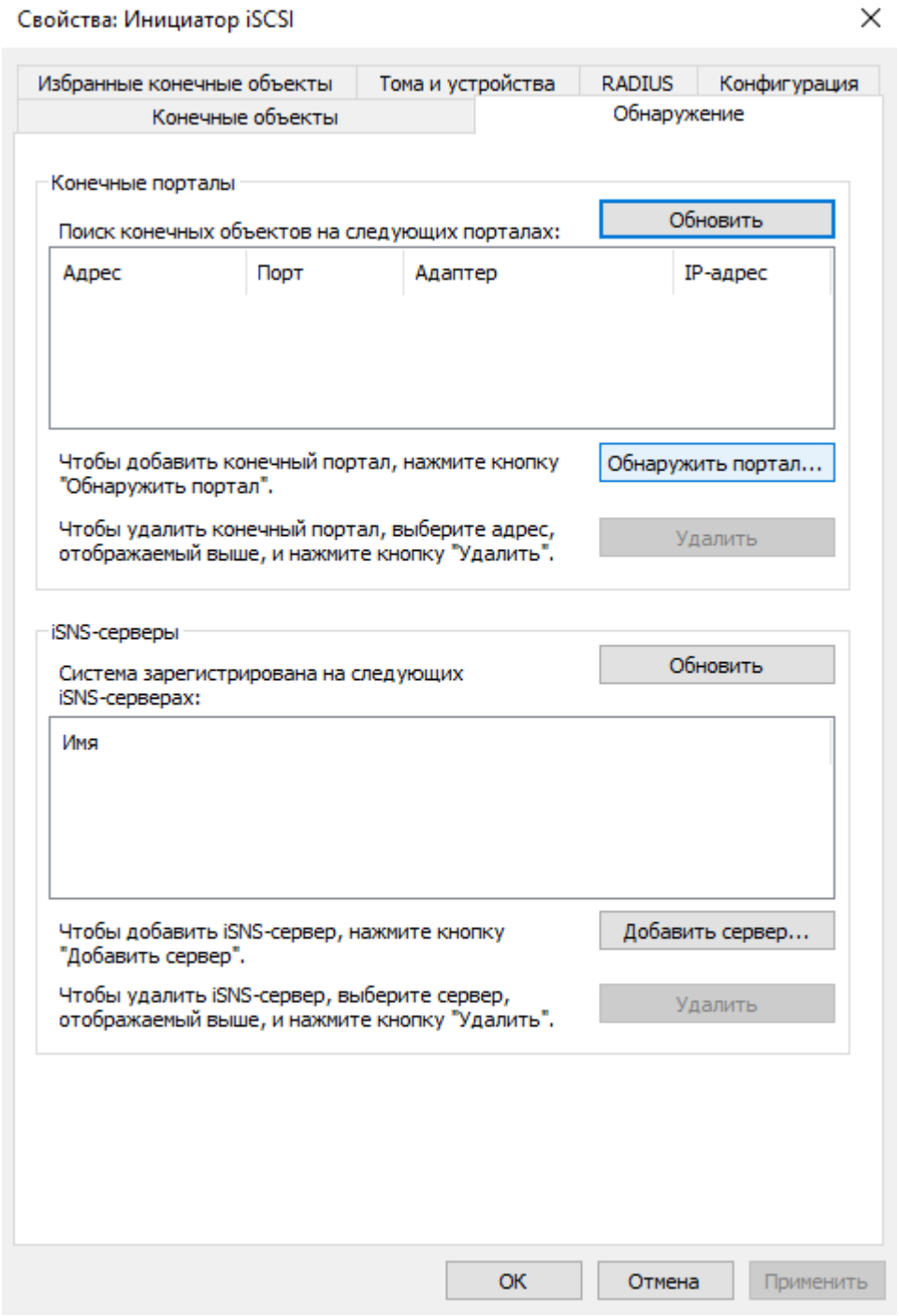
Добавленный хост будет использоваться для предоставления агенту доступа к моментальным снимкам, создаваемым в хранилище данных.

Примечание

При резервном копировании Кибер Бэкап автоматически добавляет (для хоста) и удаляет временные ресурсы (LUN), которые создаются на основе моментальных снимков ресурса с

дисками виртуальных машин.

4. Проверьте, что iSCSI-инициатор может подключиться к хранилищу данных. Для этого в приложении **Инициатор iSCSI** на вкладке **Обнаружение** добавьте портал обнаружения хранилища данных, перейдите на вкладку **Конечные объекты** и подключитесь к обнаруженному конечному объекту.



Настройка NFS-клиента

Убедитесь, что выполнены все последующие условия:

- Установлен **Клиент для NFS**.
- NFS-клиент настроен на анонимный доступ. Это можно сделать следующим образом:
  1. Откройте редактор реестра.
  2. Найдите следующий раздел реестра:
     `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default`
  3. В этом ключе создайте новый параметр **DWORD** с именем **AnonymousUID** и задайте ему значение, равное 0.
  4. В этом же ключе создайте новый параметр **DWORD** с именем **AnonymousGID** и задайте ему значение, равное 0.
  5. Перезапустите машину.

Регистрация хранилища данных SAN на сервере управления

Регистрация хранилища данных YADRO TATLIN.UNIFIED

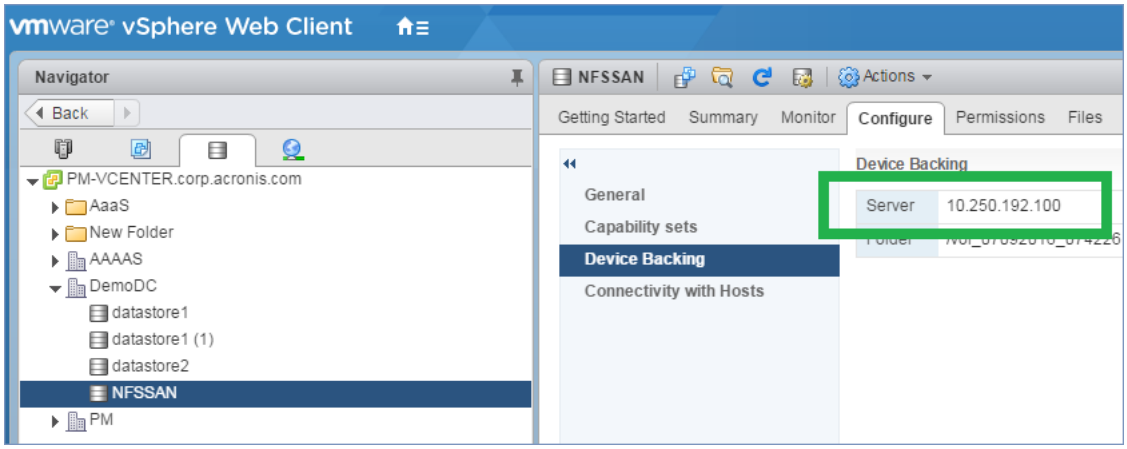
1. Перейдите в раздел **Настройки** → **Хранилище данных SAN** и нажмите **Добавить хранилище**.
2. В поле **Имя** укажите имя для хранилища.
3. В раскрывающемся списке **Выберите тип SAN** выберите тип хранилища данных **YADRO Tatlin.Unified**.
4. В поле **Имя или IP-адрес хоста** укажите DNS-имя или IP-адрес для подключения к API хранилища данных.
5. В полях **Имя пользователя** и **Пароль** укажите учетные данные пользователя для подключения к API хранилища данных. Сведения о подготовке пользователя см. в разделе *Настройка хранилища данных YADRO TATLIN.UNIFIED*.
6. Выберите от одного до нескольких агентов, которым будет предоставлен доступ на чтение к этому хранилищу данных.
7. Нажмите **Добавить**.

Регистрация хранилища данных NetApp

1. Нажмите **Настройки** → **Хранилище данных SAN**.
2. Нажмите **Добавить хранилище**.
3. [Необязательно] В **Имя** измените имя хранилища.

   Это имя будет отображено на вкладке **Хранилище данных SAN**.
4. В **Имя хоста или IP-адрес** укажите виртуальную машину хранилища NetApp Storage Virtual Machine (SVM, также называемое систематизатором), которая была указана при создании хранилища данных.

   Для нахождения требуемой информации в веб-клиенте VMware vSphere выберите хранилище данных и затем нажмите **Настроить** → **Резервная копия устройства**. Имя хоста или IP-адрес отобразится в поле **Сервер**.



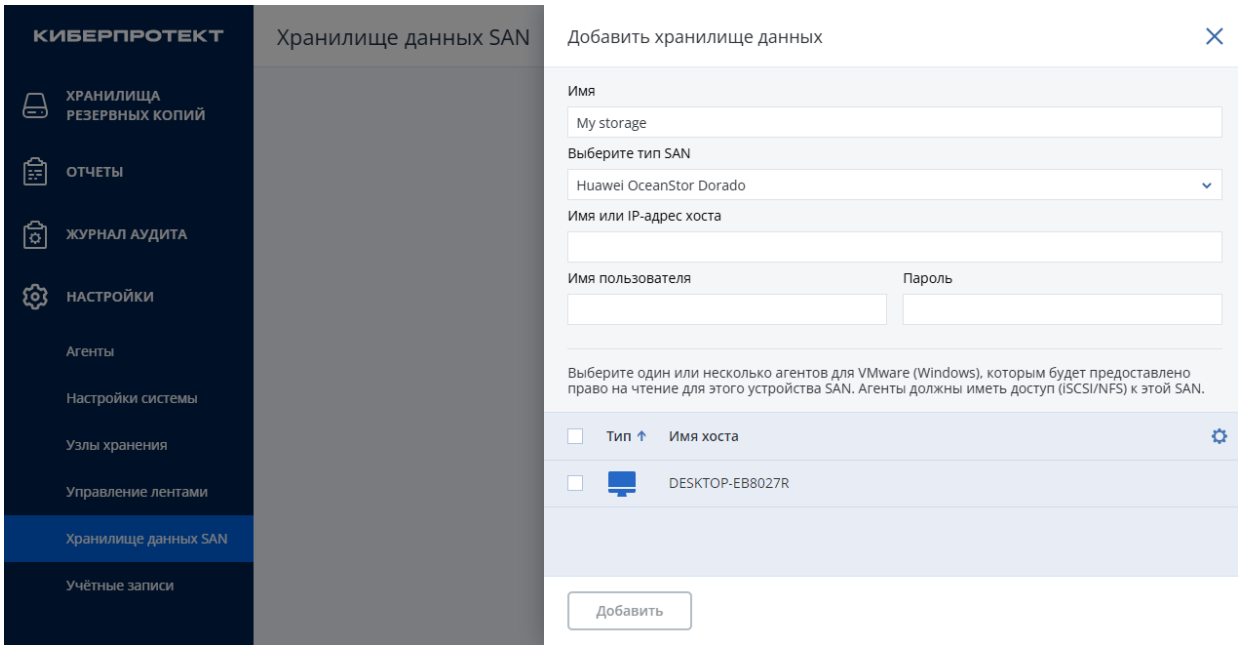
5. В полях **Имя пользователя** и **Пароль** укажите учетные данные администратора SVM.

   > **Важно**
   >
   > Указанная учетная запись должна иметь права локального администратора SVM, а не права администратора менеджера системы NetApp.

   Выберите существующего пользователя или создайте нового. Второе можно сделать в менеджере системы NetApp OnCommand по пути **Настройки** → **Безопасность** → **Пользователи**.
6. Выберите один или несколько агентов для VMware (Windows), которым будет предоставлено право на чтение для устройства SAN.
7. Нажмите **Добавить**.

Регистрация хранилища данных Huawei OceanStor (Dorado)

1. Перейдите в веб-консоль Кибер Бэкап.
2. В разделе **Настройки** → **Хранилище данных SAN** нажмите **Добавить хранилище**.



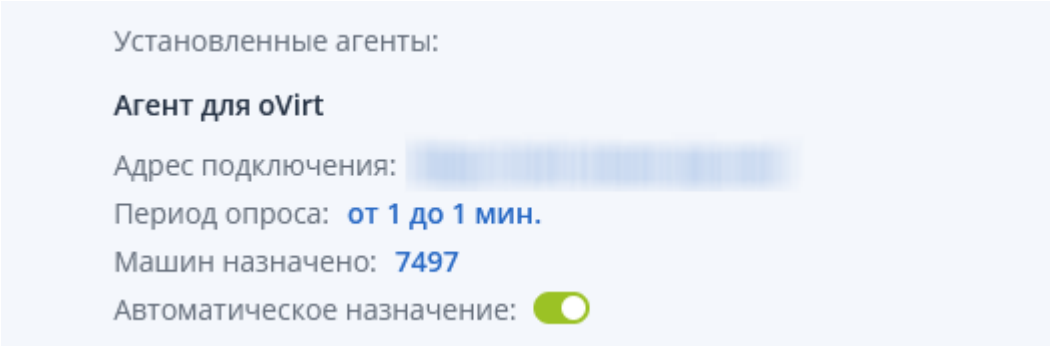
3. Укажите параметры в окне **Добавить хранилище данных**:
   - В поле **Имя** укажите название устройства;
   - В поле **Выберите тип SAN** укажите **Huawei OceanStor Dorado**;
   - В поле **Имя или IP-адрес хоста** укажите IP-адрес веб-интерфейса устройства;
   - В полях **Имя пользователя** и **Пароль** укажите логин и пароль пользователя.
4. Выберите один или несколько агентов для VMware (Windows), которым будет предоставлено право на чтение для этого устройства SAN.
5. Нажмите **Добавить**.

Настройка машины с агентом для oVirt

Регистрация агента

Для регистрации агента выполните следующие действия:

1. В веб-консоли перейдите в меню **Настройки** → **Агенты**.
2. В списке отметьте машину с агентом и нажмите справа **Сведения**.
3. В блоке **Агент для oVirt** щелкните значение в строке **Адрес подключения**.



4. В открывшемся окне введите адрес сервера и данные учетной записи для подключения к платформе виртуализации (например, `https://zvirt.company.ru`) и нажмите **Применить**.
5. В строке **Машин назначено** отображается количество назначенных машин для резервного копирования. Щелкните по значению в строке и просмотрите открывшийся список. Убедитесь, что все необходимые машины назначены. По умолчанию включено автоматическое назначение машин; если необходимо, назначьте машины вручную.

Для повышения производительности при одновременном резервном копировании рекомендуется для машины с агентом для oVirt использовать минимум 16 ГБ ОЗУ и 4 ядра ЦП.

Настройка агента

Чтобы настроить машину с локальным агентом для oVirt (Linux), выполните следующие действия (на примере РЕД ОС 8, в других ОС названия пакетов могут отличаться):

1. Установите пакет `qemu-img`:

```
dnf install qemu-img
```

2. Установите пакет `lvm2`:

```
dnf install lvm2
```

3. Отключите автоматическую активацию томов LVM в конфигурационном файле `/etc/lvm/lvm.conf`, добавив в секцию `activation` следующую строку:

```
auto_activation_volume_list = []
```

4. Отключите в LVM фильтрацию устройств по `devices file`, раскомментировав в файле `/etc/lvm/lvm.conf` параметр `use_devicesfile` и установив его значение равным 0:

```
use_devicesfile = 0
```

5. Установите пакет `iscsi-initiator-utils`:

```
dnf install iscsi-initiator-utils
```

6. Включите автозапуск службы `iscsid`:

```
systemctl enable iscsid iscsi --now
```

7. Создайте файл `/etc/iscsi/iscsid_auth.conf` и добавьте в него строки:

```
[DEFAULTS]
InitiatorName=<имя инициатора iSCSI>
```

   Где `<имя инициатора iSCSI>` — строка из файла `/etc/iscsi/initiatorname.iscsi`.

8. Установите пакет для `multipathd`:

```
dnf install device-mapper-multipath
```

9. Создайте конфигурационный файл `/etc/multipath.conf` с содержимым:

```
defaults {
  user_friendly_names no
}
```

10. Перезапустите службу `multipathd`:

```
systemctl restart multipathd
```

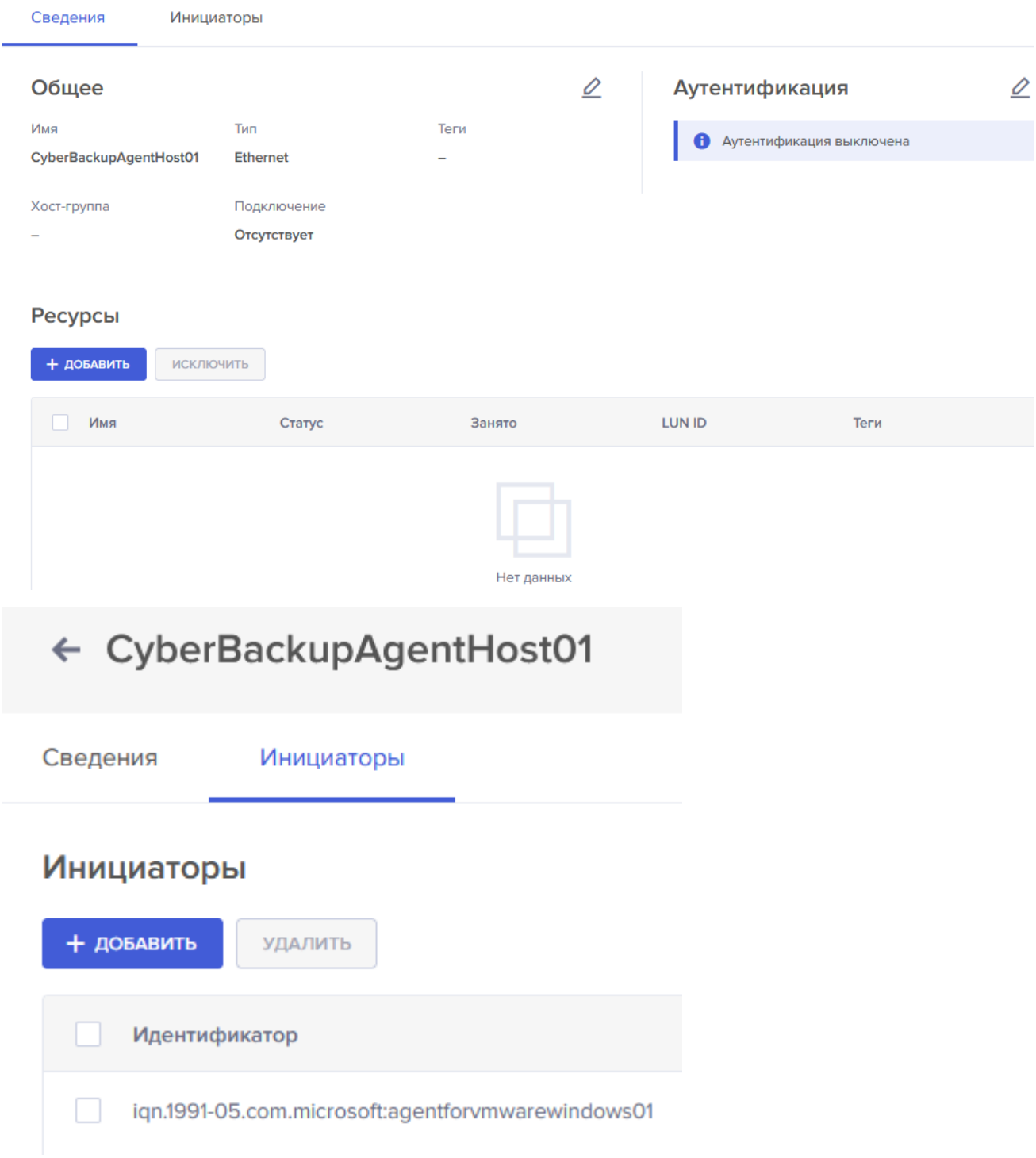
Для работы агента с системой виртуализации oVirt может потребоваться сертификат SSL.

Установите сертификат SSL или в файле `/etc/Acronis/VirtualWare.config` под поле `</registry>` добавьте строку:

```
<value name="IgnoreSslErrors" type="Tdword">"1"</value>
```

Создание хоста

1. В хранилище данных YADRO TATLIN.UNIFIED создайте хост с именем **CyberBackupAgentHost<уникальный_суффикс>** и добавьте для него IQN-имя iSCSI-инициатора машины. Ресурсы добавлять не нужно.



Известные проблемы и ограничения

- Недоступно восстановление виртуальных машин локальным агентом для oVirt (Linux); для этого используется виртуальное устройство для oVirt (для его установки см. раздел *Установка агента для oVirt (zVirt/ROSA Virtualization/РЕД Виртуализация)*.

Резервное копирование кластеризованных машин Hyper-V

В кластере Hyper-V виртуальные машины могут мигрировать между узлами кластера. Следуйте приведенным ниже рекомендациям для настройки правильного резервного копирования кластеризованных машин Hyper-V.

1. Машина должна быть доступна для резервного копирования независимо от того, на какой узел она переносится. Чтобы убедиться в том, что агент для Hyper-V имеет доступ к машине на любом узле, необходимо запустить службу агента под учетной записью пользователя домена с правами администратора на каждом из узлов кластера (см. *Установка агентов*).

   Рекомендуется указать такую учетную запись для службы агента в процессе установки агента для Hyper-V.

2. Установите агент для Hyper-V на каждом узле кластера.
3. Зарегистрируйте все агенты на сервере управления.

Высокая доступность восстановленной машины

При восстановлении резервных копий дисков на *существующей* виртуальной машине Hyper-V свойство высокой доступности данной машины остается без изменений.

Если вы восстанавливаете диски с резервной копии на *новую* виртуальную машину Hyper-V или выполняете преобразование в виртуальную машину Hyper-V *в рамках плана защиты*, полученная в результате машина не будет высокодоступной. Она считается запасной и обычно выключена. Если машину необходимо использовать в производственной среде, можно настроить для нее свойство высокой доступности с помощью оснастки **Управление отказоустойчивым кластером**.

Миграция машины

Можно выполнить миграцию машины, восстановив ее резервную копию на машину, которая не является исходной.

Доступные варианты выполнения миграции приведены в следующей таблице.

Тип виртуальной машины	**Доступные места восстановления**											
	Физическая машина	**ВМ Кибер Инфраструктура**	**ВМ VMware ESXi**	**ВМ Hyper-V**	**ВМ oVirt**[с. 841, 1]	**ВМ SpaceVM**	**ВМ ECP VeiL**	**ВМ OpenStack**[с. 841, 2]	**ВМ Basis DynamiX Enterprise**[с. 841, 2]	**ВМ OpenNebula (ПК СВ ”Брест”)**	**ВМ VM-manager**	**ВМ Proxmox**
Физическая машина	+	+	+	+	+	+	+	+	+	+	—	—
ВМ Кибер Инфраструктура	—	+	+	—	+	+	+	+	+	+	—	—
ВМ VMware ESXi	+	+	+	+	+	+	+	+	+	+	+	—
ВМ Hyper-V	+	—	+	+	+	+	+	+	+	+	—	—
ВМ oVirt[с. 841, 1]	+	+	+	+	+	+	+	+	+	+	+	—
ВМ SpaceVM	+	+	+	+	+	+	+	+	+	+	—	—
ВМ ECP VeiL	+	+	+	+	+	+	+	+	+	+	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Тип виртуальной машины	Доступные места восстановления											
	Физическая машина	ВМ КиберИнфраструктура	ВМ VMware ESXi	ВМ Hyper-V	ВМ oVirt[1]	ВМ Space-VM	ВМ ECP VeiL	ВМ OpenStack[2]	ВМ Basis DynamiX Enter-prise[2]	ВМ OpenNebula (ПК СВ ”Брест”)	ВМ VM-manager	ВМ Proxmox
ВМ OpenStack	—	+	+	—	+	+[3]	+[3]	+	+	+	—	—
ВМ Basis DynamiX Enterprise	—	+	+	—	+	+	+	+	+	+	—	—
ВМ OpenNebula (ПК СВ ”Брест”)	+	+	+	+	+	+	+	+	+	+	—	—
ВМ VMmanager	—	—	+	—	+	—	—	—	—	—	+	—
ВМ Proxmox	—	—	—	—	—	—	—	—	—	—	—	+

[1] Также zVirt, ROSA Virtualization, РЕД Виртуализация.

[2] Платформы OpenStack и Basis DynamiX Enterprise наряду с KVM используют драйверы VirtIO и VirtIO SCSI для сети и дисков. Для миграции виртуальной машины на ОС Windows или Linux на OpenStack или Basis DynamiX Enterprise необходимо установить в нее драйверы VirtIO и VirtIO SCSI, агент QEMU Guest Agent, cloud-init и убедиться, что они работают. Необходимо учитывать, что драйверы VirtIO могут по-разному работать на различных выпусках ОС Windows и версиях OpenStack и Basis DynamiX Enterprise. Подготовленная машина может не запускаться на платформах из-за особенностей настройки гипервизора, флагов ЦП или несовместимости драйверов. Рекомендуется использовать готовые образы ОС Windows, например, от Cloudbase. Дополнительные сведения для машин на ОС Windows приведены в руководстве OpenStack.

[3] Только машины на ОС Linux с дисками с интерфейсом NVMe.

Инструкции о выполнении миграции см. в следующих разделах:

- Миграция систем из физической машины в виртуальную (P2V): *Миграция систем с физической машины в виртуальную*.
- Миграция систем из виртуальной машины в виртуальную (V2V): *Виртуальная машина*.
- Миграция систем из виртуальной машины в физическую (V2P): *Виртуальная машина* или *Восстановление дисков с помощью загрузочного носителя*.

Хотя миграцию V2P можно выполнить в веб-консоли, в определенных случаях рекомендуется использовать загрузочный носитель. В ряде случаев можно создать носитель для миграции в ESXi или Hyper-V.

Носитель позволяет выполнить следующие действия:

- Выполнить миграцию P2V и миграцию V2V машины Linux с логическими томами (LVM). Используйте агент для Linux или загрузочный носитель, чтобы создать резервную копию, и загрузочный носитель для восстановления.
- Предоставить драйверы для определенного оборудования, которое имеет критически важное значения для загружаемости системы.

Миграция Linux-машины с логическими томами (LVM)

Для миграции физической или виртуальной Linux-машины, у которой есть логические тома (LVM), в виртуальную или физическую машину, необходимо следующее:

1. резервная копия исходной машины должна быть создана с помощью агента, установленного внутри данной машины;

   > **Примечание**
   >
   > Резервная копия виртуальной машины, созданная агентом для соответствующей системы виртуализации, не может быть использована для данного вида миграции.

2. восстановление должно выполняться с помощью загрузочного носителя;
3. в процессе восстановления нужно воспроизвести исходную структуру логических томов.

Миграция Linux-машины, у которой есть логические тома (LVM)

1. Убедитесь, что у вас есть резервная копия машины, которая была создана агентом, установленным внутри исходной машины.
2. Загрузите целевую машину, используя загрузочный носитель.
3. Убедитесь, что в интерфейсе загрузочного носителя используется способ представления дисков и томов как в Linux.
4. Запустите мастер восстановления, выберите резервную копию исходной машины и выберите диски для восстановления.
5. Удостоверьтесь, что количество и емкость дисков целевой машины равны или превосходят количество и емкость дисков исходной машины.
6. Воспроизведите на целевой машине такую же структуру логических томов, как на исходной машине. Для этого нажмите кнопку **Применить RAID/LVM**.
7. Завершите процесс восстановления.

Если операционная система на целевой машине не загружается после восстановления, используйте *универсальное восстановление* для решения этой проблемы.

Увеличение объёма ОЗУ виртуального устройства

Для повышения производительности операций резервного копирования и восстановления объём ОЗУ виртуального устройства (virtual appliance) может быть увеличен. При этом размер его диска должен быть достаточным для размещения как аварийного дампа памяти (при его формировании), так и файлов журналов. В противном случае файл дампа может занять всё дисковое пространство, что приведёт к некорректной работе или полному отказу функций резервного копирования и восстановления виртуальных машин.

Начиная с Кибер Бэкап версии 18.5, объём диска для вновь создаваемых виртуальных устройств по умолчанию составляет 64 ГБ (ранее — 8 ГБ).

У виртуальных устройств, созданных в более ранних версиях Кибер Бэкап, после обновления до версии 18.5 размер диска остаётся прежним. В этом случае для расширения дискового пространства рекомендуется переустановить виртуальное устройство, используя новые образы (подробнее см. в разделе *Установка агентов*), либо выполнить инструкции, приведённые в статье базы знаний.

Резервное копирование облачных виртуальных машин без доступа к гипервизору

Чтобы создать резервную копию виртуальной машины без доступа к гипервизору (т. е. находящейся в облаке), установите агент защиты на такой машине. Операции резервного копирования и восстановления выполняются точно так же, как и на физической машине.

Отличие от физической машины состоит в том, что виртуальные машины, находящиеся в облаке, невозможно загрузить с загрузочного носителя. Если необходимо выполнить восстановление в новую виртуальную машину, следуйте указанной ниже процедуре.

Порядок восстановления машины как виртуальной машины в облаке:

1. Создайте новую виртуальную машину из образа или шаблона в используемом облаке. Новая машина должна иметь такую же конфигурацию диска, как и машина, которую необходимо восстановить.
2. Установите агент для Windows или агент для Linux на новой машине.
3. Восстановите машину из резервной копии, как описано в разделе *Физическая машина*. При настройке восстановления выберите новую машину в качестве целевой.

Требования к сети

Агенты, установленные на машинах, для которых выполняется резервное копирование, должны иметь возможность обмениваться данными с сервером управления по сети.

- Если и агенты, и сервер управления установлены в одном облаке, то никаких дополнительных действий не требуется, так как все машины уже находятся в одной сети.
- Если сервер управления находится вне облака, то машины внутри облака не будут иметь доступа к локальной сети, в которой установлен сервер управления. Чтобы агенты, установленные на таких машинах, могли связываться с сервером управления, необходимо создать подключение виртуальной частной сети (VPN) между локальной и облачной сетями.

  Запросите у вашего поставщика облачной инфраструктуры, чей сервис вы используете, инструкции по созданию подключений VPN, аналогичные инструкциям, приведённым ниже:

  - Windows Azure;
  - Amazon EC2.

Мониторинг, отчёты и аудит

Панель мониторинга **Обзор** даёт возможность отслеживать текущее состояние защищённой инфраструктуры.

Раздел **Отчёты** даёт возможность создавать запланированные отчёты и отчёты по требованию с данными о защищённой инфраструктуре. Этот раздел доступен только при наличии лицензии Кибер Бэкап Расширенная редакция.

Раздел **Журнал аудита** содержит сведения о событиях, произошедших в Кибер Бэкап вследствие действий пользователей или работы системных компонентов.

Панель мониторинга ”Обзор”

Панель мониторинга **Обзор** предоставляет ряд настраиваемых виджетов для обзора защищенной инфраструктуры. Вы можете выбирать из более чем 20 виджетов, представленных в виде круговых диаграмм, таблиц, графиков, линейчатых диаграмм и списков. У виджетов есть активные элементы, на которые можно щёлкнуть для исследования возникших неполадок, их диагностики и устранения. Информация, представленная в виджетах, обновляется каждые пять минут.

Расширенная лицензия также позволяет скачать текущее состояние панели мониторинга или отправить его по электронной почте в файле формата .pdf и (или) .xlsx. Для отправки данных панели мониторинга по электронной почте убедитесь в том, что у вас сконфигурированы настройки *почтового сервера*.

Доступные виджеты зависят от выпуска Кибер Бэкап. Ниже перечислены виджеты, которые доступны во всех выпусках и отображаются по умолчанию:

Виджет	Описание
Статус защиты	Показывает текущее состояние защиты для всех машин.
Действия	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Сводка по активным оповещениям	Показывает сводную информацию об активных оповещениях по их типу и уровню серьезности.
Устройства	Показывает подробную информацию об устройствах в вашей среде.
Подробная информация об активных оповещениях	Показывает подробную информацию об активных оповещениях.
Сводные данные о хранилищах	Показывает подробную информацию о хранилищах резервных копий.

Порядок добавления виджета

Щёлкните **Добавить виджет** и выполните одно из следующих действий:

- Щёлкните виджет, который необходимо добавить. Виджет будет добавлен с настройками по умолчанию.
- Чтобы изменить виджет перед его добавлением, щёлкните значок карандаша, когда виджет выбран. После изменения виджета щёлкните **Готово**.

Порядок изменения расположения виджетов на панели мониторинга

Перетащите виджеты, щёлкнув их имена.

Порядок изменения виджета

Щёлкните значок карандаша рядом с именем виджета. Изменение виджета позволяет переименовать его, изменить диапазон времени, задать фильтры и сгруппировать строки.

Порядок удаления виджета

Щёлкните значок X рядом с именем виджета.

Виджет ”Резервные копии”

В этом виджете отображается общая информация о размере резервных копий .

В верхней строке отображается текущая статистика:

- **Резервная копия создана сегодня**: суммарный размер резервных копий в точках восстановления за последние 24 часа

В нижней строке показана общая статистика:

- Сжатый размер всех резервных копий

Виджет ”Статус защиты”

В этом виджете показано текущее состояние защиты для всех машин.

Машина может быть в одном из следующих состояний:

- Защищенные: машины, для которых применен план защиты.

- Незащищенные: машины, для которых не применен план защиты. Под ними подразумеваются как обнаруженные, так и управляемые машины без примененного плана защиты.
- Управляемое: машины с установленным агентом защиты.
- Обнаружено: машины без установленного агента защиты.

Если щёлкнуть состояние машины, для получения более подробной информации откроется список машин, которые имеют данное состояние.

Обнаруженные машины

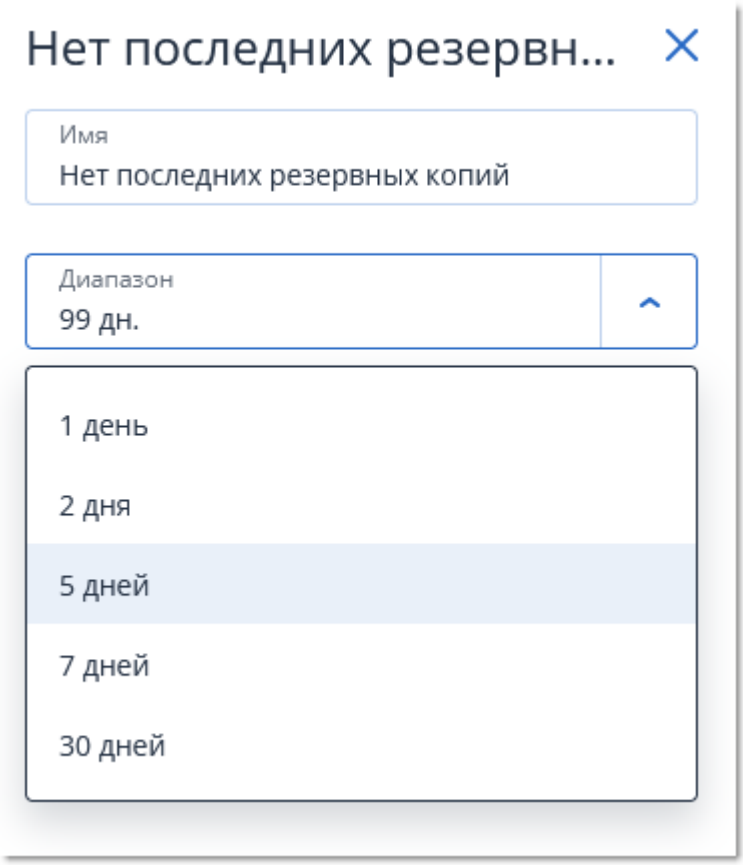
В этом виджете показан список машин, обнаруженных за указанный период времени.

Виджет ”Нет последних резервных копий”

Этот виджет показывает рабочие нагрузки с применяемыми планами защиты, дата последнего успешного резервного копирования которых была ранее диапазона времени, указанного в настройках виджета.



Когда вы добавляете этот виджет, по умолчанию он отображает информацию за последние 5 дней. Вы можете использовать раскрывающееся меню, чтобы выбрать другой период или ввести количество дней вручную. Максимальное количество дней, которое вы можете ввести, составляет 99.



Панель мониторинга ”Оповещения”

Оповещение — это сообщение, предупреждающее о текущей или потенциальной проблеме. Оповещения можно использовать разными способами:

- Раздел **Оповещения** на вкладке **Обзор** позволяет быстро определять и решать проблемы путём мониторинга текущих оповещений.

  > **Примечание**
  >
  > При поиске оповещений нельзя указывать в запросах непарные скобки, а также указывать символы перед парными скобками.

- В области виджета **Устройства** состояние устройства основывается на оповещениях. Колонка **Состояние** позволяет фильтровать устройства с проблемами.
- При настройке *уведомлений по электронной почте* можно выбрать, какие оповещения запустят уведомление.

Оповещение может иметь одну из следующих степеней серьёзности:

- **Критично**;
- **Ошибка**;
- **Предупреждение**.

Можно изменить степень серьёзности оповещения или полностью отключить их с помощью файла настройки оповещений, как описано ниже. Эта операция требует перезапуска службы сервера управления.

Изменение степени серьёзности оповещения не повлияет на уже созданные оповещения.

Файл настройки оповещений

Файл настройки оповещений расположен на машине, где работает сервер управления.

- В Windows: `<путь_установки>\AlertManager\alerts.yaml`.

  Здесь `<путь_установки>` — путь установки сервера управления. По умолчанию используется `%ProgramFiles%\Acronis`.

- В ОС Linux: `/var/lib/Acronis/AlertManager/alerts.yaml`.

Каждое оповещение — это элемент в списке `alerts`.

Ключ `name` идентифицирует оповещение.

Ключ `severity` определяет уровень серьёзности оповещения. Он может иметь одно из следующих значений: `critical` (критично), `error` (ошибка) или `warning` (предупреждение).

Ключ `enabled` определяет, включено ли оповещение. Значение должно быть `true` или `false`. По умолчанию все оповещения включены.

Изменение степени серьёзности оповещений, отключение оповещений

Для изменения степени серьёзности оповещения или его отключения выполните шаги:

1. На машине, на которой установлен сервер управления, откройте в текстовом редакторе файл `alerts.yaml`.
2. Выполните одно из следующих действий:
   - Чтобы изменить уровень серьёзности оповещения, измените для него значение ключа `severity`.
   - Чтобы отключить оповещение, измените для него значение ключа `enabled` на `false`.
3. Сохраните файл.
4. Перезапустите службу сервера управления **Acronis Service Manager Service (ASM)**, как описано

ниже.

Перезапуск службы ASM в ОС Windows

1. В меню **Поиск** операционной системы введите **services.msc** и нажмите **Enter**.
2. Щелкните правой кнопкой мыши службу **Acronis Service Manager Service** и выберите **Перезапустить**.

Перезапуск службы ASM в ОС Linux

В терминале выполните следующую команду:

```
sudo systemctl restart acronis_asm
```

Панель мониторинга ”Действия”

На вкладке **Действия** представлен обзор текущих и последних действий. По умолчанию период хранения составляет 180 дней.

Чтобы настроить содержимое вкладки **Действия**, щёлкните значок шестерни и выберите столбцы, которые нужно отобразить.

Чтобы ход выполнения действия отображался в реальном времени, установите флажок **Обновлять автоматически**.

> **Важно**
>
> Частое обновление нескольких действий снижает производительность сервера управления.

Поиск действий в списке можно выполнить по указанным ниже критериям:

- **Имя устройства** — машина, на которой выполнено действие.
- **Кем запущено** — учётная запись, от имени которой запущено действие.
- **Название плана** — наименование плана защиты.

Кроме того, можно отфильтровать действия по следующим свойствам:

- **Состояние** — например, ”Успешно”, ”С ошибками”, ”Выполняется”, ”Отменено”.
- **Тип** — например, ”Применение плана”, ”Удаление резервных копий”, ”Установка обновлений программного обеспечения”.

- **Время** — например, действия за последние сутки, неделю, месяц или действия в течение указанного периода времени в пределах периода хранения по умолчанию.

Порядок изменения периода хранения сведений о действиях

1. На машине с запущенной службой сервера управления откройте следующий файл конфигурации в текстовом редакторе:
   - В ОС Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`.
   - В ОС Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`.
2. Найдите следующий раздел:

```
database:
connection-string: ””
run-cleanup-at: ”23:59”
cleanup-batch-size: 10
max-cleanup-retries: 10
log-queries: false
max-transaction-retries: 10
shards:
- connection-string: sqlite://task-manager.sqlite
days-to-keep: 180
space: ”default”
key: ”00000000-0000-0000-0000-000000000000”
```

3. Установите нужное значение параметра `days-to-keep`.

> **Примечание**
>
> Существенное изменение продолжительности периода хранения не рекомендуется: сильное уменьшение может привести к удалению незавершённых активностей, а сильное увеличение — к снижению производительности сервера управления.

4. Перезапустите службу Service Manager, как описано в разделе *Использование сертификата, выданного доверенным центром сертификации*.

В результате период хранения сведений о действиях будет изменён.

Отчёты

При наличии лицензии Кибер Бэкап Расширенная редакция в веб-консоли доступна вкладка **Отчёты**, на которой можно просматривать, создавать и настраивать отчёты.

В отчёт попадают те данные, которые отображаются с помощью элементов их визуального представления на панели мониторинга (виджетов). Отчёт можно сформировать, используя предустановленный набор виджетов или же задав собственный пользовательский набор. Для получения отчёта сохраните его в виде файла (файлы XLSX будут содержать исходные цифровые данные).

> **Примечание**
>
> Вы можете настроить отчёты только для отделов, которыми вы управляете. Подробнее об управлении отделами см. в разделе *Управление учётными записями пользователей и отделами организации*.

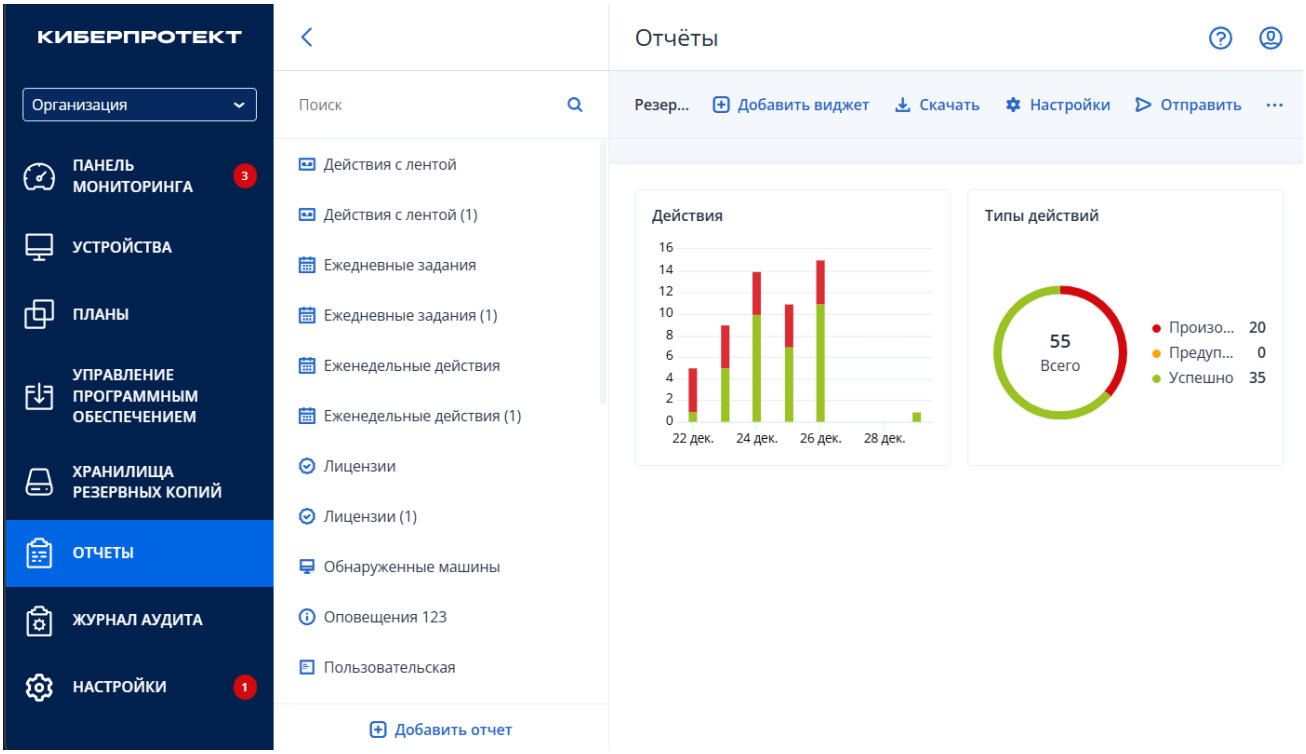
Отчёты могут быть отправлены по электронной почте или загружены по расписанию или по требованию. Для отправки отчётов по электронной почте убедитесь в том, что у вас сконфигурированы настройки *Почтового сервера*. При создании отчёта с использованием стороннего программного обеспечения настройте сохранение отчётов в формате XLSX в указанную папку.

Обзор вкладки ”Отчёты”

В средней части окна программы отображается список созданных отчётов, отсортированный по их имени. Чтобы скрыть панель со списком отчётов, нажмите на иконку со стрелкой в верхней части панели. В результате список отчётов будет скрыт. Чтобы вернуть отображение списка отчётов, щёлкните иконку с тремя горизонтальными линиями (слева от слова ”Отчёты”).

В правой области окна программы для выбранного отчёта отображаются его элементы визуального представления данных в виде виджетов, а также меню действий с отчётом.

Общий вид вкладки **Отчёты** приведён на рисунке ниже.



Варианты отчётов

В таблице перечислены отчёты по умолчанию.

Имя отчёта	Описание
Действия с лентой	Показывает список лент, которые использовались в течение последних 24 часов.
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Еженедельные действия	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Лицензии	Показывает сводную информацию о доступных лицензиях.
Обнаруженные машины	Показывает все машины, обнаруженные в сети организации.
Оповещения	Показывает оповещения, выполненные за указанный период времени.
Хранилища	Показывает статистику использования хранилищ резервных копий за указанный период времени.
Резервные копии	Показывает подробную информацию о текущих резервных копиях и точках восстановления.
Сводка	Показывает сводную информацию об устройствах, защищённых за указанный период времени.
Текущий статус	Показывает текущий статус вашей среды.
Пользовательская	Позволяет создать пустой отчёт и настроить его.

Основные операции с отчётами

С отчётами можно выполнить следующие операции:

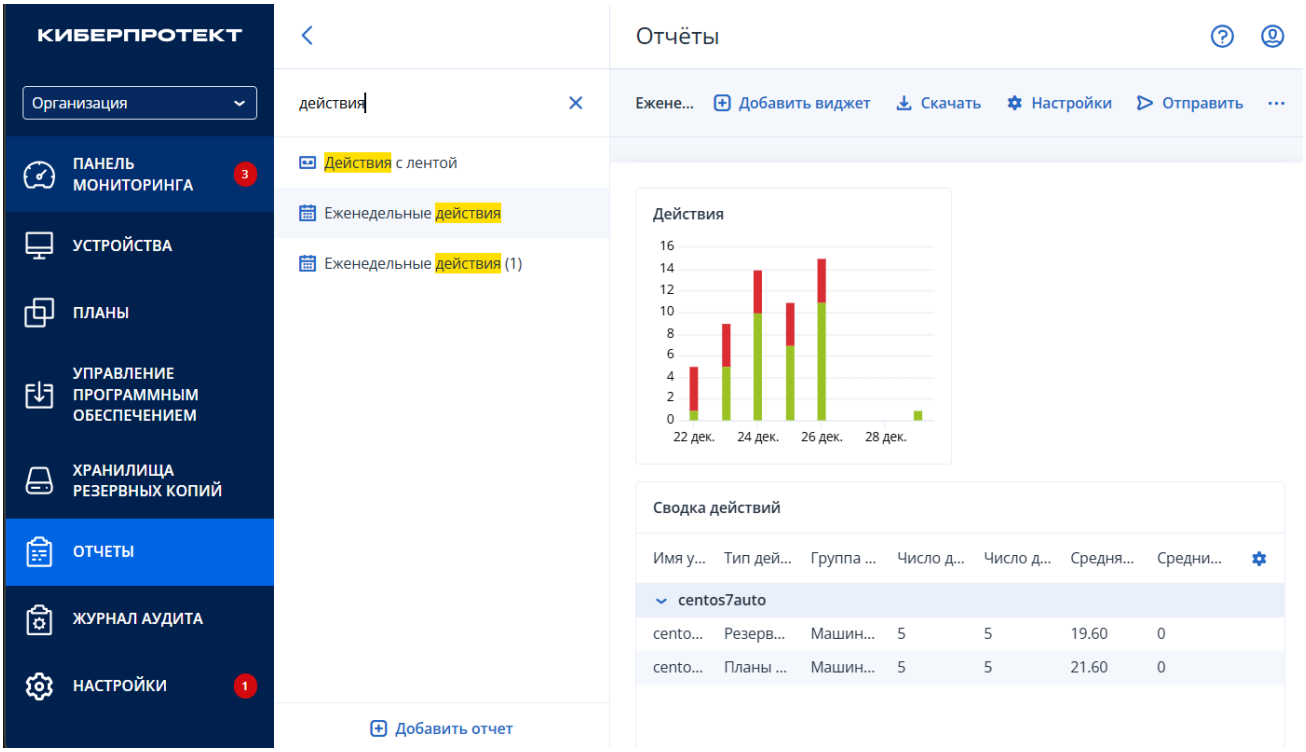
- просмотреть отчёт;
- добавить новый отчёт;
- добавить в отчёт элемент визуального представления данных;
- настроить порядок отображения в отчёте элементов визуального представления данных;
- удалить из отчёта элемент визуального представления данных;
- сохранить файл отчёта на текущей машине;
- переименовать отчёт;
- изменить диапазон времени для всех виджетов, включённых в отчёт;
- запланировать сохранение и (или) отправку отчёта по электронной почте;
- отправить файл отчёта по электронной почте по требованию;
- создать копию отчёта;
- экспортировать структуру отчёта;
- импортировать структуру отчёта;
- создать дамп данных отчёта;
- удалить отчёт.

Просмотр отчёта

Для просмотра отчёта щёлкните его имя в списке. В результате в правой области окна программы для выбранного отчёта будут отображены его элементы визуального представления данных в виде виджетов, а также меню действий с отчётом.

Виджеты являются интерактивными элементами. Например, некоторые из них позволяют получить больше информации при наведении курсора на отображаемые в диаграммах данные и нажатии на них.

Для поиска нужного отчёта введите его имя в строку поиска. Во время ввода будут отображаться отчёты, имя которых соответствует введённой комбинации символов.

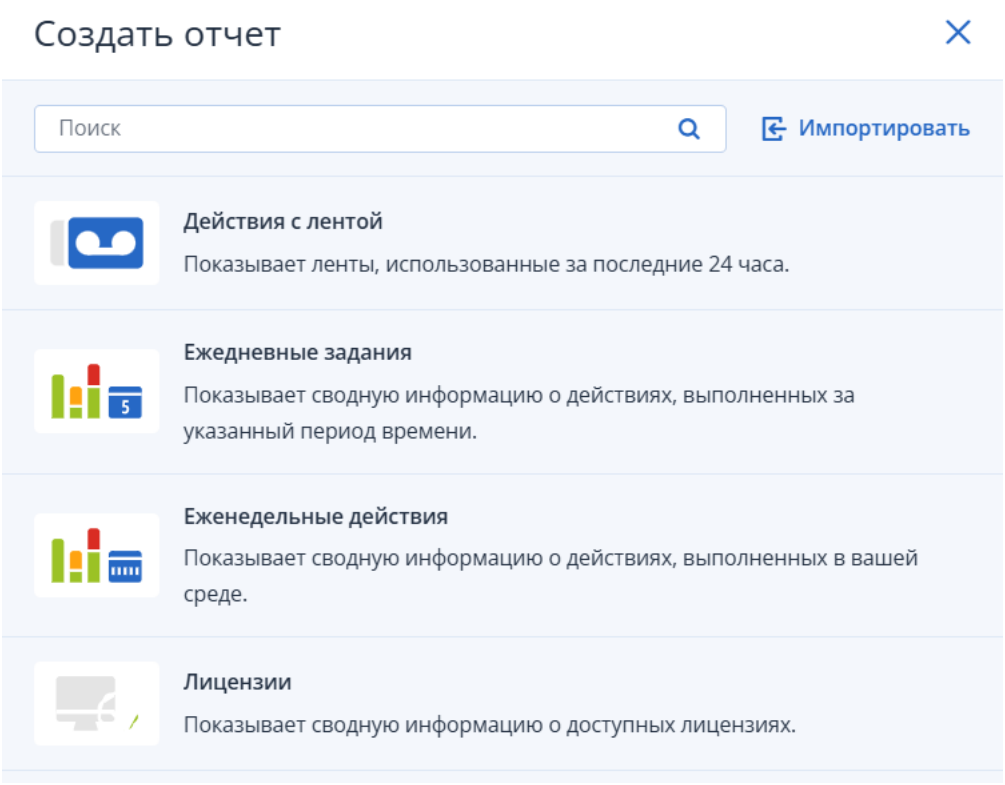


Порядок добавления отчёта

Вы можете добавить отчёт с предопределённым набором элементов визуального представления данных в виде виджетов или настроить пользовательский отчёт со своим набором.

Чтобы добавить отчёт, выполните следующие шаги:

1. В нижней части панели со списком отчётов щёлкните **Добавить отчёт**.
2. В открывшемся окне выберите тип отчёта, щёлкнув его имя.



В результате новый отчёт будет добавлен, его имя будет отображено в списке отчётов, а в нижней правой части окна появится сообщение **Отчёт создан**.

> **Примечание**
>
> При создании отчёту присваивается имя по умолчанию, соответствующее выбранному типу отчёта. При необходимости отчёт можно переименовать (см. далее в статье).

> **Примечание**
>
> Структура отчёта типа **Пользовательская** не содержит предустановленных элементов визуального представления данных в виде виджетов, их необходимо добавить в отчёт самостоятельно (см. далее в статье).

Добавление в отчёт элемента визуального представления данных

Элементы визуального представления данных в виде виджетов можно добавить в любой отчёт, для этого выполните следующие шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Добавить виджет**.

3. В открывшемся окне выберите виджет, щёлкнув его имя.

   В результате выбранный элемент визуального представления данных будет добавлен в интерфейс отчёта, а в нижнем правом углу окна программы появится всплывающее сообщение **Виджет добавлен**.

   > **Примечание**
   >
   > Новый элемент будет отображаться в верхней части отчёта. При необходимости его можно переместить (см. далее в статье).

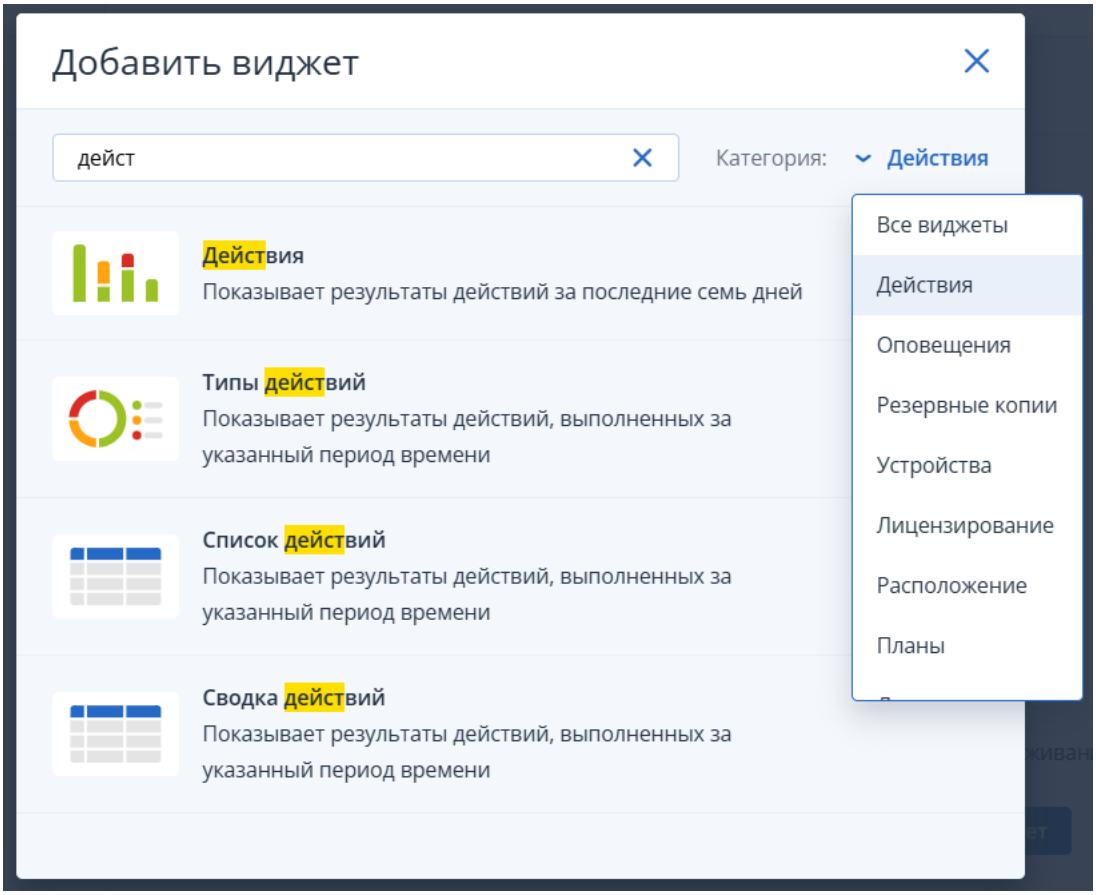
4. [Необязательно] Настройте виджет, для этого нажмите кнопку **Настроить** в области выбранного виджета и выполните необходимые настройки.

   > **Примечание**
   >
   > Для разных видов виджетов предусмотрены различные настройки.

Для поиска виджета при его добавлении Вы можете:

- ввести его имя в строку поиска (во время ввода будут отображаться виджеты, имя которых соответствует введённой комбинации символов);
- настроить отображение виджетов определённой категории, выбрав её в выпадающем списке **Категория** в верхней правой части окна;
- просмотреть виджеты доступных категорий поочерёдно, щёлкнув по имени категории для разворачивания или сворачивания списка её виджетов.

> **Примечание**
>
> При использовании нескольких методов поиска виджета их условия применяются вместе. Например, при вводе названия виджета в строке поиска и выборе категории будут отображены виджеты, соответствующие обоим условиям.



Настройка порядка отображения в отчёте элементов визуального представления данных

Чтобы настроить в отчёте порядок отображения элементов визуального представления данных, наведите курсор на название виджета и, зажав левую клавишу мыши, переместите его на новое место.

Удаление из отчёта элемента визуального представления данных

Чтобы удалить из отчёта элемент визуального представления данных, нажмите в его области значок крестика.

В результате элемент будет удалён, а внизу справа появится всплывающее сообщение **Виджет удалён**.

> **Примечание**
>
> Данную операцию можно отменить, нажав **Отмена** в области всплывающего сообщения.

Сохранение файла отчёта на текущей машине

Можно сохранить файл выбранного отчёта на машине, с помощью которой открыта веб-консоль. Для этого выполните следующие шаги:

1. Нажмите кнопку **Скачать** на панели меню выбранного отчёта.
2. Выберите один из вариантов:
   - Excel и PDF (будут скачаны два файла: один в формате XLSX, другой — в формате PDF);
   - Excel (будет скачан один файл в формате XLSX);
   - PDF (будет скачан один файл в формате PDF).

   В результате выполненных действий отчёт будет сохранён на текущей машине.

Переименование отчёта

Чтобы переименовать отчёт, выполните следующие действия:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Настройки**.
3. Введите новое имя отчёта в поле **Имя**.
4. Нажмите кнопку **Сохранить**.

В результате выполненных действий отчёт будет переименован.

Изменение диапазона времени для всех элементов визуального представления данных, включённых в отчёт

Чтобы настроить отображение данных за определённый период времени в элементах визуального представления, выполните следующие шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Настройки**.
3. Выберите значение в выпадающем списке **Диапазон**.
4. Нажмите кнопку **Сохранить**.

В результате в элементах визуального представления данных будет отображена информация за выбранный период времени.

Планирование сохранения и (или) отправки файла с отчётом по электронной почте

Сохранение файла с отчётом или отправка его по электронной почте, либо оба действия одновременно могут выполняться по установленному расписанию.

Для того чтобы установить расписание, выполните шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Настройки**.
3. Переведите переключатель **Запланировано** в положение **Включено**.
4. Установите флажки для требуемых действий (можно выбрать оба варианта):
   - **отправлять отчёт по электронной почте**;
   - **сохранить как файл на сервере управления**.

   В зависимости от выбора укажите адрес электронной почты, путь к папке или и то, и другое.

   > **Важно**
   >
   > Для отправки отчётов по электронной почте убедитесь в том, что у вас сконфигурированы настройки *Почтового сервера*.

5. Выберите формат формат отчёта: PDF, XLSX или и то, и другое.
6. Выберите язык в выпадающем списке (доступны русский и английский).
7. Настройте отчётный период (ежемесячно, еженедельно или ежедневно).
8. Укажите дни и время сохранения и (или) отправления отчёта.
9. Нажмите кнопку **Сохранить**.

Отправление файла с отчётом по электронной почте по требованию

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите кнопку **Отправить**.

> **Важно**
>
> Для отправки отчётов по электронной почте убедитесь в том, что у вас сконфигурированы настройки *Почтового сервера*.

Создание копии отчёта

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия в правом верхнем углу.
3. Выберите **Клонировать**.

В результате будет создана копия отчёта, его имя будет отображаться в списке отчётов, а в нижнем правом углу окна программы появится всплывающее сообщение **Отчёт создан**.

Экспорт структуры отчёта

Вы можете экспортировать структуру отчёта (набор виджетов и настройки расписания) в файл JSON. Это может оказаться полезным при переустановке сервера управления или для копирования структуры отчёта на другой сервер управления.

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия в правом верхнем углу.
3. Выберите **Экспорт**.

В результате на машине, с помощью которой открыта веб-консоль, будет будет сохранён файл JSON с параметрами отчёта.

Импорт структуры отчёта

Вы можете импортировать структуру отчёта (набор виджетов и настройки расписания) из файла JSON. Это может оказаться полезным при переустановке сервера управления или для копирования структуры отчёта из другого сервера управления.

Чтобы импортировать структуру отчёта, нажмите кнопку **Добавить отчёт** внизу списка отчётов. Затем в открывшемся окне нажмите **Импортировать** и выберите файл со структурой отчёта. В результате выполненных действий отчёт с импортированной структурой будет добавлен, а в нижнем правом углу окна программы появится всплывающее сообщение ”Отчёт создан”.

Дамп данных отчёта

Вы можете сохранить дамп данных отчёта в файл CSV. Дамп содержит все данные отчёта (без фильтрации) за определённый промежуток времени.

ПО динамически генерирует дамп данных. При указании большого промежутка времени выполнение данного действия может занять продолжительное время.

Для сохранения дампа данных отчёта выполните шаги:

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия в правом верхнем углу.
3. Выберите **Данные дампа**.
4. В открывшемся окне в поле **Расположение** укажите путь к папке для файла CSV.
5. В поле **Диапазон времени** выберите диапазон времени.
6. Нажмите кнопку **Сохранить**.

В результате выполненных действий файл CSV будет сохранён в указанную папку.

Удаление отчёта

1. Выберите отчёт в списке, щёлкнув его имя.
2. Нажмите значок многоточия в правом верхнем углу.
3. Выберите **Удалить отчёт**.
4. Подтвердите действие, нажав кнопку **Удаление** во всплывающем окне **Удалить отчёт**.

В результате выполненных действий отчёт будет удалён.

Журнал аудита

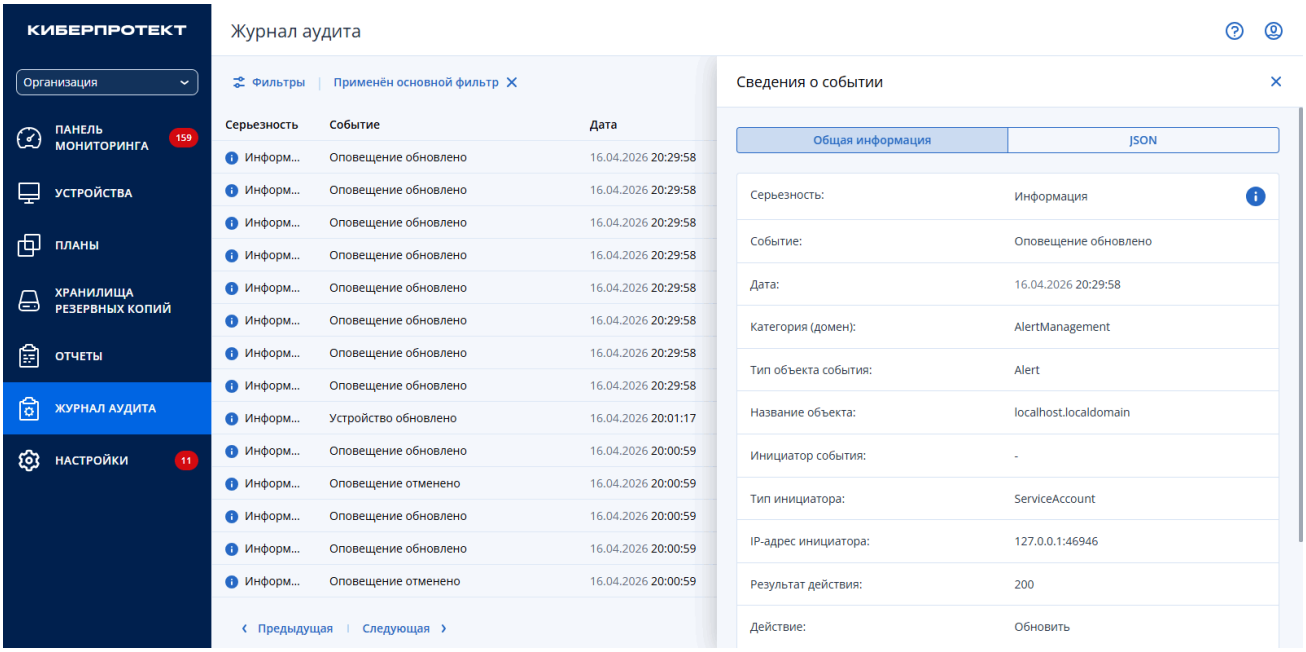
Журнал аудита содержит сведения о событиях, произошедших в Кибер Бэкап вследствие действий пользователей или работы системных компонентов (подробнее см. в разделе *Регистрируемые события*).

По умолчанию журнал аудита хранится в базе данных продукта, однако при необходимости записи журнала можно отправлять на Syslog-сервер (см. *Отправка записей журнала аудита на Syslog-сервер*).

Чтобы просмотреть список событий, перейдите в раздел **Журнал аудита**. Он доступен, только если включено *сохранение событий аудита*. События отображаются постранично с сортировкой по дате и времени в обратном порядке (от более новых к более старым). Для переключения между страницами используйте кнопки **< Предыдущая** и **Следующая >** внизу слева. Для настройки количества отображаемых записей журнала выберите значение в списке **Показывать строк:** или введите в поле ввода произвольное значение.

Для настройки отображения информации о событиях щёлкните шестерёнку вверху справа и в открывшемся окне установите или снимите флажки для выбранных столбцов. После этого внесённые изменения будут применены. Для закрытия окна щёлкните вне его области.

Для просмотра сведений о событии щёлкните по нему в списке.



На вкладке **Общая информация** будут отображены сведения о выбранном событии. При необходимости на вкладке **JSON** можно просмотреть подробные сведения о событии в формате JSON, а также скопировать их, нажав соответствующую кнопку.

Срок хранения записи в журнале — 90 дней. Записи, срок хранения которых истёк, удаляются автоматически. Кроме того, очистить журнал аудита можно вручную (см. *Управление журналом аудита*).

Основной поиск событий

Чтобы найти события с помощью основного поиска, выполните следующие действия:

1. Щёлкните **Фильтры** над списком событий и перейдите на вкладку **Основной**.
2. Укажите от одного до нескольких критериев поиска:
    - название отдела,
    - уровень важности события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
    - период времени (можно выбрать один из предопределённых периодов или вручную указать его начало и окончание),
    - тип объекта события (можно выбрать от одного до нескольких значений в выпадающем списке, в котором приведены все возможные значения),
    - объект события,
    - инициатор события,
    - тип инициатора события (можно выбрать от одного до нескольких значений в выпадающем

списке, в котором приведены все возможные значения),

- IP-адрес инициатора события.

3. Нажмите **Применить** для отображения результатов.

Расширенный поиск событий

Чтобы найти события с помощью расширенного поиска, выполните следующие действия:

1. Щёлкните **Фильтры** над списком событий и перейдите на вкладку **Расширенный**.
2. Введите поисковый запрос. Параметры и операторы, которые можно использовать в запросе, приведены в таблицах ниже.
3. Нажмите **Применить** для отображения результатов.

Кроме параметров и операторов, можно использовать круглые скобки для группировки условий поиска, например:

```
(status = '204' OR status = '200') AND action = 'Login'
```

Таблица 14.3: Параметры расширенного поиска

Параметр	Описание	Примеры
`uuid`	Идентификатор события. Идентификатор можно узнать, просмотрев JSON-представление события.	`uuid = '0193c41a-6f13-7aa4-8448-2cad89f23385'`
`tenant_name`	Название отдела.	`tenant_name = 'Accounting'`
`src_ip`	IP-адрес и порт инициатора события.	`src_ip LIKE '192.168.10.10%'`
`level`	Уровень важности события. Возможные значения: • `info` — информация; • `warning` — предупреждение; • `critical` — критично; • `error` — ошибка.	`level = 'warning'`
`obj_name`	Имя объекта события.	`obj_name = 'WIN2019X64-5\Administrator'`

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Параметр	Описание	Примеры
`obj_domain`	Категория (область) события. Возможные значения можно узнать, просмотрев JSON-представления событий.	`obj_domain = 'TaskManagement'`
`obj_type`	Название типа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий.	`obj_type = 'Task'`
`obj_subtype`	Название подтипа объекта события. Возможные значения можно узнать, просмотрев JSON-представления событий.	`obj_subtype = 'Backup::Disks'`
`action`	Название действия. Возможные значения можно узнать, просмотрев JSON-представления событий.	`action IN ('Login', 'Logout')`
`status`	Результат действия.	`status = '200'`
`principal_type`	Название типа инициатора события. Возможные значения: • `User` — инициатором события является пользователь; • `ServiceAccount` — инициатором события является системный компонент.	`principal_type = 'User'`
`principal_name`	Имя инициатора события.	`principal_name LIKE '%admin%'`
`event.timestamp`	Дата и время события. Операторы поиска **<**, **>**, **=**, **!=**, **IN**, **NOT IN** и **LIKE** не поддерживаются.	`event.timestamp <= '2024-11-30 12:00:00Z'` `event.timestamp >= '2024-11-30 12:00:00Z'`

Таблица 14.4: Операторы расширенного поиска

Оператор	Описание	Примеры
`<параметр> = <значение>`	Оператор сравнения ”равно”.	`level = 'warning'`
`<параметр> != <значение>`	Оператор сравнения ”не равно”.	`level != 'info'`

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Оператор	Описание	Примеры
`<параметр> < <значение>`	Оператор сравнения ”меньше”.	`status < '400'`
`<параметр> > <значение>`	Оператор сравнения ”больше”.	`status > '200'`
`<параметр> <= <значение>`	Оператор сравнения ”меньше или равно”.	`event.timestamp <= '2024-11-30 12:00:00Z'`
`<параметр> >= <значение>`	Оператор сравнения ”больше или равно”.	`event.timestamp >= '2024-11-30 12:00:00Z'`
`<выражение> AND <выражение>`	Логический оператор ”И”.	`src_ip LIKE '192.168.10.10%' AND level = 'info'`
`<выражение> OR <выражение>`	Логический оператор ”ИЛИ”.	`level = 'critical' OR level = 'warning'`
`<параметр> IN (<значение 1>, ..., <значение n>)`	Проверяет, присутствует ли значение параметра в заданном наборе значений.	`level IN ('critical', 'warning')`
`<параметр> NOT IN (<значение 1>, ..., <значение n>)`	Проверяет, отсутствует ли значение параметра в заданном наборе значений.	`level NOT IN ('critical', 'warning')`
`<параметр> LIKE <шаблон значения>`	Проверяет, соответствует ли значение параметра указанному шаблону (регистр символов не учитывается). В шаблоне можно использовать знак процента (**%**), который подменяет любую, в том числе и пустую, последовательность символов.	`principal_name LIKE '%admin%'`

Использование сохранённых поисковых запросов

Чтобы сохранить поисковый запрос, нажмите **Сохранить как шаблон**, введите имя и при необходимости описание запроса и нажмите **Сохранить**.

Сохранённый запрос можно выполнить, выбрав его в поле **Шаблон фильтрации** и нажав **Применить**. Для удаления сохраненного запроса щёлкните значок корзины рядом с его именем и нажмите **Удалить** в окне подтверждения удаления.

Регистрируемые события

В журнале аудита Кибер Бэкап фиксируются события следующих категорий:

- назначение статусов оповещениям;
- регистрация агентов;
- аутентификация и авторизация;

- действия с планами защиты;
- действия с устройствами и их группами;
- резервное копирование;
- действия с пользователями и группами;
- действия с хранилищами;
- действия с архивами.

Более подробная информация о записываемых в журнал событиях приведена в таблицах ниже.

События назначения статусов оповещениям

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Оповещение создано (Alert created)	Информация (info)	Имя ресурса	Alert	—	200
Оповещение обновлено (Alert updated)	Информация (info)	Имя ресурса	Alert	—	200
Оповещение отменено (Alert reset)[1]	Информация (info)	Имя ресурса	Alert	Имя пользователя	204

События регистрации агентов

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Агент зарегистрирован (Agent registered)	Информация (info)	Имя агента (имя хоста)	Agent	—	200
Регистрация агента отменена (Agent registration revoked) При отмене регистрации через *командную строку* или при *удалении продукта*.	Информация (info)	Имя агента (имя хоста)	Agent	—	200

(продолжается на следующей странице)

[1] При использовании массового действия с оповещениями, например, **Очистить всё**, для каждого оповещения будет создана отдельная запись в журнале аудита.

(продолжение с предыдущей страницы)

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Регистрация агента отменена (Agent registration revoked) При удалении машины через веб-консоль (подробнее см. в разделе *Удаление продукта*).	Информация (info)	Имя агента (имя хоста)	Agent	Имя пользователя, инициировав-шего удаление агента	200

События аутентификации и авторизации

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Резуль-тат дей-ствия
Успешный вход в систему (Logged in)	Информация (info)	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	Session	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200
Не удалось войти в систему (Fail to log in)	Предупрежде-ние (warning)	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	Session	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	401
Успешный выход из системы (Logged out)	Информация (info)	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	Session	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200

События при действиях с планами защиты

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
План защиты создан (Backup plan created)	Информация (info)	Имя плана	Policy	Имя пользователя	20x
План защиты обновлён (Backup plan updated)	Информация (info)	Имя плана	Policy	Имя пользователя	20x
План защиты удалён (Backup plan deleted)	Информация (info)	Имя плана	Policy	Имя пользователя	204
Статус установки плана (Plan deployment state)	Информация (info)	Имя плана	Policy	—	200
Политика применена к устройству (Policy applied to workload)	Информация (info)	Имя плана	PolicyApplication	Имя пользователя	20x

События при действиях с устройствами и их группами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Устройство создано (Workload created)	Информация (info)	Имя ресурса	Workload	—	200
Устройство обновлено (Workload updated)	Информация (info)	Имя ресурса	Workload	—	200
Устройство удалено (Workload deleted)	Информация (info)	Имя ресурса	Workload	—	200
Группа устройств создана (Workload group created)	Информация (info)	Имя группы	GroupMembership	Имя пользователя	201

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Участники добавлены в статическую группу устройств (Workload static group member added)	Информация (info)	Имя группы	GroupMembership	—	200
Участники добавлены в динамическую группу устройств (Workload dynamic group member added)	Информация (info)	Имя группы	GroupMembership	—	200
Участники удалены из статической группы устройств (Workload static group member removed)	Информация (info)	Имя группы	GroupMembership	—	200
Участники удалены из динамической группы устройств (Workload dynamic group member removed)	Информация (info)	Имя группы	GroupMembership	—	200
Группа устройств удалена (Workload group deleted)	Информация (info)	Имя группы	GroupMembership	Имя пользователя	200

События резервного копирования

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Резервное копирование помещено в очередь (Backup queued)	Информация (info)	Имя ресурса	Task	Если тип инициатора — **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора — **ServiceAccount**: '-'.	200
Резервное копирование назначено агенту (Backup assigned to agent)	Информация (info)	Имя ресурса	Task	Если тип инициатора — **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора — **ServiceAccount**: '-'.	200
Ошибка при назначении резервного копирования агенту (Error assigning backup to agent)	Предупреждение (warning), если задача завершена с кодом warning. Критично (critical), если задача завершена с кодом error.	Имя ресурса	Task	Имя пользователя	500
Резервное копирование начато (Backup started)	Информация (info)	Имя ресурса	Task	Если тип инициатора — **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора — **ServiceAccount**: '-'.	200

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Резервное копирование выполнено (Backup completed)	Информация (info)	Имя ресурса	Task	Если тип инициатора — **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора — **ServiceAccount**: '-'.	200
Резервное копирование завершилось с предупреждением (Backup finished with warning)	Предупреждение (warning), если задача завершена с кодом warning. Критично (critical), если задача завершена с кодом error.	Имя ресурса	Task	Если тип инициатора — **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора — **ServiceAccount**: '-'.	200
Резервное копирование завершилось с ошибкой (Backup failed)	Предупреждение (warning), если задача завершена с кодом warning. Критично (critical), если задача завершена с кодом error.	Имя ресурса	Task	Если тип инициатора — **User**: • имя хоста и имя пользователя (для ОС Windows); • имя пользователя (для ОС Linux). Если тип инициатора — **ServiceAccount**: '-'.	500
Задача на восстановление создана (Recovery task created)	Информация (info)	—	Activity	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200
Задача на восстановление запущена (Recovery task started)	Информация (info)	Имя ресурса	Activity	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Задача на восстановление выполнена (Recovery task completed)	Информация (info)	Имя ресурса	Activity	Для ОС Windows: имя хоста и имя пользователя. Для ОС Linux: имя пользователя.	200

События действий с пользователями и группами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Изменение привилегий пользователя/группы (User/group privileges updated)	Информация (info)	-/BUILTIN (для группы Administrators)	UserPrivileges	Имя пользователя	200

События действий с хранилищами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Хранилище создано (Storage created)	Информация (info)	Имя хранилища	Vault	—	200
Хранилище обновлено (Storage updated)	Информация (info)	Имя хранилища	Vault	• Имя пользователя (если тип инициатора — **User**); • '-' (если тип инициатора — **ServiceAccount**).	200

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Хранилище удалено (Storage deleted)	Информация (info)	Имя хранилища	Vault	—	200

События действий с архивами

Событие	Серьёзность	Название объекта	Тип объекта события	Инициатор события	Результат действия
Архив создан (Archive created)	Информация (info)	Имя файла резервной копии	Archive	—	200
Архив обновлён (Archive updated)	Информация (info)	Имя файла резервной копии	Archive	—	200
Архив удалён (Archive deleted)	Информация (info)	Имя файла резервной копии	Archive	—	200
Точка восстановления создана (Recovery point created)	Информация (info)	Имя точки восстановления (см. далее)	RecoveryPoint	—	200
Точка восстановления удалена (Recovery point deleted)	Информация (info)	Имя точки восстановления (см. далее)	RecoveryPoint	—	200

Имя точки восстановления задаётся в формате `<ГГГГ>-<ММ>-<ДД> <чч>:<мм>:<сс> <смещение> UTC`.

В этом выражении:

- `<ГГГГ>` — год четырьмя цифрами (например, `2026`).
- `<ММ>` — месяц двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `06`).
- `<ДД>` — день двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `02`).

- `<чч>` — часы двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `09`).
- `<мм>` — минуты двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `07`).
- `<сс>` — секунды двумя цифрами; если значение меньше 10, то перед ним указывается ноль (например, `05`).
- `<смещение>` — смещение времени относительно UTC (например, `+0000`).

Пример: `2026-06-02 09:07:05 +0000 UTC`.

Настройка внешнего мониторинга средствами Grafana

Кибер Бэкап позволяет с помощью OpenTelemetry Collector передавать различные данные телеметрии в системы внешнего мониторинга.

Далее в разделе будет рассмотрена настройка для системы мониторинга Grafana.

Настройка состоит из следующих шагов:

1. Создание учётной записи администратора с ролью **Оператор мониторинга** (см. раздел *Отделы и административные учетные записи*).
2. Настройка OpenTelemetry Collector.
3. Настройка источников данных для системы мониторинга (см. разделы *Настройка Prometheus в качестве источника данных* и *Настройка Grafana Loki в качестве источника данных*).
4. Настройка системы мониторинга Grafana (см. раздел *Настройка системы мониторинга Grafana*).

Настройка OpenTelemetry Collector

Настройка производится на машине с сервером управления Кибер Бэкап и состоит из следующих шагов:

- Настройка Memory Limiter. Memory Limiter позволяет OpenTelemetry Collector корректно работать с данными телеметрии, не выходя при этом за рамки потребления оперативной памяти.
- Настройка данных телеметрии. В данные телеметрии необходимо добавить специальные метаданные для её идентификации в системах внешнего мониторинга.

Настройка Memory Limiter

1. Откройте конфигурационный файл `config.yml`:
   - в ОС Linux: `/usr/lib/Acronis/OpenTelemetryCollector/config.yml`;
   - в ОС Windows: `C:\Program Files\Acronis\OpenTelemetryCollector\config.yml`.
2. Измените значения параметров `memory_limiter` на следующие:

```
processors:
  memory_limiter:
    check_interval: 1s
    limit_mib: 500
    spike_limit_mib: 100
```

3. Добавьте параметр `memory_limiter` в раздел `service.pipelines`:

```
service:
  pipelines:
    metrics:
      receivers: [otlp]
      processors: [batch, memory_limiter]
      exporters: [file/metrics]
    logs:
      receivers: [otlp]
      processors: [batch, memory_limiter]
      exporters: [file/metrics]
```

> **Важно**
>
> `memory_limiter` необходимо добавить и для `metrics`, и для `logs`.

Настройка данных телеметрии

1. Откройте конфигурационный файл `config.yml`:
   - в ОС Linux: `/usr/lib/Acronis/OpenTelemetryCollector/config.yml`;
   - в ОС Windows: `C:\Program Files\Acronis\OpenTelemetryCollector\config.yml`.
2. Добавьте параметр `resource` в раздел `Processor`:

```
processors:
  resource:
    attributes:
    - key: ru.cyberprotect.cb.stand.name
      action: upsert
      value: YOUR_VALUE
```

где `ru.cyberprotect.cb.stand.name` и `YOUR_VALUE` — метаданные, по которым системы внешнего мониторинга смогут идентифицировать метрики и записи журналов.

Важно

Значения метаданных должны быть уникальны и при этом иметь низкую кардинальность.

3. Добавьте параметр `resource` в раздел `service:pipelines`:

```
service:
  pipelines:
    metrics:
      receivers: [otlp]
      processors: [batch, memory_limiter, resource]
      exporters: [file/metrics]
    logs:
      receivers: [otlp]
      processors: [batch, memory_limiter, resource]
      exporters: [file/metrics]
```

Важно

`resource` необходимо добавить и для `metrics`, и для `logs`.

Настройка Prometheus в качестве источника данных

Настройка Prometheus в качестве источника данных состоит из следующих шагов:

1. Настройка OpenTelemetry Collector для предоставления двух специальных точек доступа (далее — конечная точка) `/metrics`:
   - с метриками сервера управления Кибер Бэкап;
   - с метриками внутренней телеметрии.

2. Настройка Node Exporter или Windows Exporter в зависимости от используемой ОС.
3. Настройка Prometheus для сбора метрик.

Настройка OpenTelemetry Collector

Добавление конечной точки с метриками сервера управления Кибер Бэкап

1. Откройте конфигурационный файл `config.yml`:
   - в ОС Linux: `/usr/lib/Acronis/OpenTelemetryCollector/config.yml`;
   - в ОС Windows: `C:\Program Files\Acronis\OpenTelemetryCollector\config.yml`.
2. Добавьте в раздел `exporters` конечную точку:

   ```
   exporters:
     prometheus:
       endpoint: 0.0.0.0:8889
       resource_to_telemetry_conversion:
         enabled: true
   ```

   где `0.0.0.0:8889` — строка, указывающая IP-адрес и порт для конечной точки `/metrics`.
3. Добавьте конечную точку в раздел `service.pipelines`:

   ```
   service:
     pipelines:
       metrics:
         receivers: [otlp]
         processors: [batch, memory_limiter, resource]
         exporters: [file/metrics, prometheus]
   ```

Теперь основные метрики OpenTelemetry Collector доступны на конечной точке `/metrics` в стандартом формате Prometheus.

Добавление конечной точки для внутренней телеметрии

OpenTelemetry Collector может предоставлять различную информацию о своей работе в виде метрик. Это позволяет наблюдать за его работой и реагировать на проблемы.

Для настройки внутренней телеметрии:

1. Откройте конфигурационный файл `config.yml`:
   - в ОС Linux: `/usr/lib/Acronis/OpenTelemetryCollector/config.yml`;

- в ОС Windows: `C:\Program Files\Acronis\OpenTelemetryCollector\config.yml`.

2. Добавьте в раздел `service.telemetry` данные конечной точки:

```
service:
  telemetry:
    resource:
      ru.cyberprotect.cb.stand.name: YOUR_VALUE
```

> **Важно**
>
> `YOUR_VALUE` — значение атрибута `ru.cyberprotect.cb.stand.name`, указанное при настройке данных телеметрии (см. подраздел ”Настройка данных телеметрии” в разделе *Настройка внешнего мониторинга*).

Теперь внутренние метрики OpenTelemetry Collector будут доступны по адресу `http://127.0.0.1:8888/metrics`.

При необходимости укажите IP-адрес и порт для конечной точки в разделе `service.telemetry`:

```
service:
  telemetry:
    resource:
      ru.cyberprotect.cb.stand.name: YOUR_VALUE
    metrics:
      readers:
        - pull:
            exporter:
              prometheus:
                host: '0.0.0.0'
                port: 8890
```

> **Важно**
>
> `YOUR_VALUE` — значение атрибута `ru.cyberprotect.cb.stand.name`, указанное при настройке данных телеметрии (см. подраздел ”Настройка данных телеметрии” в разделе *Настройка внешнего мониторинга*).
>
> `host` и `port` — IP-адрес и порт, по которым доступна конечная точка `/metrics`.

Перезапустите службу сервера управления Кибер Бэкап.

Настройка Node Exporter

В ОС Linux для сбора различных системных метрик вроде загрузки ЦП, использования памяти и сетевой статистики можно использовать специальный инструмент – Node Exporter.

Скачайте актуальную версию Node Exporter, распакуйте и запустите:

```
# NOTE: Replace the URL with one from the above mentioned "downloads" page.
# Node Exporter is available for multiple OS targets and architectures.
# Downloads are available at:
# https://github.com/prometheus/node_exporter/releases/download/v<VERSION>/node_exporter-<VERSION>
↪.<OS>-<ARCH>.tar.gz
#
# <VERSION>, <OS>, and <ARCH> are placeholders:
# - <VERSION>: Release version (e.g., 1.10.2)
# - <OS>: Operating system (e.g., linux, darwin, freebsd)
# - <ARCH>: Architecture (e.g., amd64, arm64, 386)
#
# For this example, we will use Node Exporter version 1.10.2 for a Linux system with amd64¬
↪architecture.

wget https://github.com/prometheus/node_exporter/releases/download/v1.10.2/node_exporter-1.10.2.
↪linux-amd64.tar.gz
tar xvfz node_exporter-1.10.2.linux-amd64.tar.gz
cd node_exporter-1.10.2.linux-amd64
./node_exporter
```

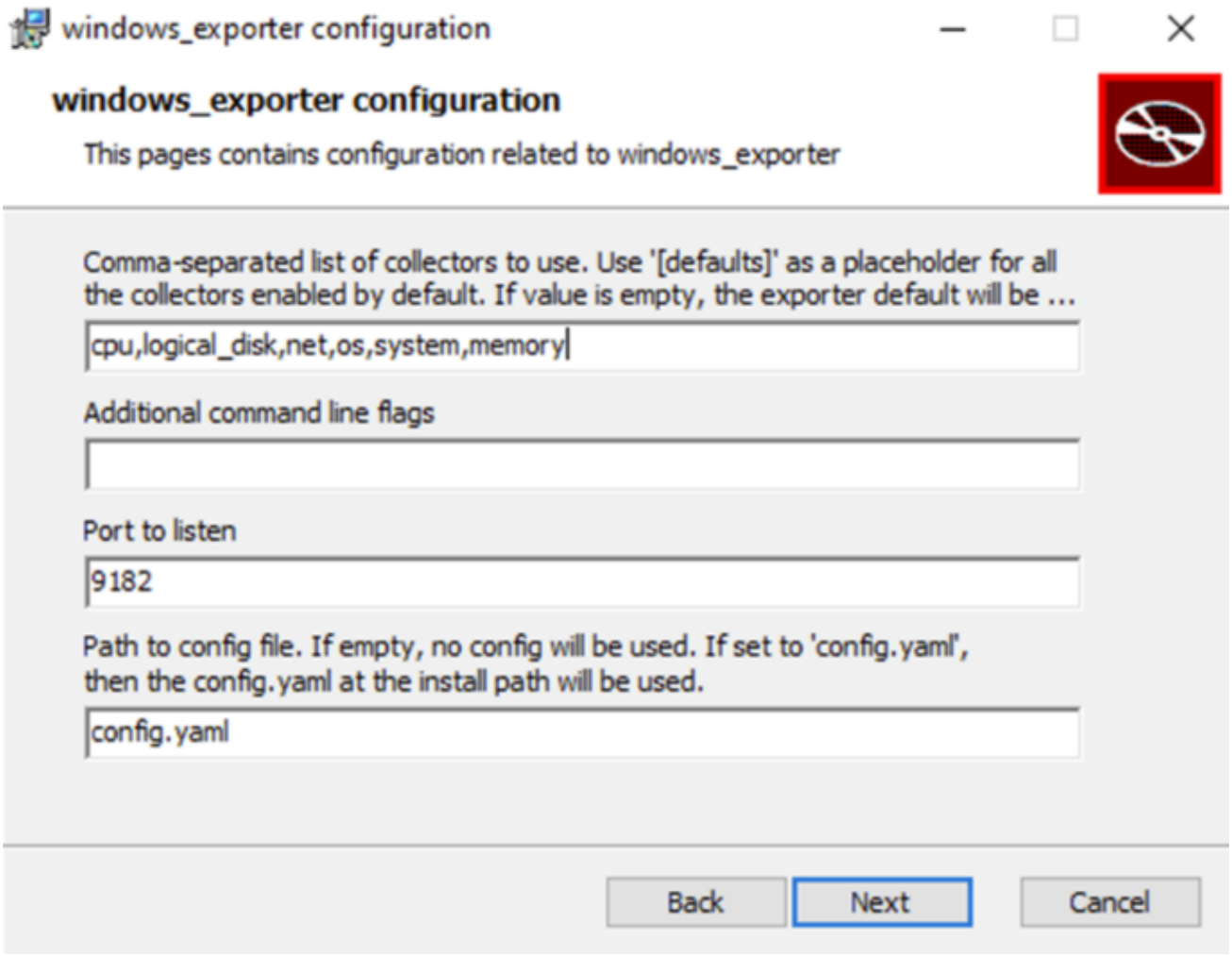
Все необходимые коллекторы для сбора метрик базовой контрольной панели включены по умолчанию. После запуска Node Exporter будет предоставлять метрики на конечной точке `/metrics` через порт 9100.

Настройка Windows Exporter

В ОС Windows для сбора различных системных метрик вроде загрузки ЦП, использования памяти и сетевой статистики можно использовать специальный инструмент — Windows Exporter.

Windows Exporter распространяется в виде .msi-установщика; скачайте актуальную версию и установите.

При установке укажите необходимые для работы коллекторы (через запятую): `cpu`, `logical_disk`, `net`, `os`, `system`, `memory` и укажите порт (по умолчанию 9182):



После установки Windows Exporter будет предоставлять метрики на конечной точке `/metrics` через порт 9182.

Настройка Prometheus для сбора метрик

Добавьте параметры метрик в Prometheus. Например, при использовании ОС Linux:

```
scrape_configs:
  - job_name: 'cb-otel-collector'
    static_configs:
      - targets: ['otel-collector:8889']
    metrics_path: '/metrics'

  - job_name: 'cb-otel-collector-internal-telemetry'
    static_configs:
      - targets: ['otel-collector:8888']
    metrics_path: '/metrics'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  - job_name: 'cb-node-exporter'
    static_configs:
      - targets: ['node-exporter:9100']
    metrics_path: '/metrics'
```

При использовании ОС Windows вместо `cb-node-exporter` укажите `cb-windows-exporter` с соответствующим портом 9182:

```
scrape_configs:
  - job_name: 'windows-node-exporter'
    static_configs:
      - targets: ['windows-exporter:9182']
    metrics_path: '/metrics'
```

Важно

Значения `otel-collector`, `node-exporter` и `windows-exporter` необходимо заменить на действительные IP-адреса.

Перезапустите Prometheus:

```
# systemctl reload prometheus
```

В результате Prometheus будет собирать все необходимые метрики.

Настройка Grafana Loki в качестве источника данных

Настройка Grafana Loki в качестве источника данных состоит из двух шагов:

1. Настройка OpenTelemetry Collector для экспорта записей журналов в Grafana Loki.
2. Настройка Grafana Loki для корректного приёма записей журналов от OpenTelemetry Collector.

Настройка OpenTelemetry Collector для экспорта записей журналов в Grafana Loki

Настройка для Grafana Loki без аутентификации

1. Откройте конфигурационный файл `config.yml`:
   - в ОС Linux: `/usr/lib/Acronis/OpenTelemetryCollector/config.yml`;

- в ОС Windows: `C:\Program Files\Acronis\OpenTelemetryCollector\config.yml`.

2. Добавьте OTLP-экспортер для Grafana Loki в раздел `exporters`:

```
exporters:
  otlphttp/loki:
    endpoint: http://<loki-addr>/otlp
```

Где `http://<loki-addr>/otlp` URL-адрес Grafana Loki.

3. Включите OTLP-экспортер в раздел `service.pipelines`:

```
service:
  pipelines:
    logs:
      receivers: [..., filelog/task-manager, filelog/alert-manager]
      processors: [..., batch, memory_limiter, resource]
      exporters: [..., otlphttp/loki]
```

Важно

В строке `receivers` необходимо добавить `filelog/task-manager` и `filelog/alert-manager`.

В строке `processors` необходимо добавить `batch`, `memory_limiter` и `resource`.

Перезапустите службу сервера управления Кибер Бэкап.

Настройка для Grafana Loki с аутентификацией

1. Откройте конфигурационный файл `config.yml`:
   - в ОС Linux: `/usr/lib/Acronis/OpenTelemetryCollector/config.yml`;
   - в ОС Windows: `C:\Program Files\Acronis\OpenTelemetryCollector\config.yml`.
2. Добавьте расширение `basicauth` в конфигурацию:

```
extensions:
  basicauth/otlp:
    client_auth:
      username: username
      password: password
```

3. Включите OTLP-экспортер с указанием расширения `basicauth` в раздел `exporters`:

```
exporters:
  otlphttp/loki:
    auth:
      authenticator: basicauth/otlp
    endpoint: http://<loki-addr>/otlp
```

Где `http://<loki-addr>/otlp` URL-адрес Grafana Loki.

4. Включите OTLP-экспортер в раздел `service.pipelines`:

```
service:
  extensions: [basicauth/otlp]
  pipelines:
    logs:
      receivers: [..., filelog/task-manager, filelog/alert-manager]
      processors: [..., batch, memory_limiter, resource]
      exporters: [..., otlphttp/loki]
```

Важно

В строке `receivers` необходимо добавить `filelog/task-manager` и `filelog/alert-manager`.

В строке `processors` необходимо добавить `batch`, `memory_limiter` и `resource`.

Перезапустите службу сервера управления Кибер Бэкап.

Настройка Grafana Loki для корректного приема записей журналов от OpenTelemetry Collector

Актуальные версии Loki поддерживают формат OpenTelemetry для приёма записей журналов. Для корректного приема записей журналов в Loki должна быть включена работа с структурированными метаданными (по умолчанию включено в Loki 3.0 и более поздних версиях).

Установите параметр `allow_structured_metadata` в значение `true` в конфигурационном файле Loki:

```
limits_config:
  allow_structured_metadata: true
```

Настройка системы мониторинга Grafana

Для корректной работы системы мониторинга Grafana с Кибер Бэкап необходимо выполнить следующие действия:

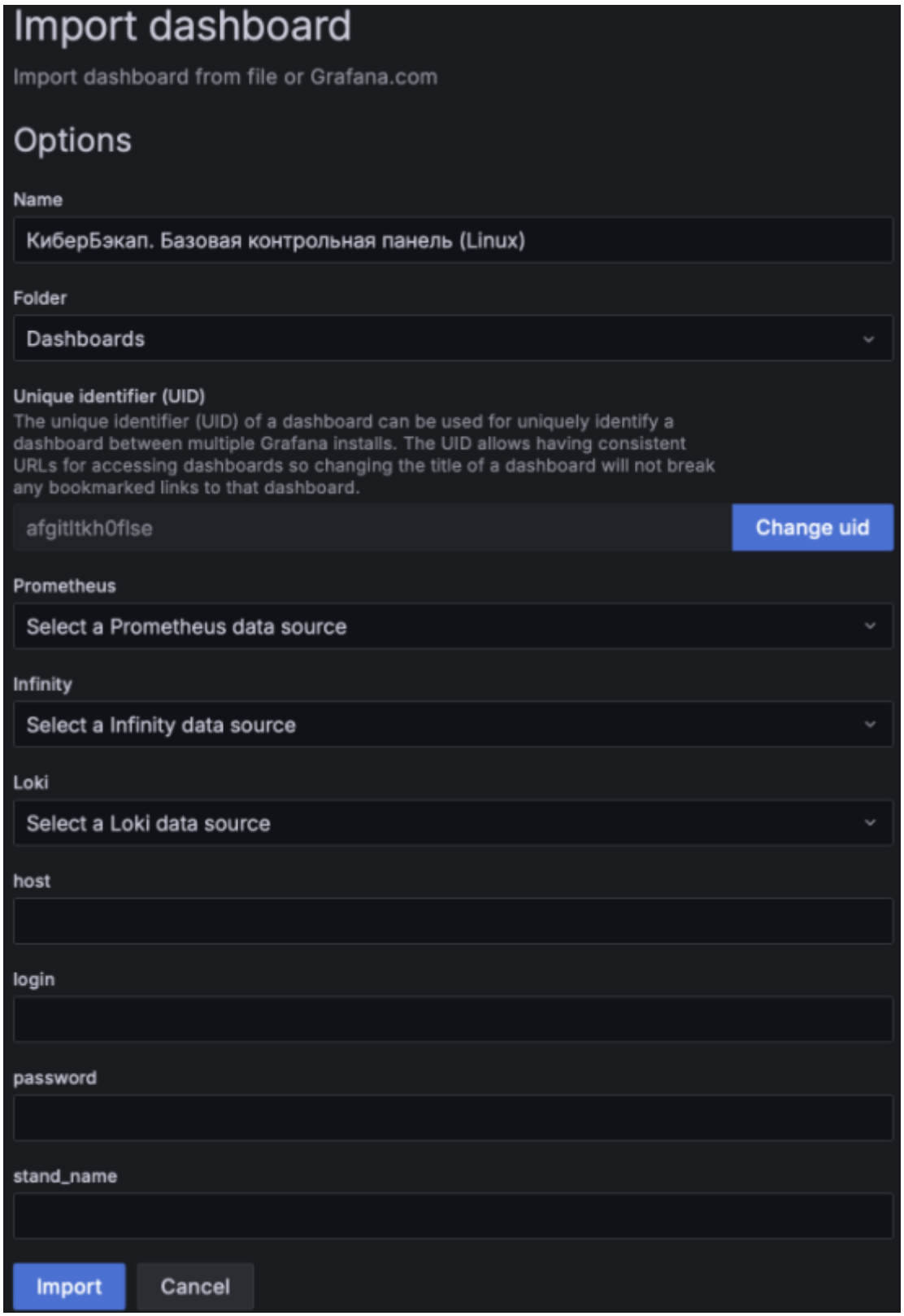
1. Установить плагин Infinity (скачайте плагин с официального сайта).
2. Создать и настроить источники данных для панели мониторинга.
3. Произвести импорт и настройку панели мониторинга.

Создание и настройка источников данных для панели мониторинга

- Создайте источник данных Infinity. Для создания обратитесь к документации разработчика.
- Создайте источник данных Prometheus (см. раздел *Настройка Prometheus в качестве источника данных*).
- Создайте источник данных Grafana Loki и подключите его к экземпляру Grafana Loki (см. раздел *Настройка Grafana Loki в качестве источника данных*).

Импорт и настройка панели мониторинга

1. Скачайте файл с панелью мониторинга в зависимости от ОС, на которой работает сервер управления Кибер Бэкап, из статьи базы знаний.
2. Импортируйте панель мониторинга в платформу Grafana с помощью стандартного механизма платформы.
3. Заполните поля меню импорта.



- **Name**. Укажите наименование панели мониторинга.
- **Folder**. Укажите папку, в которую будет импортирована панель мониторинга.
- **Prometheus**. Выберите из выпадающего списка источник данных, связанный с вашим

экземпляром Prometheus.

- **Infinity**. Выберите из выпадающего списка источник данных Infinity.
- **Loki**. Выберите из выпадающего списка источник данных, связанный с вашим экземпляром Grafana Loki.
- **host**. Укажите адрес и порт веб-консоли Кибер Бэкап. Например, `http://host:9877`
- **login**. Укажите имя учетной записи с ролью **Оператор мониторинга** (см. раздел *Отделы и административные учетные записи*.)
- **password**. Укажите пароль от учетной записи с ролью **Оператор мониторинга**.
- **stand_name**. Введите значение атрибута `ru.cyberprotect.cb.stand.name`, указанное при настройке данных телеметрии (см. подраздел ”Настройка данных телеметрии” в разделе *Настройка внешнего мониторинга*).

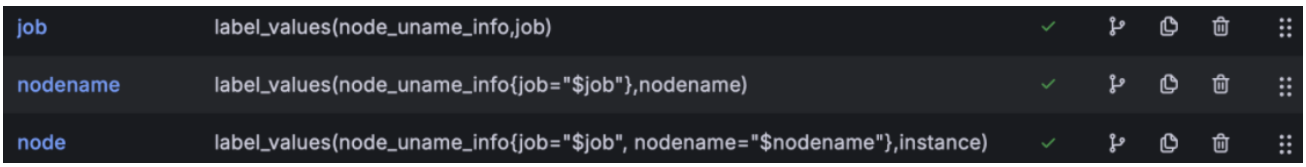
> **Примечание**
>
> Названия полей могут отличаться в зависимости от используемой версии платформы Grafana.

Настройка панелей платформы Grafana

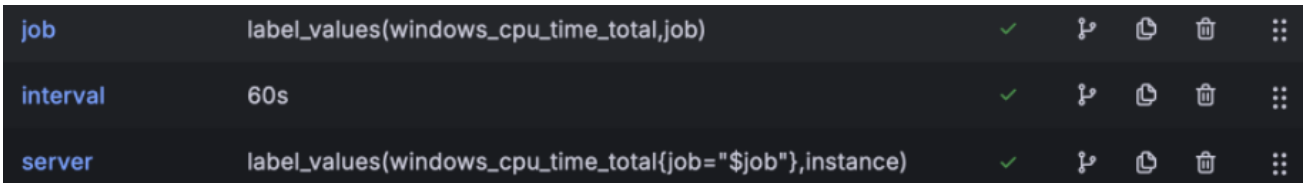
Настройка системных панелей

Системные панели используют метрики, полученные из Node Exporter или Windows Exporter. Метрики Node Exporter отличаются от метрик Windows Exporter, поэтому для PromQL-запросов используются разные переменные.

Для ОС Linux используются переменные `job`, `nodename` и `node`.



Для ОС Windows используются переменные `job`, `interval` и `server`.

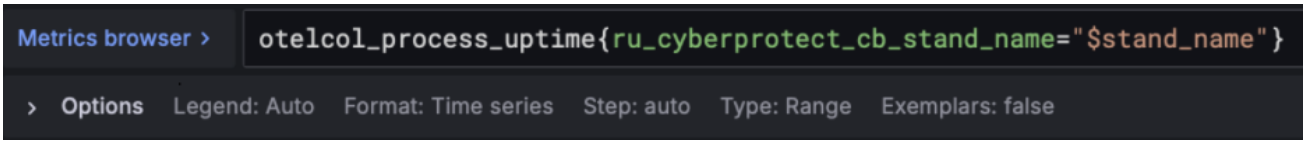


При необходимости измените значения переменных.

Настройка панели с временем доступности

Панель времени доступности отображает время работы сервера управления Кибер Бэкап.

По умолчанию панель использует метрику `otelcol_process_uptime`, ассоциированную со значением атрибута `ru.cyberprotect.cb.stand.name`, которое было указано при настройке данных телеметрии (см. подраздел ”Настройка данных телеметрии” в разделе *Настройка внешнего мониторинга*).



Настройка панелей с журналами

Для работы с журналами используется атрибут `ru.cyberprotect.cb.stand.name`, которой был указан при настройке данных телеметрии (см. подраздел ”Настройка данных телеметрии” в разделе *Настройка внешнего мониторинга*).

Для корректной работы панели в Grafana Loki должна быть включена работа с структурированными метаданными.

Внешний мониторинг средствами Zabbix

Кибер Бэкап позволяет настроить интеграцию с системой внешнего мониторинга Zabbix версий 6.0 — 8.0.

Настройка состоит из следующих шагов:

1. Создание учётной записи администратора с ролью **Оператор мониторинга** (см. раздел *Отделы и административные учетные записи*).
2. Импорт и настройка шаблонов (см. далее в этом разделе).
3. Назначение шаблона хосту (см. далее в этом разделе).

По завершении настройки интеграции Кибер Бэкап с Zabbix доступен просмотр панели мониторинга (см. далее в этом разделе).

Импорт и настройка шаблонов

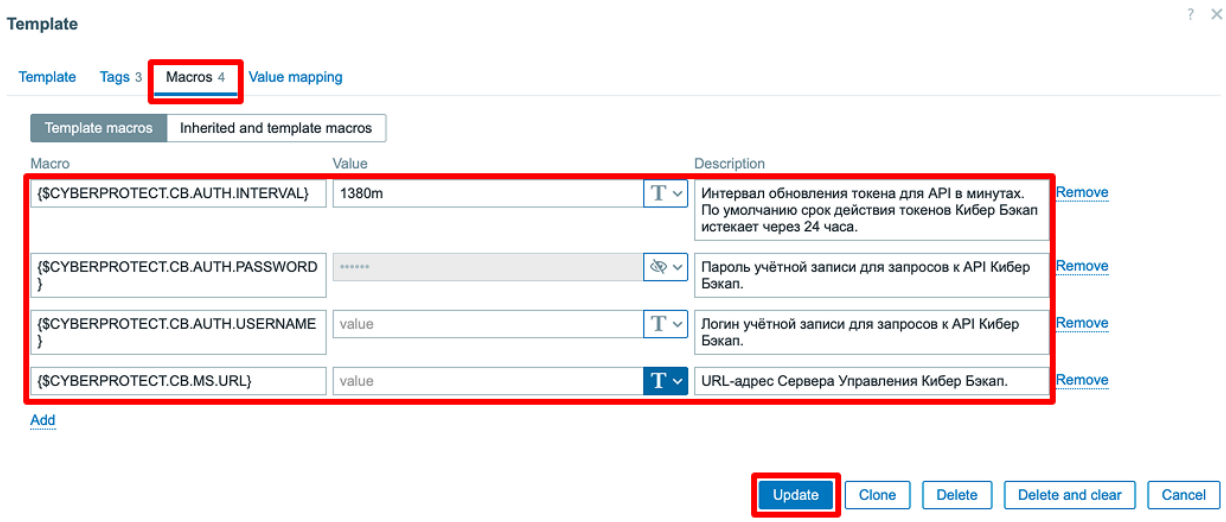
Чтобы импортировать и настроить шаблоны, выполните следующие действия:

1. Скачайте файл с шаблонами в формате YAML.
2. Импортируйте скачанный файл в Zabbix. После успешной загрузки в веб-интерфейсе Zabbix появятся новые шаблоны:

- **Cyberprotect Cyber Backup by HTTP**;
- **Cyberprotect Cyber Backup MS by HTTP**.

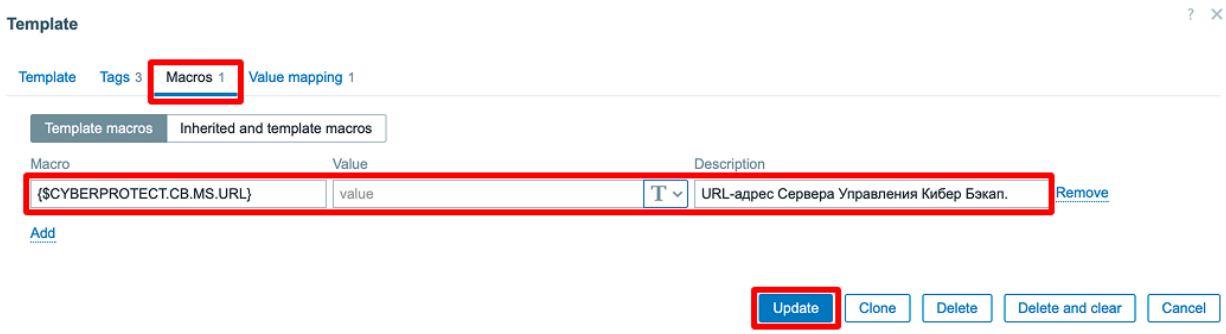


3. Для сбора метрик от хоста сервера управления Кибер Бэкап выполните следующие действия:
    1. Установите Zabbix Agent на машину сервера управления Кибер Бэкап, если он ещё не установлен, и настройте его подключение к серверу Zabbix.
    2. Скачайте и импортируйте базовый шаблон Zabbix, соответствующий используемой операционной системе (ОС) и версии Zabbix:
        - Linux by Zabbix agent — если сервер управления Кибер Бэкап работает на базе ОС Linux;
        - Windows by Zabbix agent — если сервер управления Кибер Бэкап работает на базе ОС Windows.
4. Откройте шаблон **Cyberprotect Cyber Backup by HTTP** и перейдите на вкладку **Macros** в веб-интерфейсе Zabbix.
5. Укажите значения для следующих макросов (их описание также приведено в поле **Description** веб-интерфейса Zabbix):
    - **{$CYBERPROTECT.CB.AUTH.USERNAME}** — имя учётной записи для API-запросов Кибер Бэкап.
    - **{$CYBERPROTECT.CB.AUTH.PASSWORD}** — пароль учётной записи для API-запросов Кибер Бэкап.
    - **{$CYBERPROTECT.CB.MS.URL}** — URL-адрес сервера управления Кибер Бэкап.
    - [Необязательно] **{$CYBERPROTECT.CB.AUTH.INTERVAL}** — частота обновления токена авторизации (значение по умолчанию — 24 часа). При необходимости укажите новое значение.
6. Нажмите **Update**.

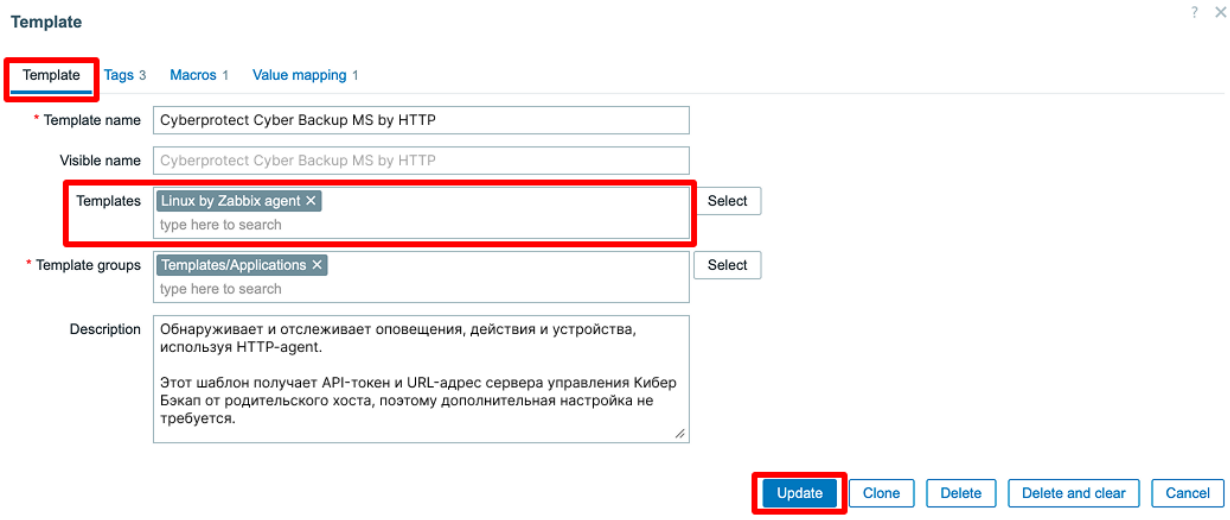


7. Откройте шаблон **Cyberprotect Cyber Backup MS by HTTP** и перейдите на вкладку **Macros** в веб-интерфейсе Zabbix.

8. Укажите значение для макроса **{$CYBERPROTECT.CB.MS.URL}** и нажмите **Update**.

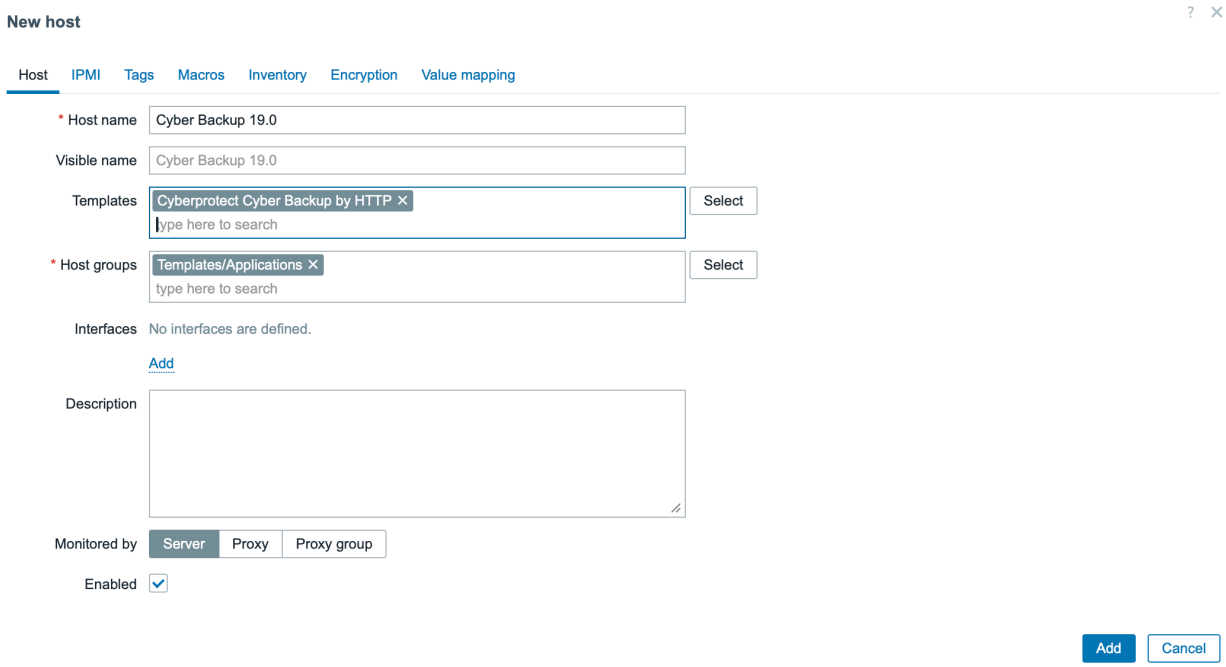


9. В шаблоне **Cyberprotect Cyber Backup MS by HTTP** перейдите на вкладку **Template** и добавьте ранее импортированный шаблон **Linux by Zabbix agent** или **Windows by Zabbix agent** в поле **Templates**, после этого нажмите **Update**.



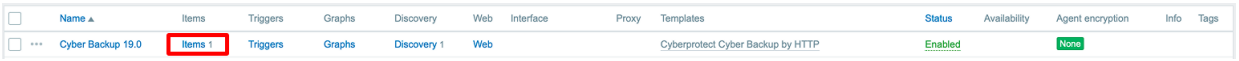
Назначение шаблона хосту

1. Назначьте импортированный ранее шаблон **Cyberprotect Cyber Backup by HTTP** хосту Кибер Бэкап в Zabbix. Если хост не существует, создайте его.

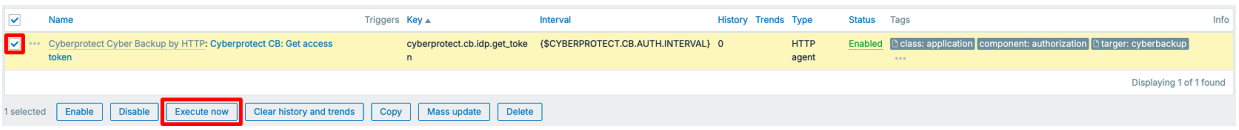


> **Примечание**
>
> При добавлении шаблонов **Linux by Zabbix Agent** или **Windows by Zabbix Agent** в шаблон **Cyberprotect Cyber Backup MS by HTTP** для работы Zabbix Agent в режиме пассивных проверок (passive checks) требуется обязательное добавление интерфейса агента. Для этого в строке **Interfaces** нажмите **Add** → **Agent** и укажите IP-адрес машины сервера управления Кибер Бэкап. Без настройки данного интерфейса сбор метрик ОС выполняться не будет.

2. Запустите правило низкоуровневого обнаружения (LLD), нажав **Items** в строке хоста. Данная процедура выполняется только один раз.



3. Отметьте флажком элемент **Cyberprotect CB: Get access token** и нажмите **Execute now**.



По истечении 10—15 секунд в списке отобразится новый хост.

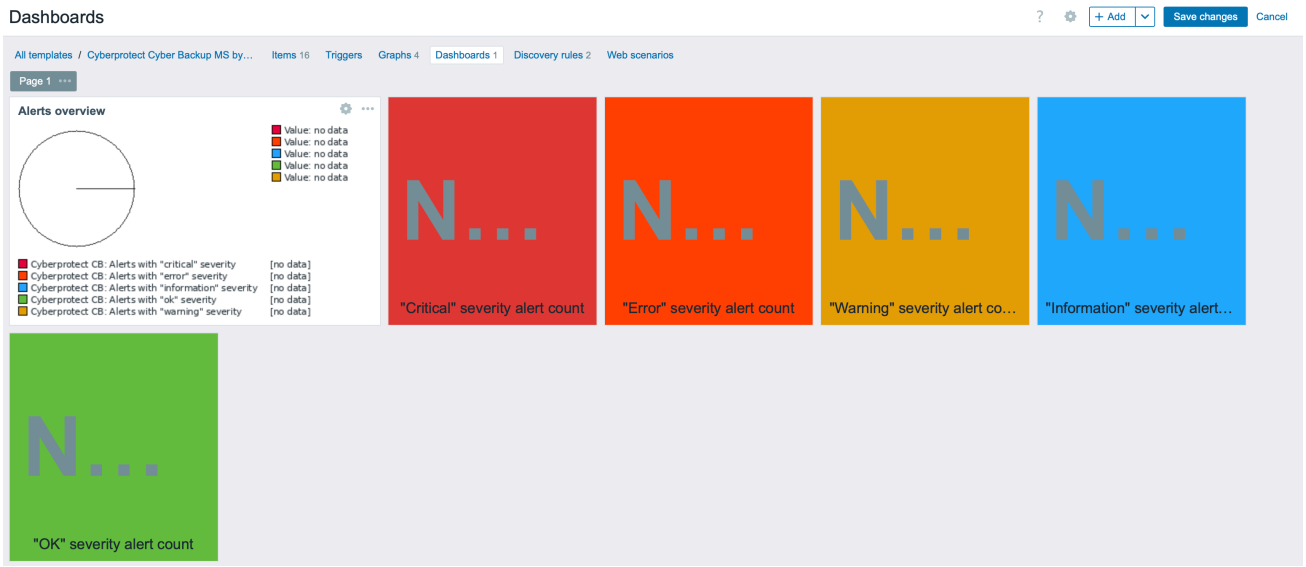


Примечание

Запуск правила низкоуровневого обнаружения зависит от частоты обновления токена авторизации. Частота обновления задаётся макросом **{$CYBERPROTECT.CB.AUTH.INTERVAL}**.

Просмотр панели мониторинга

Шаблон **Cyberprotect Cyber Backup MS by HTTP** поставляется с панелью мониторинга.



При привязке шаблона **Cyberprotect Cyber Backup by HTTP** к хосту автоматически создаётся панель мониторинга, ассоциированная с данным хостом и отображающая его метрики.

Для просмотра панели мониторинга хоста выполните следующие действия:

1. В веб-интерфейсе Zabbix перейдите в раздел **Monitoring** → **Hosts**.
2. Нажмите на имя созданного хоста.
3. В открывшемся контекстном меню выберите **Dashboards**.

Ленточные устройства

Лента — носитель (картридж с магнитной лентой) для записи и хранения данных.

Чистящая лента — лента, предназначенная для технического обслуживания ленточных приводов.

Ленточное устройство — общий термин, обозначающий оборудование для работы с лентами. Включает как ленточные библиотеки, так и автономные ленточные приводы.

Ленточный привод — устройство чтения данных с лент и записи данных на ленты.

Ленточная библиотека — автоматизированная система хранения данных большой емкости, содержащая следующие компоненты:

- множество слотов хранения для размещения лент;
- один или несколько ленточных приводов;
- механизм для автоматического перемещения лент между слотами и приводами.

Библиотека может содержать и другие компоненты, например, устройства чтения штрихкодов или принтеры штрихкодов.

В следующих разделах описано использование ленточных устройств для хранения резервных копий.

Типы и свойства лент

Кибер Бэкап поддерживает следующие известные типы носителей:

- перезаписываемые ленты;
- ленты типа WORM (write-once-read-many — однократная запись, множественное чтение);
- чистящие ленты.

Кроме того, Кибер Бэкап поддерживает работу с лентами, которые не удалось отнести ни к одному из известных типов (см. далее подраздел ”Ленты неизвестного типа”).

Кибер Бэкап обеспечивает совместимость со многими ленточными устройствами. По вопросам поддержки конкретного оборудования см. соответствующую документацию.

Перезаписываемые ленты

Перезаписываемые ленты являются основным типом ленточных носителей в Кибер Бэкап для резервного копирования. Используйте их для хранения информации, которую предполагается перезаписывать.

Особенности перезаписываемых лент:

- неограниченное количество циклов записи;
- используются по умолчанию для резервного копирования;
- могут иметь аппаратную защиту от записи.

Перезаписываемые ленты используются по умолчанию для автоматического пополнения пользовательских пулов.

Ленты типа WORM

Ленты этого типа предназначены для записи неизменяемых архивов. Используйте эти ленты для хранения резервных копий, которые не будут меняться в течение всего срока хранения.

Кибер Бэкап поддерживает запись данных на пустые и на частично заполненные WORM-ленты. При этом операции перезаписи и стирания данных будут предотвращаться.

Для лент WORM предусмотрено автоматическое пополнение пользовательских пулов. Для его включения в существующем пуле перейдите в **Настройки** → **Управление лентами** → **Пулы лент** → **Пользовательский пул** → **Правка пула** и отметьте флажком пункт **Носителями однократной записи (тип WORM)**.

Важно

Данные, записанные на WORM-ленты, нельзя будет впоследствии перезаписать или стереть.

Использование WORM-носителей для архивного хранения

Для архивного хранения на WORM-лентах *создайте* отдельный пул. Используйте этот пул для создания неизменяемых архивов. Включите для этого пула автоматическое пополнение WORM-лентами или перенесите их в него вручную.

Создайте план защиты для WORM-лент. При его выполнении автоматически будет выбрана WORM-лента с доступным местом.

При необходимости WORM-ленты будут автоматически добавляться из пула **Свободные ленты**.

Примечание

При назначении плана защиты убедитесь, что в библиотеке достаточно пустых WORM-лент.

Аппаратная защита от записи

Перезаписываемые ленты и ленты WORM оснащены аппаратной защиты от записи.

С включенной защитой на ленте невозможно выполнять следующие действия:

- записывать и перезаписывать данные;
- стирать существующие данные.

Важно

Физическое положение переключателя защиты от записи имеет приоритет по отношению к настройкам программы.

При расхождении данных о положении переключателя с данными программы выполните *инвентаризацию*.

Чистящие ленты

Эти специальные ленты предназначены для профилактической очистки ленточных приводов.

Особенности чистящих лент:

- автоматически определяются и остаются в пуле **Нераспознанные ленты**;
- имеют ограниченный ресурс (до 50 циклов очистки);
- не могут использоваться для хранения данных;
- не перемещаются в другие пулы.

Оставшийся ресурс каждой ленты автоматически отслеживается после каждой процедуры очистки.

Ленты неизвестного типа

Этот статус лента получает в том случае, если в результате *инвентаризации* Кибер Бэкап не удается автоматически установить ее тип. При этом такие ленты все равно можно использовать для операций резервного копирования.

По умолчанию в Кибер Бэкап ленты неизвестного типа обрабатываются как перезаписываемые.

При каждом взаимодействии с такой лентой будет вновь автоматически выполняться попытка идентификации.

Ленты этого типа можно размещать в пользовательских пулах и автоматически пополнять ими эти пулы.

Поддержка резервного копирования на ленту

Агенты защиты могут выполнять резервное копирование данных на ленточное устройство напрямую или через узел хранения. В любом случае обеспечивается полностью автоматическая работа ленточного устройства. Если ленточное устройство с несколькими накопителями подключено к узлу хранения, несколько агентов могут одновременно выполнять резервное копирование на магнитные ленты.

Важно

Для корректной работы необходимо, чтобы доступ к ленточным устройствам и управление ими осуществлялись только через продукт Кибер Бэкап. Любые действия, выполняемые в обход продукта, могут привести к ошибкам.

Совместимость с RSM и программным обеспечением других поставщиков

Сосуществование с программным обеспечением других поставщиков

Невозможно работать с лентами на машине, на которой установлено программное обеспечение других поставщиков с фирменными средствами управления лентами. Для использования лент на таких машинах необходимо удалить или отключить программное обеспечение других поставщиков.

Взаимодействие с диспетчером съемных носителей Windows (RSM)

Агенты защиты и узлы хранения не используют RSM. При *обнаружении ленточного устройства* они отключают устройство от RSM (если они не используются другим программным обеспечением). Чтобы работать с ленточным устройством, убедитесь, что устройство не включается в RSM ни пользователями, ни программным обеспечением других поставщиков. Если ленточное устройство включено в RSM, повторите процедуру распознавания ленточного устройства.

Поддерживаемое оборудование

Кибер Бэкап поддерживает внешние устройства SCSI. Это устройства, подключаемые к Fibre Channel или с помощью интерфейсов SCSI, iSCSI, Serial Attached SCSI (SAS). Кроме того, Кибер Бэкап поддерживает ленточные устройства, подключенные через USB.

В ОС Windows Кибер Бэкап может выполнять резервное копирование на ленточное устройство, даже если не установлены драйверы для соответствующего устройства смены носителей. Такое ленточное устройство отображается в диспетчере устройств как неизвестный сменщик носителей. Однако драйверы для накопителей устройства должны быть установлены. В Linux и при загрузке с носителя резервное копирование на ленточное устройство без драйверов невозможно.

Распознавание устройств, подключенных к IDE или SATA, не гарантируется. Это зависит от того, установлены ли в операционной системе необходимые драйверы.

Чтобы узнать, поддерживается ли то или иное устройство, используйте инструмент совместимости оборудования. Можно отправить отчет с результатами теста в Киберпротект.

База данных управления лентами

Информация обо всех ленточных устройствах, подключенных к машине, хранится в базе метаданных управления лентами. Путь к базе данных по умолчанию:

- В ОС Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database**.
- В ОС Linux: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**.

Размер базы данных зависит от количества резервных копий, которые хранятся на ленточных носителях, и приблизительно равен 10 МБ на каждые сто резервных копий. База данных может быть больше, если библиотека ленточных носителей содержит тысячи резервных копий. В таком случае, возможно, потребуется сохранить базу данных ленточных носителей на другом томе.

База данных также хранит:

- Информацию о чистящих носителях и их местоположении;
- Счетчики использованных и оставшихся циклов очистки;
- Историю выполненных операций очистки.

Как изменить расположение базы данных в Windows

1. Остановите службу `MMS`.

   Если ленточные носители подключены к узлу хранения, остановите службу `storagenode`.
2. Переместите файлы из расположения по умолчанию в новое расположение.
3. В реестре найдите ключ `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`.
4. Укажите новый путь к каталогу в значении реестра `ArsmDmlDbProtocol`. Строка может содержать до 32765 символов.
5. Запустите службу `MMS` или `storagenode`.

Как изменить расположение базы данных в Linux

1. Остановите службу `acronis_mms`.

   Если ленточные носители подключены к узлу хранения, остановите службу `storageserver`.

2. Переместите файлы из расположения по умолчанию в новое расположение.
3. Откройте файл конфигурации `/etc/Acronis/ARSM.config` в текстовом редакторе.
4. Найдите строку `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Измените путь под этой строкой.
6. Сохраните файл.
7. Запустите службу `acronis_mms` или `storageserver`.

Параметры записи на ленты

Параметры записи на ленту (размер блока данных и размер кэша) позволяют выполнить тонкую настройку программного обеспечения для получения максимальной производительности. Для записи на ленту требуются оба параметра, но обычно необходимо настроить только размер блока данных. Оптимальное значение зависит от типа ленточного устройства и от данных, подлежащих резервному копированию, например, от количества файлов и их размера.

> **Примечание**
>
> Программа читает ленту блоками данных такого же размера, который использовался для записи данных на ленту. Если ленточное устройство не поддерживает этот размер блоков данных, чтение завершится сбоем.

Параметры заданы на каждой машине, к которой подключено ленточное устройство. Это может быть машина, на которой установлен агент или узел хранения. На машине под управлением Windows настройка выполняется в реестре. На машине Linux она выполняется в файле конфигурации `/etc/Acronis/BackupAndRecovery.config`.

В Windows создайте соответствующие разделы реестра и их значения DWORD. На машине Linux добавьте следующий текст в конце файла конфигурации непосредственно перед тегом `</registry>`:

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Tword">value</value>
     <value name="DefaultBlockSize" type="Tword">value</value>
</key>
```

DefaultBlockSize

Это размер блока данных (в байтах), используемый для записи на ленты.

Возможные значения: 65536, 131072, 262144, 524288, 1048576. Рекомендуемое значение: 65536 или 262144.

Если данное значение равно 0 или параметр отсутствует, размер блока данных определяется следующим образом:

- В Windows данное значение принимается от драйвера ленточного устройства.
- В Linux данное значение составляет 64 КБ.

Раздел реестра (на машине под управлением Windows): `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize`.

Строка в файле `/etc/Acronis/BackupAndRecovery.config` (на машине под управлением Linux):

```
<value name="DefaultBlockSize" type="Tword">value</value>
```

Если указанное значение не принимается ленточным устройством, то программа делит его на два до тех пор, пока не будет достигнуто приемлемое значение или значение 32 байта. Если приемлемое значение не найдено, то программа умножает указанное значение на два до тех пор, пока не будет достигнуто приемлемое значение или значение 1 МБ. Если ни одно значение не принимается диском, резервное копирование завершится сбоем.

WriteCacheSize

Это размер буфера (в байтах), используемый для записи на ленты.

Возможные значения: 65536, 131072, 262144, 524288, 1048576, но не меньше значения параметра `DefaultBlockSize`. Рекомендуемое значение: 4 * DefaultBlockSize.

Если значение составляет 0 или данный параметр отсутствует, размер буфера составляет 1 МБ. Если операционная система не поддерживает это значение, то программа делит его на два до тех пор, пока не будет достигнуто приемлемое значение или значение параметра `DefaultBlockSize`. Если значение, поддерживаемое операционной системой, не найдено, резервное копирование завершится сбоем.

Раздел реестра (на машине под управлением Windows): `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize`

Строка в файле /etc/Acronis/BackupAndRecovery.config (на машине под управлением Linux):

```
<value name="WriteCacheSize" type="Tword">value</value>
```

Если указать ненулевое значение, которое не поддерживается операционной системой, резервное копирование завершится сбоем.

Связанные с лентой параметры резервного копирования

Настраиваемые параметры резервного копирования *Управление лентами* позволяют определить следующие возможности.

- Следует ли включить восстановление файлов из образов дисков на лентах.
- Следует ли возвращать ленты в слот после выполнения плана защиты.
- Следует ли извлекать ленты после завершения резервного копирования.
- Следует ли использовать свободную ленту для каждой резервной копии.
- Следует ли перезаписывать данные на ленте при создании полной резервной копии (только для изолированных ленточных устройств).
- Следует ли использовать наборы лент для различения использованных лент, например, для резервных копий, созданных в разные дни недели или для резервных копий разных типов машин.

Параллельные операции

Кибер Бэкап может одновременно выполнять операции с различными компонентами ленточного устройства. В ходе операции с накопителем (резервное копирование, восстановление, *повторное сканирование* или *стирание*) можно запустить операцию, в которой используется устройство смены носителей (*перемещение* ленты в другой слот или *извлечение* ленты), и наоборот. Если в библиотеке ленточных носителей больше одного накопителя, можно запустить операцию с одним накопителем во время операции с другим. Например, несколько машин могут одновременно выполнять резервное копирование или восстановление, используя разные устройства одной и той же библиотеки ленточных носителей.

Операция *обнаружения новых ленточных устройств* может выполняться одновременно с любой другой операцией. Во время *инвентаризации* недоступны никакие другие операции, кроме обнаружения новых ленточных устройств.

Очистка привода может выполняться параллельно с операциями на других приводах. Очищаемый привод блокируется на время операции (обычно 2-5 минут).

Операции, которые нельзя выполнить параллельно, помещаются в очередь.

Ограничения

Существуют следующие ограничения использования ленточных устройств:

1. Резервное копирование и репликация резервных копий почтовых ящиков Microsoft Exchange на ленты не поддерживаются.
2. Невозможно выполнить резервное копирование физических и виртуальных машин с поддержкой приложений.
3. Консолидация резервных копий на лентах невозможна. В результате схема резервного копирования **Всегда инкрементное** недоступна при резервном копировании на ленты.
4. Дедупликация резервных копий на лентах невозможна.
5. Кибер Бэкап не может автоматически перезаписать ленту с резервными копиями, которые не удалены, а также в тех случаях, когда на других лентах есть зависимые резервные копии.
6. Резервное копирование невозможно, если требуется очистка привода. Используйте операцию ”Очистка привода” для профилактического обслуживания в промежутках между резервным копированием.
7. Чистящие носители не могут быть использованы для операций с данными и не могут быть перемещены из пула **Нераспознанные ленты**.
8. Восстановление из резервной копии на ленте под управлением операционной системы невозможно, если это восстановление требует перезагрузки операционной системы. Для такого восстановления используйте загрузочный носитель.
9. Можно *проверить* любые резервные копии на лентах, однако выбрать для проверки целое хранилище на ленте или ленточное устройство невозможно.
10. Управляемое хранилище на лентах невозможно защитить паролем. Вместо этого защитите паролем резервные копии.
11. При репликации резервных копий на ленты не поддерживается мультиплексирование (см. *Управление лентами*).
12. Устройства, использующие протокол NDMP (Network Data Management Protocol), не поддерживаются.
13. Принтеры штрихкодов не поддерживаются.
14. Ленты, форматированные в файловую систему Linear Tape File System (LTFS), не поддерживаются.
15. Если при резервном копировании на ленте заканчивается свободное место, продолжить копирование можно только на пустую ленту.

16. Резервное копирование на какой-либо из накопителей ленточной библиотеки невозможно, если требуется очистка данного накопителя или очистка уже выполняется.

    Для успешного выполнения операций резервного копирования рекомендуется регулярно выполнять очистку накопителей ленточной библиотеки в промежутках между операциями.

17. Не рекомендуется использовать в ленточных библиотеках кассеты без бар-кодов. Использование таких кассет может приводить к сбоям.

Начало работы с ленточным устройством

Резервное копирование машины на локально подключенное ленточное устройство

Предварительные требования

- Ленточное устройство должно быть подключено к машине в соответствии с инструкциями производителя.
- На машине установлен агент защиты.

Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите в веб-консоль Кибер Бэкап.
3. В разделе **Настройки** → **Управление лентами** разверните узел машины и щёлкните **Ленточные устройства**.
4. Убедитесь, что отображается подключенное ленточное устройство. Если нет, нажмите кнопку **Поиск устройств**.
5. Проведите инвентаризацию лент:
    1. Щёлкните имя ленточного устройства.
    2. Щёлкните **Инвентаризация** для обнаружения загруженных лент. Оставьте включенным параметр **Полная инвентаризация**. Не включайте функцию **Перенести нераспознанные или импортированные ленты в пул "Свободные ленты"**. Щёлкните **Начать инвентаризацию сейчас**.

        Результат: загруженные ленты перенесены в соответствующие пулы, как указано в разделе *Инвентаризация*.

> **Примечание**
>
> Полная инвентаризация всего ленточного устройства может занять длительное время.

3. Если загруженные ленты перенесены в пул **Нераспознанные ленты** или **Импортированные ленты**, но требуются для резервного копирования, *переместите* такие ленты в пул **Свободные ленты** вручную.

> **Примечание**
>
> Ленты, отправленные в пул **Импортированные ленты**, содержат резервные копии, записанные ПО Кибер Бэкап. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.

Резервное копирование

Создайте план защиты, как описано в разделе *Резервное копирование*. Затем укажите хранилище резервных копий, щёлкнув **Пул лент**.

Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Хранилища резервных копий** → **Пул лент**.
- Ленты с резервными копиями будут перемещены в пул.

Резервное копирование на ленточное устройство, подключенное к узлу хранения

Предварительные требования

- Узел хранения должен быть зарегистрирован на сервере управления.
- Ленточное устройство должно быть подключено к узлу хранения в соответствии с инструкциями производителя.

Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите в веб-консоль Кибер Бэкап.

3. Щёлкните **Настройки** → **Управление лентами**, разверните узел с именем узла хранения и щёлкните **Ленточные устройства**.
4. Убедитесь, что отображается подключенное ленточное устройство. Если нет, нажмите кнопку **Поиск устройств**.
5. Проведите инвентаризацию лент:
    1. Щёлкните имя ленточного устройства.
    2. Щёлкните **Инвентаризация** для обнаружения загруженных лент. Оставьте включенным параметр **Полная инвентаризация**. Не включайте функцию **Переместить нераспознанные или импортированные пулы лент в пул "Свободные ленты"**. Щёлкните **Начать инвентаризацию сейчас**.

        Результат: загруженные ленты перенесены в соответствующие пулы, как указано в разделе *Инвентаризация*.

        > **Примечание**
        >
        > Полная инвентаризация всего ленточного устройства может занять длительное время.

    3. Если загруженные ленты перенесены в пул **Нераспознанные ленты** или **Импортированные ленты**, но требуются для резервного копирования, *переместите* такие ленты в пул **Свободные ленты** вручную.

        > **Примечание**
        >
        > Ленты, отправленные в пул **Импортированные ленты**, содержат резервные копии, записанные ПО Кибер Бэкап. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.

    4. Определите, что требуется сделать: выполнить резервное копирование в *пул* или *создать новый пул*.

        Наличие нескольких пулов позволяет использовать отдельный набор лент для каждой машины или каждого отдела компании.

    5. Если выбранный пул может, при необходимости, принимать ленты из пула **Свободные ленты**, пропустите этот шаг.

        В противном случае перенесите ленты из пула **Свободные ленты** в выбранный пул.

> **Примечание**
>
> Чтобы узнать, может ли пул принимать ленты из пула **Свободные ленты**, щёлкните пул, а затем щёлкните **Правка пула**.

Резервное копирование

Создайте план защиты, как описано в разделе *Резервное копирование*. При указании хранилища резервных копий выберите пул лент.

Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Хранилища резервных копий**, затем выберите пул лент.
- После завершения резервного копирования ленты с резервными копиями будут перемещены в выбранный пул.

Советы по дальнейшему использованию библиотеки ленточных носителей

- Полная инвентаризация не требуется каждый раз, когда загружается новая лента. Для экономии времени используйте процедуру, описанную в разделе *Инвентаризация*, подраздел ”Сочетание быстрой и полной инвентаризации”.
- В той же библиотеке ленточных носителей можно создать другие пулы и выбрать любой из них в качестве места сохранения резервных копий.

Восстановление с ленточного устройства из операционной системы

Как выполнить восстановление с ленточного устройства из операционной системы

1. Войдите в веб-консоль Кибер Бэкап.
2. Нажмите **Устройства** и выберите машину, для которой есть резервная копия.
3. Щёлкните **Восстановление**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Данное ПО отобразит список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.

6. *Настройте* другие параметры восстановления.
7. Нажмите **Запуск восстановления**, чтобы запустить операцию восстановления.
8. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    1. Загрузите ленту.
    2. Выполните быструю *инвентаризацию*.
    3. Нажмите **Панель мониторинга** → **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
    4. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

Если не отображаются резервные копии, хранящиеся на лентах

Это может означать, что база данных с содержимым лент не найдена или повреждена.

Для восстановления базы данных выполните следующие действия.

1. Выполните быструю *инвентаризацию*.

    > **⚠ Предупреждение**
    >
    > Во время инвентаризации *не* включайте функцию **Перенести нераспознанные и импортированные ленты в пул "Свободные ленты"**. Если этот переключатель включен, можно потерять все резервные копии.

2. Проведите *Повторное сканирование* пула **Нераспознанные ленты**. В результате будет получено содержимое загруженных лент.
3. Если какие-либо из обнаруженных резервных копий продолжаются на других лентах, которые еще не сканировались, загрузите эти ленты по запросу и выполните их повторное сканирование.

Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства

1. Загрузите в ленточное устройство ленты, необходимые для восстановления.
2. Загрузите машину с загрузочного носителя.
3. Выберите **Локальное управление этой машиной** или дважды щёлкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.

4. Если ленточное устройство подключено с использованием интерфейса iSCSI, настройте устройство, как описано в *Настройка устройств iSCSI и NDAS*.
5. Щёлкните **Управление лентами**.
6. Нажмите кнопку **Инвентаризация**.
7. В **Объекты для инвентаризации** выберите ленточное устройство.
8. Нажмите **Запуск** для запуска инвентаризации.
9. После завершения инвентаризации нажмите **Закрыть**.
10. Нажмите **Действия** → **Восстановить**.
11. Щёлкните **Выбрать данные** и нажмите кнопку **Обзор**.
12. Разверните **Ленточные устройства**, а затем выберите необходимое устройство. Система запросит подтверждение повторного сканирования. Нажмите **Да**.
13. Выберите пул **Нераспознанные ленты**.
14. Выберите ленты для повторного сканирования. Чтобы выбрать все ленты пула, установите флажок рядом с заголовком столбца **Имя ленты**.
15. Если ленты содержат защищенную паролем резервную копию, установите соответствующий флажок и укажите пароль для резервной копии в поле **Пароль**. Если пароль не указан или недействителен, резервная копия не будет обнаружена. Помните об этом в случае, если после повторного сканирования резервные копии не обнаружены.

    Если ленты содержат несколько резервных копий, защищенных разными паролями, необходимо повторить сканирование несколько раз, поочередно указывая пароли.
16. Нажмите **Запуск** для запуска повторного сканирования. В результате будет получено содержимое загруженных лент.
17. Если какие-либо из обнаруженных резервных копий продолжаются на других лентах, которые еще не сканировались, загрузите эти ленты по запросу и выполните их повторное сканирование.
18. После завершения повторного сканирования нажмите кнопку **ОК**.
19. В представлении ”Архив” выберите резервную копию, затем выберите данные, которые требуется восстановить. После нажатия кнопки **ОК** на странице **Восстановление данных** отобразится список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
20. Настройте другие параметры восстановления.
21. Нажмите кнопку **ОК**, чтобы начать восстановление.

22. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    1. Загрузите ленту.
    2. Выполните быструю *инвентаризацию*.
    3. Нажмите **Обзор** → **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
    4. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения

1. Загрузите в ленточное устройство ленты, необходимые для восстановления.
2. Загрузите машину с загрузочного носителя.
3. Выберите **Локальное управление этой машиной** или дважды щёлкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
4. Нажмите кнопку **Восстановить**.
5. Щёлкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. В поле **Путь** введите `bsp://<адрес узла хранения>/<имя пула>/`, где `<адрес узла хранения>` — это IP-адрес узла хранения, содержащего нужную резервную копию, а `<имя пула>` — имя пула лент. Нажмите кнопку **ОК** и укажите учетные данные для доступа к пулу.
7. Выберите резервную копию, а затем данные для восстановления. После нажатия кнопки **ОК** на странице **Восстановление данных** отобразится список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
8. Настройте другие параметры восстановления.
9. Нажмите кнопку **ОК**, чтобы начать восстановление.
10. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    1. Загрузите ленту.
    2. Выполните быструю *инвентаризацию*.
    3. Нажмите **Обзор** → **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.

4. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

Управление лентами

Обнаружение ленточных устройств

При обнаружении ленточных устройств программа резервного копирования находит ленточные устройства, подключенные к машине, и помещает информацию о них в базу данных управления лентами. Обнаруженные ленточные устройства отключаются от RSM.

Как правило, ленточное устройство обнаруживается автоматически сразу же после подключения устройства к машине, на которой установлен продукт. Однако вам может потребоваться обнаружение ленточных устройств в следующих случаях:

- После подключения или повторного подключения ленточного устройства.
- После установки или переустановки программы резервного копирования на машине, к которой подключено ленточное устройство.

Как обнаружить ленточные устройства

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину, к которой подключено ленточное устройство.
3. Выберите **Поиск устройств**. Будут отображены подключенные ленточные устройства, их накопители и слоты.

Пулы лент

В программе резервного копирования используются пулы лент, представляющие собой логические группы лент. В Кибер Бэкап предустановлены следующие пулы лент (служебные пулы):

- Нераспознанные ленты;
- Импортированные ленты;
- Свободные ленты.

Для размещения резервных копий в хранилищах используются пользовательские пулы, в том числе пользовательский пул по умолчанию. Предусмотрена возможность создания собственных пользовательских пулов.

Ленты можно перемещать между пулами. Подробнее об этом см. раздел *Перемещение в другой пул*.

Служебные пулы

Нераспознанные ленты

Пул содержит ленты, которые записывались сторонними приложениями. Для записи на такие ленты их необходимо явным образом *переместить* в пул **Свободные ленты**. Переместить ленты из этого пула в какой-либо другой, кроме пула **Свободные ленты**, нельзя.

Импортированные ленты

Пул содержит ленты, которые записывались программой Кибер Бэкап в ленточном устройстве, подключенном к другому узлу хранения или агенту. Для записи на такие ленты их необходимо явным образом *переместить* в пул **Свободные ленты**. Переместить ленты из этого пула в какой-либо другой, кроме пула **Свободные ленты**, нельзя.

Свободные ленты

Пул содержит свободные (пустые) ленты. В этот пул можно вручную *перемещать* ленты из других пулов.

При переносе ленты в пул **Свободные ленты** программа Кибер Бэкап удаляет информацию о резервных копиях на ней. Чтобы восстановить резервные копии, выполните повторное сканирование.

Пул используется по умолчанию для резервного копирования, когда не требуется создавать собственные пулы. Обычно он применяется к одному ленточному устройству с небольшим числом лент.

Пользовательские пулы

Для разделения резервных копий с различными данными необходимо создать несколько пулов. Например, можно создать пользовательские пулы для разделения:

- резервных копий разных отделов компании;
- резервных копий разных машин;
- резервных копий системных томов и пользовательских данных.

Операции с пулами

Создание пула

Для создания пользовательского пула выполните следующие действия:

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которым прикреплено ленточное устройство, и затем

нажмите **Пулы лент** около необходимой машины.

3. Нажмите **Создать пул**.
4. Введите имя пула.
5. [Необязательно] Настройте автоматическое пополнение, выбрав один из следующих вариантов:
   - Снимите флажок **Пополнять автоматически из пула "Свободные ленты"** для ручного управления носителями.
   - Оставьте флажок **Пополнять автоматически из пула "Свободные ленты"** и выберите тип лент, которыми создаваемый пул будет автоматически пополняться:
     - **Перезаписываемыми носителями** (по умолчанию) — стандартные операции;
     - **Носителями однократной записи (тип WORM)** — для архивного хранения неизменяемых данных.

> **Примечание**
>
> При выборе по умолчанию (**Перезаписываемыми носителями**) для автопополнения из пула **Свободные ленты** также будут использоваться ленты неизвестного типа.

6. Нажмите **Создать**.

Изменение пула

> **Примечание**
>
> Изменение параметров доступно только для пользовательского пула. Параметры служебного пула изменению не подлежат.

Как изменить пул

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Выберите требуемый пользовательский пул и нажмите кнопку **Правка пула**.
4. Можно изменить имя или настройки пула. Дополнительные сведения о настройках пула см. в разделе *Создание пула*.

5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

Удаление пула

Можно удалять только *созданные* пользовательские пулы. Нельзя удалить служебные пулы лент (**Нераспознанные ленты**, **Импортированные ленты** и **Свободные ленты**), а также **Пул по умолчанию**.

Перед удалением пула выполните следующие действия:

- Переместите все ленточные носители в другой пул. *Переместите* ленты в пул **Свободные ленты** или воспользуйтесь процедурой *стирания*, если ленты содержат неактуальные данные.
- Внесите изменения в планы защиты, в которых данный пул указан в качестве хранилища резервных копий. В противном случае выполнение этих планов защиты завершится сбоем.

Как удалить пул

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. Выберите требуемый пул и нажмите кнопку **Удалить**.
4. Подтвердите удаление пула.

Операции с лентами

Перемещение в другой слот

Используйте эту операцию в следующих ситуациях:

- необходимо извлечь несколько лент из ленточного устройства одновременно;
- ленточное устройство не имеет устройства оперативной смены носителя, и извлекаемые ленты находятся в слотах несъемных магазинов.

Необходимо переместить ленты в слоты одного магазина, а затем извлечь магазин вручную.

Порядок перемещения ленты в другой слот

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.

4. Нажмите **Переместить в слот**.
5. Выберите новый слот, в который нужно перенести выбранную ленту.
6. Нажмите **Переместить**, чтобы начать операцию.

Перемещение в другой пул

Операция позволяет перенести одну или несколько лент из одного пула в другой.

Существуют следующие возможности:

- *Перемещение лент в пул "Свободные ленты"*;
- *Перемещение лент между пулами*.

> **Важно**
>
> Чистящие ленты всегда отображаются в пуле **Нераспознанные ленты**; перенести их в другой пул нельзя.

Допустимое перемещение лент

В таблицах ниже приводятся разрешенные перемещения лент между пулами в зависимости от типа перемещаемых лент, находящихся в них.

Перезаписываемые ленты

Исходный пул / Целевой пул	**Пользовательские пулы**	**Служебные пулы**		
		Свободные ленты	**Нераспознанные ленты**	**Импортированные ленты**
Пользовательские пулы	Перемещение: • пустые ленты — через веб-консоль • ленты с данными — через командную строку	Перемещение	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Исходный пул / Целевой пул		Пользовательские пулы	Служебные пулы		
			Свободные ленты	Нераспознанные ленты	Импортированные ленты
Служебные пулы	Свободные ленты	Перемещение (как пустые) Автоматическое пополнение	—	—	—
	Импортированные ленты	Сканирование	Перемещение	—	—
	Нераспознанные ленты	Сканирование	Перемещение	—	—

Ленты WORM

Исходный пул / Целевой пул		Пользовательские пулы	Служебные пулы		
			Свободные ленты	Нераспознанные ленты	Импортированные ленты
Пользовательские пулы		Перемещение: • пустые ленты — через веб-консоль • ленты с данными — через командную строку	Перемещение (только пустые)	—	—
Служебные пулы	Свободные ленты	Перемещение Автоматическое пополнение	—	—	—
	Импортированные ленты	Сканирование	Перемещение	—	—
	Нераспознанные ленты	Сканирование	Перемещение	—	—

Особенности перемещения WORM-лент:

- Пустые WORM-ленты можно перемещать между всеми пулами;

- WORM-ленты с данными можно перемещать между пользовательскими пулами;
- При перемещении в пул **Свободные ленты** данные на WORM-лентах не удаляются.

Чистящие ленты

Исходный пул / Целевой пул		**Пользовательские пулы**	**Служебные пулы**		
			Свободные ленты	**Нераспознанные ленты**	**Импортированные ленты**
Пользовательские пулы		—	—	—	—
Служебные пулы	Свободные ленты	—	—	—	—
	Импортированные ленты	—	—	—	—
	Нераспознанные ленты	—	—	—	—

Ограничения для чистящих носителей:

- Можно перемещать только между слотами хранения;
- Используйте *очистку привода* для контролируемой очистки.

Ленты неизвестного типа

Исходный пул / Целевой пул	**Пользовательские пулы**	**Служебные пулы**		
		Свободные ленты	**Нераспознанные ленты**	**Импортированные ленты**
Пользовательские пулы	Перемещение: • пустые ленты — через веб-консоль • ленты с данными — через командную строку	Перемещение	—	—

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

Исходный пул / Целевой пул		Пользовательские пулы	Служебные пулы		
			Свободные ленты	Нераспознанные ленты	Импортированные ленты
Служебные пулы	Свободные ленты	Перемещение Автоматическое пополнение	—	—	—
	Импортированные ленты	Сканирование	Перемещение	—	—
	Нераспознанные ленты	Сканирование	Перемещение	—	—

Перемещение лент в пул "Свободные ленты"

Если требуется повторно использовать ленты, на которых содержатся старые и ненужные резервные копии или просто оптимизировать ваше пространство, используйте перемещение лент в пул **Свободные ленты**.

Операция производится только с выбранными лентами. Тем не менее, информация о резервных копиях порой содержится и на других (созависимых) лентах. Перед непосредственным выполнением операции происходит автоматический поиск и обнаружение таких лент.

Предупреждение

При переносе ленты с резервными копиями в пул **Свободные ленты** Кибер Бэкап удаляет информацию об этих резервных копиях на перемещаемой ленте и на созависимых лентах. Для восстановления удаленной информации потребуется повторное сканирование ленты.

Ограничения

- Ленты WORM с данными нельзя перенести из пользовательского пула в пул **Свободные ленты**.
- Перемещение носителей выполняется в соответствии с *таблицами допустимого перемещения*.

Перемещение

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.

4. Нажмите **Переместить в пул**.
5. Выберите пул **Свободные ленты**.
6. Нажмите **Переместить** для сохранения изменений.

Ход выполнения перемещения отображается в разделе **Панель мониторинга** → **Действия**.

Перемещение лент между пулами

Операция может потребоваться при необходимости перераспределения ресурсов между пользовательскими пулами: пополнение пулов, балансировка нагрузки и т. д.

> **Важно**
>
> Операция применяется только к лентам, не содержащим данных резервных копий.

Перед выполнением операции проводится автоматическая проверка отсутствия данных на лентах. При обнаружении лент с данными или лент, занятых другими операциями, операция будет продолжена, а эти ленты исключены из операции. Исключенные ленты останутся в своих исходных пулах. Если при проверке на всех лентах будут обнаружены данные, операция будет отменена.

Ограничения

- Отсутствие данных резервных копий на лентах;
- Перемещение носителей выполняется в соответствии с *таблицами допустимого перемещения*.

Перемещение

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. [Необязательно] Нажмите **Создать новый пул**, если требуется создать другой пул для выбранных лент. Выполните действия, описанные в разделе *Создание пула*.
4. Щёлкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
5. Нажмите **Переместить в пул**.
6. Выберите пул, в который необходимо перенести ленты.
7. Нажмите **Переместить** для сохранения изменений.

Ход выполнения перемещения отображается в разделе **Панель мониторинга** → **Действия**.

Инвентаризация

Операция инвентаризации обнаруживает ленты, загружаемые в ленточное устройство, и присваивает имена лентам, у которых их нет.

Существует два вида инвентаризации: ручная и автоматическая.

Ручная инвентаризация

Ручная инвентаризация запускается по требованию пользователя.

Методы инвентаризации

Существует два метода ручной инвентаризации.

Быстрая инвентаризация

Агент или узел хранения сканируют штрихкоды лент и проверяют наличие в системе информации об этих лентах. Если информация о ленте обнаружена (лента ранее использовалась в этой системе), Кибер Бэкап распознает ленту и автоматически возвращает её в соответствующий пул.

Если информация о ленте отсутствует (лента новая или использовалась в другой системе), она направляется в пул нераспознанных лент.

Используйте этот метод для распознания лент, которые используются одним и тем же ленточным устройством, подключенным к одной и той же машине.

Если ленточная библиотека не поддерживает сканирование штрихкодов, все ленты направляются в пул нераспознанных лент. В этом случае для распознания лент выполните полную инвентаризацию или используйте комбинацию быстрой и полной инвентаризации, как описано далее в этом разделе.

Полная инвентаризация

В процессе полной инвентаризации агент или узел хранения анализирует информацию, считанную с инвентаризируемых лент, и определяет следующие параметры:

- тип ленты и ее характеристики;
- содержимое лент и доступное пространство;
- состояние аппаратной защиты от записи.

В следующих таблицах показано, в какие пулы направляются ленты после полной инвентаризации.

Использовал ленту	Считывает ленту	В какой пул направляется лента
Агент	Тот же агент	Пул, где лента была раньше
	Другой агент	Импортированные ленты
	Узел хранения	Импортированные ленты
Узел хранения	Тот же узел хранения	Пул, где лента была раньше
	Другой узел хранения	Импортированные ленты
	Агент	Импортированные ленты
Приложение для резервного копирования стороннего производителя	Агент или узел хранения	Нераспознанные ленты

Ленты, отличные от обычных заполненных, направляются в пулы, соответствующие типу ленты.

Тип ленты	В какой пул направляется лента
Пустая лента	Свободные ленты
Чистящая лента	Нераспознанные ленты

Комбинация быстрой и полной инвентаризации

Полная инвентаризация всего ленточного устройства может занять длительное время. Если требуется инвентаризация только нескольких лент, сделайте следующее.

1. Выполните быструю инвентаризацию ленточного устройства.
2. Щёлкните пул нераспознанных лент. Найдите ленты, которые нужно инвентаризировать, и отметьте, в каких слотах они находятся.
3. Выполните полную инвентаризацию этих слотов.

Что делать после инвентаризации

Если вы хотите создавать резервные копии на лентах, которые были помещены в пул нераспознанных лент или пул импортированных лент, *переместите* их в пул свободных лент, а затем в пользовательский пул. Если пул, в котором вы хотите создавать резервные копии, пополняем, можно оставить ленты в пуле свободных лент.

Если требуется восстановление с ленты, которая была помещена в пул нераспознанных лент или импортированных лент, необходимо *повторно сканировать* эту ленту. Лента будет перемещена в пул, который вы выбрали во время повторного сканирования, и резервные копии, которые хранятся на ленте, появятся в хранилище.

Последовательность действий

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину, к которой подключено ленточное устройство, а затем выберите ленточное устройство, для которого необходимо выполнить инвентаризацию.
3. Нажмите кнопку **Инвентаризация**.
4. [Необязательно] Для выбора быстрой инвентаризации отключите функцию **Полная инвентаризация**.
5. [Необязательно] Включите функцию **Перенести неопознанные и импортированные ленты в пул "Свободные ленты"**.

   > **Предупреждение**
   >
   > Подключайте эту функцию только в том случае, если вы абсолютно уверены, что данные, которые хранятся на лентах, больше не нужны и ленты можно перезаписать.

6. Нажмите **Начать инвентаризацию сейчас** для запуска инвентаризации.

Автоинвентаризация

Автоинвентаризация — это инвентаризация, работающая в фоновом режиме. Она выполняется для своевременного обнаружения изменений в ленточных устройствах и поддержания их актуального статуса. Автоинвентаризация и инвентаризация не работают вместе.

Автоинвентаризация имеет меньший приоритет по сравнению с обычной инвентаризацией. Если на текущий момент работает инвентаризация или есть инвентаризации, ждущие своей очереди на выполнение, автоинвентаризация не запускается. Если запустить инвентаризацию, то выполняющаяся на текущий момент автоинвентаризация будет прервана.

Автоинвентаризация запускается периодически согласно параметрам настройки. Настройка периода выполнения автоинвентаризации производится в конфигурационном файле `tape_devices.xml`. Расположение конфигурационного файла: `C:\ProgramData\Acronis\BackupAndRecovery\ARSM\Configuration` (в Windows) и `/var/lib/Acronis/BackupAndRecovery/ARSM/Configuration` (в Linux). Вы можете настроить параметр `autoinventory` самостоятельно. Атрибут `period` параметра `autoinventory` настраивается в следующих границах: от 3 до 7200 (в секундах). По умолчанию значение параметра равно 180.

```
<autoinventory>
    <enabled value="1"/>
    <period value="180"/>
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
</autoinventory>
```

Повторное сканирование

Сведения о содержимом лент хранятся в особой базе данных. В ходе операции повторного сканирования выполняется чтение содержимого лент и, если содержимое не соответствует информации, имеющейся в базе данных, обновляется база данных. Резервные копии, обнаруженные в результате этой операции, помещаются в заданный пул.

За одну операцию можно просканировать ленты из одного пула.

Для повторного сканирования лент с многопотоковой резервной копией или с многопотоковой и мультиплексированной резервной копией понадобится как минимум такое же количество приводов, которое было использовано при создании этой резервной копии. Такие резервные копии невозможно заново отсканировать, используя автономное ленточное устройство.

Повторное сканирование рекомендуется в следующих случаях:

- Если база данных узла хранения или управляемой машины потеряна или повреждена;
- Если сведения о ленте в базе данных устарели (например, содержимое ленты было изменено другим узлом хранения или агентом);
- Если требуется получить доступ к резервным копиям, сохраненным на лентах при работе с загрузочным носителем;
- Если по ошибке *удалены* сведения о ленте из базы данных. При повторном сканировании удаленной ленты резервные копии, сохраненные на ней, вновь появляются в базе данных и становятся доступными для восстановления данных;
- Если резервные копии были удалены из ленты вручную или с помощью правил хранения, но нужно сделать их доступными для восстановления данных. Перед повторным сканированием такой ленты *извлеките* ее, *удалите* сведения о ней из базы данных, а затем снова вставьте ленту в устройство.

Порядок повторного сканирования лент

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Ленточные устройства** около необходимой машины.
3. Выберите ленточное устройство, в которое загружены ленты.
4. Выполните быструю *инвентаризацию*.

> **Примечание**
>
> Во время инвентаризации *не* включайте функцию **Перенести нераспознанные и импортированные ленты в пул "Свободные ленты"**.

5. Выберите пул **Нераспознанные ленты**. После быстрой инвентаризации большинство лент направляется именно в этот пул. Также возможно повторное сканирование лент из любого другого пула.
6. Выберите отдельные ленты для индивидуального сканирования.
7. Нажмите **Повторное сканирование**.
8. Выберите пул, в который будут помещаться резервные копии после обнаружения.
   - Для лент из пользовательского пула — только текущий пул (целевой пул изменить нельзя);
   - Для лент из служебных пулов — любой пользовательский пул.
9. При необходимости установите флажок **Включить восстановление файлов из образов дисков на лентах**.

   Если этот флажок установлен, программа создает специальные дополнительные файлы на жестком диске машины, к которой подсоединено ленточное устройство. Восстановление файлов из резервных копий дисков возможно до тех пор, пока эти дополнительные файлы будут в порядке. Обязательно установите флажок, если ленты содержат *резервные копии с поддержкой приложений*. В противном случае вы не сможете восстановить данные приложений из этих резервных копий.
10. Нажмите **Запуск повторного сканирования** для запуска повторного сканирования.

Результат: повторно отсканированные ленты перемещаются в выбранный пул. Резервные копии, сохраненные на лентах, находятся в этом пуле. Если резервная копия расположена на нескольких лентах, то вторая лента будет отсканирована автоматически и резервная копия будет добавлена в пул.

Переименование

Если программой обнаружена новая лента, ей автоматически назначается имя в следующем формате: **Лента XXX**, где **XXX** — уникальный номер. Ленты нумеруются последовательно. Операция переименования позволяет вручную изменить имя ленты.

Порядок переименования лент

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите **Переименовать**.
5. Введите новое имя выбранной ленты.
6. Нажмите **Переименовать** для сохранения изменений.

Стирание

> **Важно**
>
> Операцию стирания отменить невозможно.

Если лента находилась в пуле **Нераспознанные ленты** или **Импортированные ленты**, то после стирания она будет перемещена в пул **Свободные ленты**. Лента, размещенная в любом другом пуле, не перемещается.

Ленты WORM не могут быть стерты независимо от содержимого.

Ленты с включенной аппаратной защитой от записи требуют предварительного снятия защиты.

Порядок стирания лент

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Стереть**. Система попросит подтвердить операцию.
5. Выберите способ стирания:
    - **Быстрое стирание**. Удаляются заголовки резервных копий, а из базы данных удаляется информация об этих резервных копиях. Информация о самой ленте сохраняется в базе данных.
    - **Полное стирание**. Физически удаляются все резервные копии, сохраненные на ленте, а из

базы данных удаляется информация об этих резервных копиях. Однако информация о самой ленте сохраняется в базе данных.

6. Нажмите **Стереть**, чтобы начать операцию.

Извлечение

Для успешного извлечения ленты из библиотеки ленточных носителей библиотека ленточных носителей должна иметь устройство оперативной смены носителя (mail-slot), которое не должно быть блокировано пользователем или другой программой.

Порядок извлечения лент

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Извлечь**. Программа попросит ввести описание ленты. Рекомендуется описать физическое место, в котором будут храниться ленты. Во время восстановления программа покажет это описание, и вы легко найдете ленты.
5. Нажмите кнопку **Извлечь**, чтобы начать операцию.

После того как лента извлечена вручную или *автоматически*, рекомендуется написать на ленте ее имя.

Удаление

В ходе операции удаления из базы данных удаляются данные о резервных копиях, хранимых на выбранной ленте, и о самой ленте.

Можно удалить только автономную (*извлеченную*) ленту.

Порядок удаления ленты

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите кнопку **Удалить**. Система попросит подтвердить операцию.
5. Нажмите **Удалить**, чтобы удалить ленту.

Действия в случае удаления ленты по ошибке

В отличие от *стертой* ленты, данные из удаленной ленты не удаляются физически. Поэтому можно вновь сделать доступными резервные копии, сохраненные на такой ленте. Выполните следующие действия.

1. Загрузите ленту в ленточное устройство.
2. Выполните быструю *инвентаризацию*, чтобы обнаружить ленту.

   > **Примечание**
   >
   > Во время инвентаризации *не* включайте функцию **Перенести нераспознанные и импортированные ленты в пул "Свободные ленты"**.

3. Выполните *повторное сканирование*, чтобы сопоставить данные, сохраненные на лентах, с базой данных.

Указание набора лент

Данная операция позволяет указать набор лент.

Набор лент представляет собой группу лент одного пула.

В отличие от указания набора лент в *параметрах резервного копирования*, где допустимо использование переменных, здесь допустимо указание только строковых значений.

Выполнение данной операции приведет к созданию программным обеспечением резервной копии *указанных* лент в соответствии с определенным правилом (например, для сохранений резервных копий за понедельник на ленте 1, резервных копий за вторник на ленте 2 и т. д.). Укажите определенный набор лент для каждой требуемой ленты и затем укажите тот же тип лент или используйте соответствующие переменные в параметрах резервного копирования.

В вышеупомянутом примере следует указать набор лент `Monday` для ленты 1, `Tuesday` для ленты 2 и т. д. В параметрах резервного копирования укажите `[День недели]`. В данном случае надлежащая лента будет использована в соответствующий день недели.

Порядок указания набора лент для одной или нескольких лент

1. Нажмите **Настройки** → **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство, и затем нажмите **Пулы лент** около необходимой машины.
3. Щёлкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.

4. Нажмите **Набор лент**.
5. Введите имя набора лент. Если для указанных лент уже был задан набор лент, он будет заменен. Для исключения лент из набора лент без перемещения их в другой набор удалите существующее имя набора лент.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

Ручная очистка ленточных приводов

Ручная очистка осуществляется с помощью специальных чистящих носителей (см. раздел *Типы ленточных носителей*).

Рекомендуется регулярно проводить очистку ленточных приводов для профилактики ошибок оборудования.

> **Примечание**
>
> Операцию очистки нельзя отменить после ее начала.

Чтобы очистить ленточный привод, выполните следующие действия:

1. Нажмите **Настройки** → **Управление лентами**.
2. Под необходимой машиной нажмите **Ленточные устройства** и далее выберите ленточную библиотеку, а затем ленточный привод.
3. На панели **Действия** нажмите **Выполнить очистку**.
4. Выберите чистящий носитель из списка доступных. Система показывает количество оставшихся циклов очистки для каждого носителя.

   > **Примечание**
   >
   > Кибер Бэкап определяет количество оставшихся циклов очистки после первого применения чистящего носителя.

5. Нажмите **Очистить**.

Очистка привода занимает 2-5 минут. Привод недоступен во время очистки.

Настройки системы

Чтобы получить доступ к этим настройкам, щёлкните **Настройки** → **Настройки системы**.

Раздел **Настройки системы** видим только для *администраторов организации*.

Уведомления по электронной почте

Кибер Бэкап поддерживает возможность автоматической отправки уведомлений о событиях резервного копирования (включая предупреждения и сообщения об ошибках) по электронной почте.

Можно использовать:

- Глобальные настройки уведомлений по электронной почте. Общие настройки для всех уведомлений, отправляемых по электронной почте с сервера управления. Настройка глобальных уведомлений показана далее в этом разделе.
- Настройки резервного копирования по умолчанию (см. раздел *Параметры резервного копирования по умолчанию*). Настройки применяются к плану защиты при его создании. Действуют для событий, возникающих во время резервного копирования.
- Индивидуальные настройки для плана защиты (см. раздел *Уведомления по электронной почте*). Настройки отправки уведомлений отдельного плана защиты для событий, возникающих во время резервного копирования.

Настройки уведомлений в плане защиты дополняют глобальные настройки. Если один и тот же адрес электронной почты указан в глобальных настройках и в настройках плана защиты, уведомление на него придёт дважды: сначала в соответствии с глобальными настройками, а затем — с настройками плана защиты.

Важно

При изменении глобальных настроек уведомлений изменяются все планы защиты, в которых они используются. Изменение *настроек по умолчанию* обновит параметры только для новых планов защиты и не затронет существующие.

Перед настройкой уведомлений обязательно настройте параметры *сервера электронной почты*.

Изменение глобальных настроек почтовых уведомлений

1. Выберите **Настройки** → **Настройки системы** → **Уведомления по электронной почте**.
2. Переведите переключатель **Получать уведомления по электронной почте** в положение **Включено**.
3. В поле **Адрес электронной почты получателя** введите адрес электронной почты, на который будут приходить уведомления. Можно указать несколько адресов, разделяя их точкой с запятой.
4. [Необязательно] В поле **Шаблон темы** укажите шаблон уведомления.

   Можно использовать следующие переменные:

   - `[Оповещение]` — сводка оповещений;
   - `[Устройство]` — имя устройства;
   - `[План]` — название плана, для которого создано оповещение;
   - `[Сервер управления]` — имя хоста машины, на которой установлен сервер управления;
   - `[Отдел]` — название отдела, которому принадлежит машина.

   Шаблон по умолчанию: [Оповещение] Устройство: [Устройство] План: [План]
5. В разделе **Ежедневные краткие сведения об активных оповещениях** укажите время отправки сводки оповещений. Сводка содержит количество и тип активных оповещений в Кибер Бэкап.

   > **Примечание**
   >
   > Установите флажок **Не отправлять сообщения "Нет активных оповещений"**, чтобы не получать сообщения об отсутствии новых уведомлений.

6. В разделе **Отправлять уведомления о следующих событиях** установите флажки для событий, о которых необходимо получать уведомления. Их можно выбрать из списка всех возможных оповещений, сгруппированных по степени серьезности.
7. В блоке **Группировка уведомлений** выберите один из вариантов:

   - **Включено** (значение по умолчанию) — уведомления группируются по планам защиты (один план может быть применён к нескольким устройствам).

     При выборе этого значения по умолчанию устанавливается флажок **Получать успешные сгруппированные уведомления**. В этом случае отправляются все группы уведомлений, включая полностью успешные. Снимите флажок, если уведомления о полностью успешных операциях не требуются.
   - **Отключено** — уведомления отправляются по каждому устройству отдельно, даже если к ним

применён один и тот же план защиты.

> **Примечание**
>
> Группировка уведомлений работает с ресурсами PostgreSQL, CommuniGate Pro, VK WorkMail, VK WorkDisk, Mailion и Kubernetes.

8. Выберите язык, который будет использоваться в уведомлениях по электронной почте.
9. Чтобы применить настройки, нажмите кнопку **Сохранить**.

   Чтобы вернуться к последним сохранённым настройкам, нажмите кнопку **Очистить**.

Сервер электронной почты

Можно указать почтовый сервер, который будет использоваться для отправки уведомлений с сервера управления.

Выбор почтового сервера

1. Последовательно выберите пункты **Настройки** → **Настройки системы** → **Сервер электронной почты**.
2. В разделе **Почтовая служба** выберите один из перечисленных ниже пунктов.
   - Другое,
   - Mail.ru,
   - Yandex,
   - Gmail.

     В учетной записи Gmail должен быть включен параметр **Ненадежные приложения**. Дополнительную информацию см. по ссылке https://support.google.com/accounts/answer/6010255.
3. [Только для пользовательской почтовой службы] Задайте указанные ниже настройки.
   - В поле **Сервер SMTP** введите имя сервера исходящей почты (SMTP).
   - В поле **Порт SMTP** укажите порт сервера исходящей почты. По умолчанию это порт 25.
   - Укажите, следует ли использовать шифрование SSL или TLS. Выберите **Нет**, чтобы отключить шифрование.
   - Если SMTP требует выполнять проверку подлинности, установите флажок **Для сервера SMTP требуется проверка подлинности**, а затем укажите учетные данные учетной записи, которая

будет использоваться для отправки сообщений. Если вы не уверены, требует ли сервер SMTP проверки подлинности, обратитесь за помощью к сетевому администратору или поставщику услуг электронной почты.

4. [Только для Mail.ru, Yandex и Gmail] Укажите данные учетной записи, которая будет использоваться для отправки сообщений.
5. В поле **Отправитель** введите имя отправителя. Это имя будет указываться в поле **От** уведомлений по электронной почте.
6. [Необязательно] Щёлкните **Отправить тестовое сообщение**, чтобы проверить, правильно ли работают уведомления по электронной почте с заданными настройками. Введите адрес электронной почты, на который следует отправить тестовое сообщение.

Настройка уведомлений в MAX

Кибер Бэкап поддерживает возможность автоматической отправки уведомлений о событиях резервного копирования (включая предупреждения и сообщения об ошибках) в созданный пользователем канал на платформе MAX. Уведомления направляются с помощью интеграции через специализированного чат-бота.

Примечание

В целях повышения безопасности и стабильности работы платформа MAX накладывает ограничения на отправку сообщений:

- не более 30 запросов в секунду (RPS) на уровне всего чат-бота;
- не более 2 запросов в секунду (RPS) непосредственно в один чат.

Подготовительные работы

Для успешной настройки уведомлений выполните следующие предварительные шаги:

1. Установите корневой (Root) и промежуточные (Sub) сертификаты Национального удостоверяющего центра Минцифры в качестве доверенных на машине сервера управления Кибер Бэкап. Для этого выполните следующие действия:
   1. Перейдите на веб-сайт ”Госуслуги” в раздел сертификатов и выберите вкладку с операционной системой, которая установлена на машине сервера управления Кибер Бэкап.
   2. Скачайте и установите сертификаты безопасности, следуя инструкциям на веб-сайте ”Госуслуги”.

> **Важно**
>
> При установке сертификатов на машину с ОС Windows в окне **Мастер импорта сертификатов** выберите **Локальный компьютер**.

3. Перезапустите службу сервера управления Кибер Бэкап, выполнив команды от имени привилегированного пользователя:

   В ОС Linux

   ```
   sudo service acronis_asm restart
   ```

   В ОС Windows

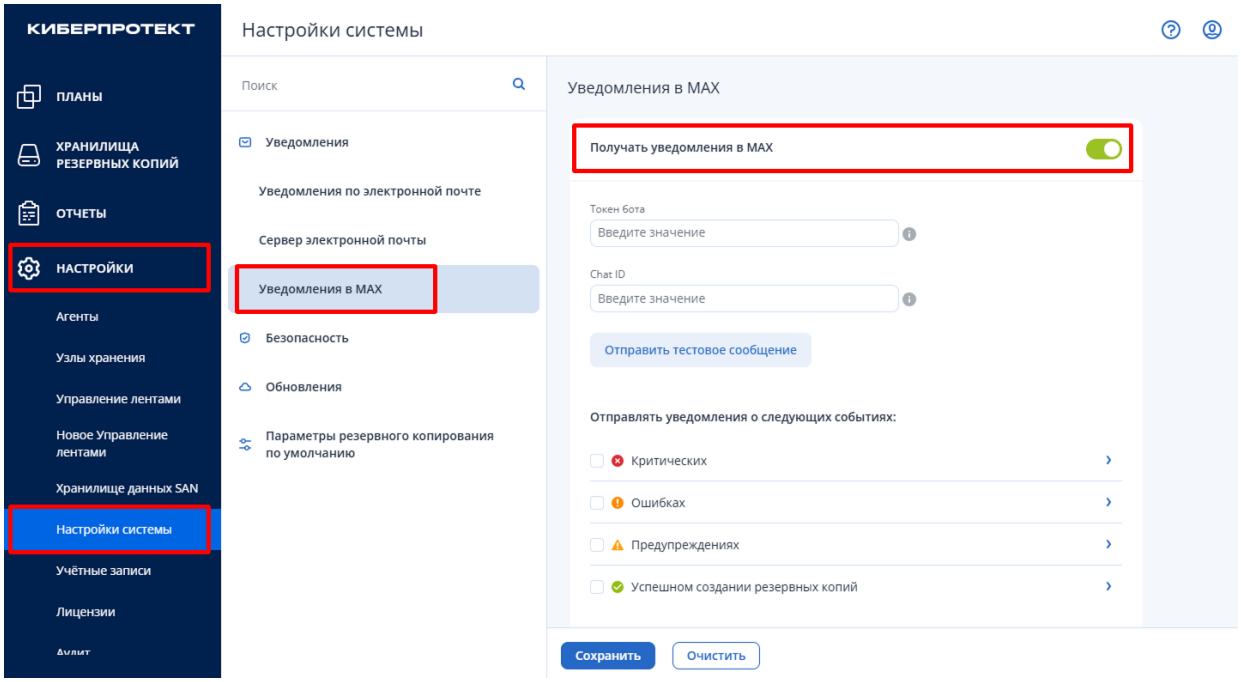
   ```
   net stop asm
   net start asm
   ```

2. На платформе MAX создайте профиль и пройдите верификацию.
3. Создайте чат-бот и зарегистрируйте его на платформе MAX.
4. Получите токен чат-бота (он потребуется для настройки отправления уведомлений из Кибер Бэкап).
5. Создайте чат (канал, группу или диалог) в MAX, куда будут отправляться сообщения из Кибер Бэкап.

Настройка отправления уведомлений в MAX

Чтобы настроить отправление уведомлений в MAX, выполните следующие действия:

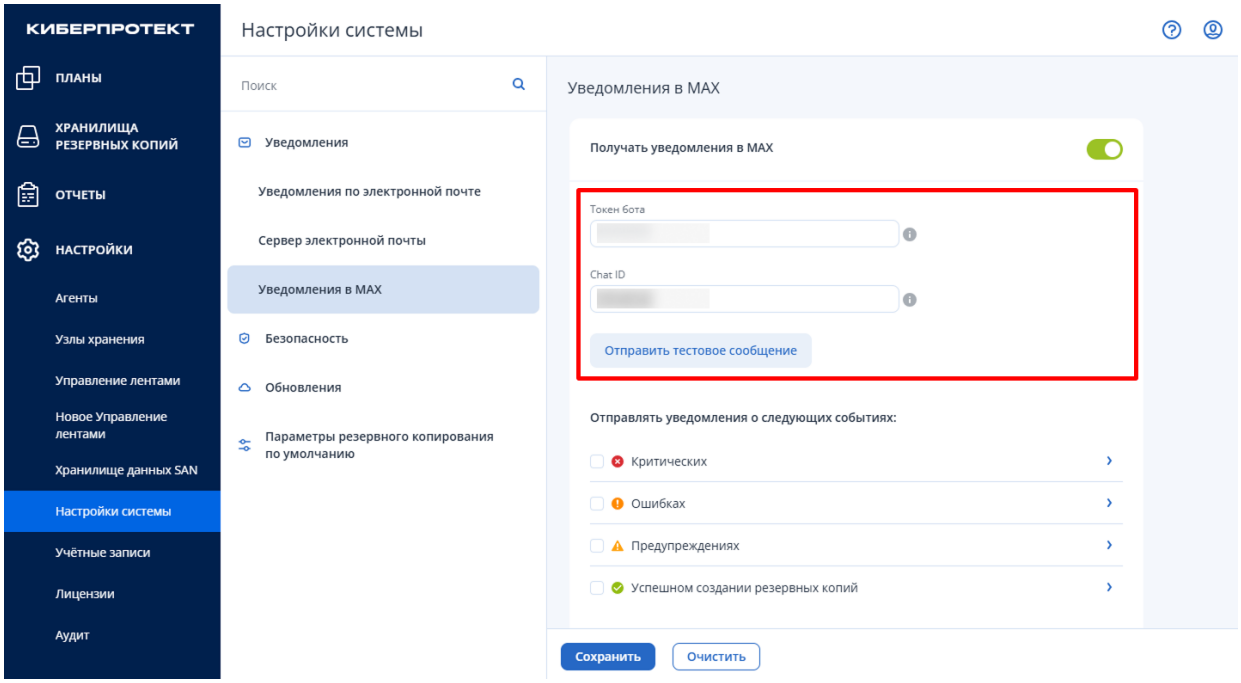
1. В веб-консоли Кибер Бэкап выберите **Настройки** → **Настройки системы** → **Уведомления в MAX**.
2. Переведите переключатель **Получать уведомления в MAX** в положение **Включено**.



3. Укажите токен чат-бота в поле **Токен бота** (подробнее о токене доступа см. в документации платформы MAX).

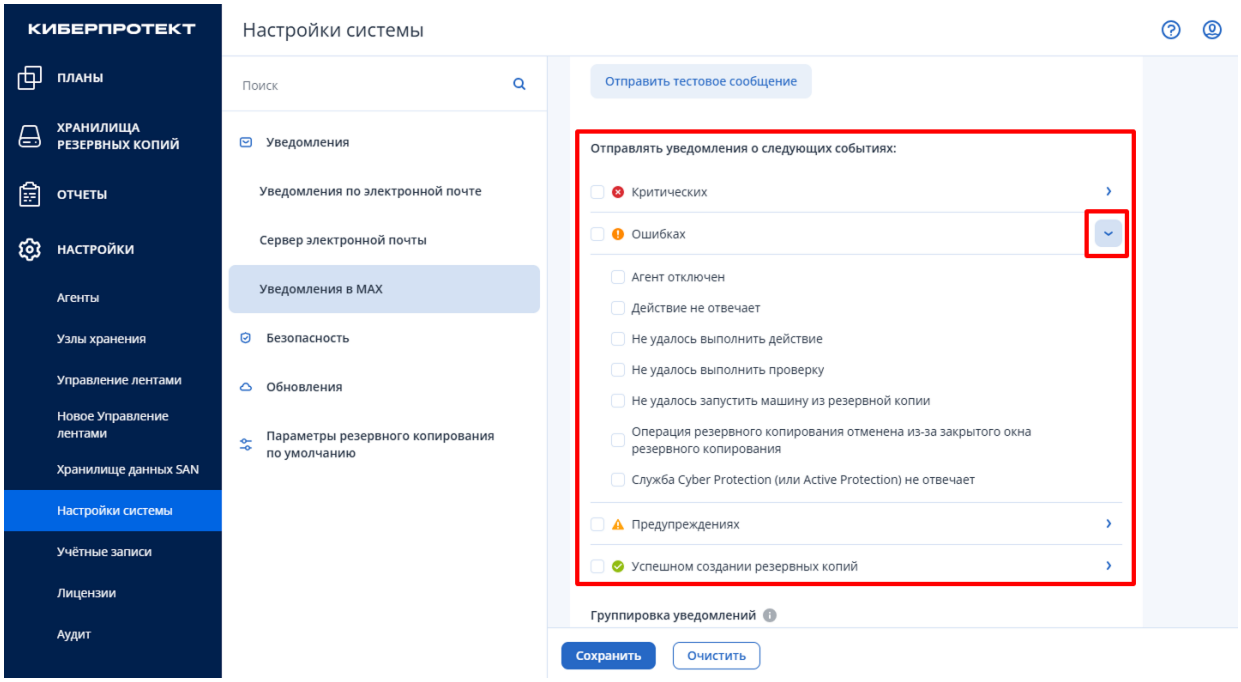
4. В поле **Chat ID** через запятую укажите не более 10 идентификаторов чатов, в которые будут отправляться уведомления.

   Для проверки в указанные чаты можно отправить тестовое сообщение соответствующей кнопкой.



5. В блоке **Отправлять уведомления о следующих событиях:** выберите события, для которых будут направляться уведомления. Для детального просмотра раскройте список, нажав на иконку со

стрелкой в строке названия группы событий. По умолчанию события не выбраны.



6. В блоке **Группировка уведомлений** выберите один из вариантов:

   - **Включено** (значение по умолчанию) — уведомления группируются по планам защиты (один план может быть применён к нескольким устройствам).

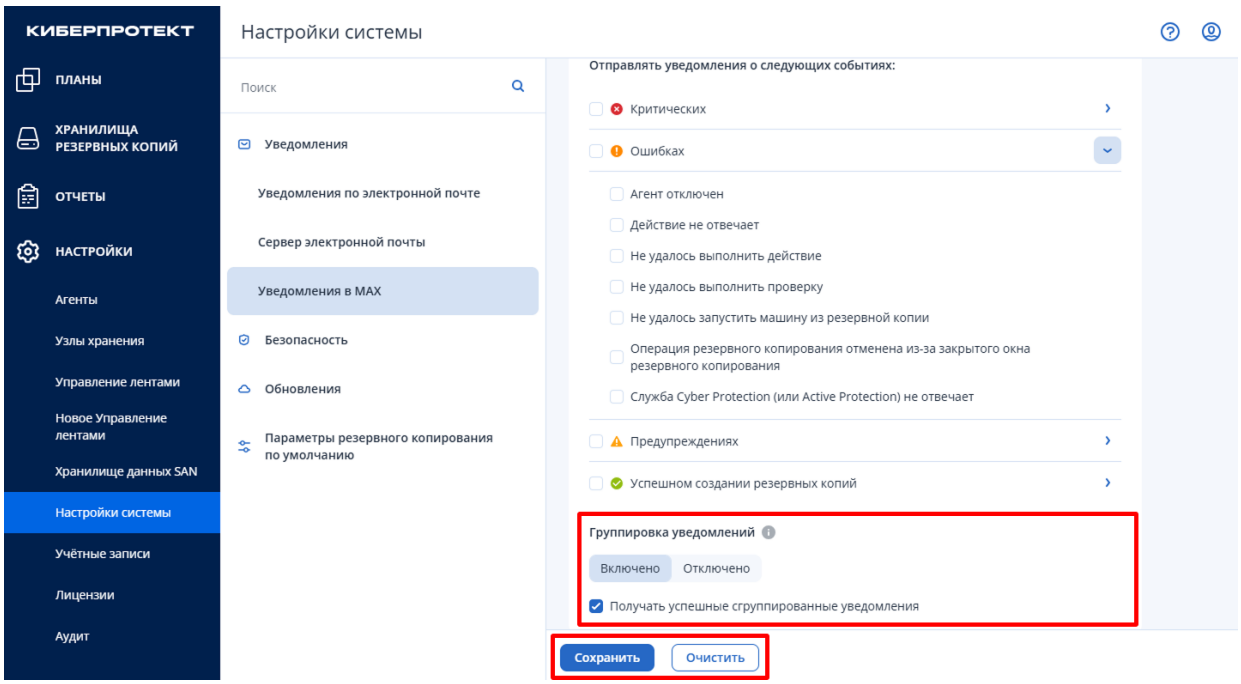
     При выборе этого значения по умолчанию устанавливается флажок **Получать успешные сгруппированные уведомления**. В этом случае отправляются все группы уведомлений, включая полностью успешные. Снимите флажок, если уведомления о полностью успешных операциях не требуются.

   - **Отключено** — уведомления отправляются по каждому устройству отдельно, даже если к ним применён один и тот же план защиты.

> **Примечание**
>
> Группировка уведомлений работает с ресурсами PostgreSQL, CommuniGate Pro, VK WorkMail, VK WorkDisk, Mailion и Kubernetes.

7. Чтобы применить настройки, нажмите кнопку **Сохранить**.

   Чтобы вернуться к последним сохранённым настройкам, нажмите кнопку **Очистить**.



Безопасность

Эти параметры позволяют повысить безопасность Кибер Бэкап.

Завершить сеансы работы неактивных пользователей через

Этот параметр позволяет указать время ожидания до автоматического выхода по причине неактивности пользователя. Когда до истечения времени ожидания остается одна минута, программа выводит пользователю запрос на подтверждение активности. Если этот запрос останется без ответа, будет выполнен выход из программы по тайм-ауту с потерей всех несохраненных изменений.

Значение по умолчанию: **Включено. Тайм-аут: 10 минут.**

> **Примечание**
>
> Максимальная продолжительность активной сессии пользователя составляет 24 часа.

Показать уведомление о последнем входе текущего пользователя

Этот параметр позволяет показать дату и время последнего успешного входа пользователя, количество сбоев аутентификации с момента последнего успешного входа и IP-адрес, с которого был выполнен последний успешный вход. Эта информация отображается в нижней части экрана при каждом входе пользователя.

Значение по умолчанию: **Отключено**.

Предупреждать об истечении срока действия локального пароля или пароля домена

Этот параметр позволяет отображать срок истечения пароля пользователя для доступа к серверу управления Кибер Бэкап. Это локальный пароль или пароль домена, с которым пользователь входит на машину с установленным сервером управления. Время до окончания срока действия пароля отображается в нижней части экрана и в меню учётной записи в верхнем правом углу.

Значение по умолчанию: **Отключено**.

Обновления

Этот параметр определяет, будет ли Кибер Бэкап проверять наличие новой версии при каждом входе администратора организации в веб-консоль Кибер Бэкап.

Значение по умолчанию: **Включено**.

Если этот параметр отключен, администратор может проверить обновления вручную, как описано в разделе *Проверка наличия обновлений программного обеспечения*.

Параметры резервного копирования по умолчанию

Параметры резервного копирования по умолчанию применяются ко всем новым планам защиты, создаваемым на сервере управления. Администратор может изменить эти значения, как описано далее. В этом случае новые параметры будут применяться к планам, созданным после внесения изменений, а на уже существующие планы защиты новые настройки не повлияют.

Настройка параметров резервного копирования по умолчанию

1. Войдите в веб-консоль Кибер Бэкап как администратор.
2. Нажмите **Настройки** → **Настройки системы**.
3. Нажмите **Параметры резервного копирования по умолчанию** для раскрытия списка параметров.
4. Выберите параметр и внесите необходимые изменения.
5. Нажмите кнопку **Сохранить**.

Параметры резервного копирования можно изменять для конкретного плана защиты при его создании или последующем изменении.

Настройка PAM-модуля

Кибер Бэкап поддерживает работу с локальными пользователями и политиками безопасности операционной системы (ОС), установленной на машине сервера управления. Такие параметры, как количество неудачных попыток входа и период последующей блокировки учётной записи, определяются настройками ОС.

Для повышения уровня защищённости в ОС Linux необходимо настроить эти параметры в конфигурационном файле `/etc/pam.d/acronisagent` после установки Кибер Бэкап. При этом на машине, в зависимости от используемого дистрибутива ОС Linux, должен быть установлен один из модулей: **pam_tally2.so** или **pam_faillock.so**.

На машинах под управлением ОС Windows дополнительная настройка не требуется.

Примеры параметров конфигурационного файла

Далее приведены примеры настройки ограничения количества неудачных попыток аутентификации. Настройка конфигурационного файла подсистемы PAM зависит от используемого на машине сервера управления модуля (**pam_tally2.so** или **pam_faillock.so**).

При использовании указанных параметров учётная запись (включая учётную запись с привилегированными правами root) будет заблокирована на 30 секунд после 3-х неудачных попыток входа в веб-консоль Кибер Бэкап.

- Если используется модуль **pam_tally2.so**, добавьте в файл `/etc/pam.d/acronisagent` следующие строки:

  ```
  account required pam_tally2.so
  auth required pam_tally2.so onerr=fail deny=3 unlock_time=30 even_deny_root
  ```

  См. также документацию модуля.

- Если используется модуль **pam_faillock.so**, добавьте в файл `/etc/pam.d/acronisagent` следующие строки:

  ```
  account required        pam_faillock.so
  auth    required        pam_faillock.so authfail deny=3 unlock_time=30 even_deny_root  ¬
  ↪audit root_unlock_time=30
  ```

  См. также документацию модуля.

Предупреждение о редактировании конфигурационного файла

Соблюдайте осторожность при изменении конфигурационных файлов. Блокировка PAM обрабатывается через account_server, а не напрямую. Из-за сложности учёта всех аспектов конфигурации PAM при отображении ошибок входа в систему могут возникать несоответствия.

В случае если пользователь редактировал конфигурационный файл в Кибер Бэкап, все дальнейшие действия он предпринимает на свой страх и риск. Киберпротект не несёт никакой ответственности за любые последствия, возникшие в результате самостоятельного изменения пользователем конфигурационных файлов.

Управление журналом аудита

Журнал аудита отключен по умолчанию. Включить его (как и снова отключить) может администратор с помощью переключателя **Сохранять события аудита** в разделе **НАСТРОЙКИ** → **Аудит** → **Журнал аудита**.

Примечание

При обновлении продукта состояние журнала аудита сохраняется: если он был включен на момент обновления, он останется включен, и наоборот.

Очистка журнала аудита

Очистить журнал аудита можно вручную в разделе **НАСТРОЙКИ** → **Аудит** → **Журнал аудита**:

- щёлкнув **Очистить** возле значения размера журнала;
- отметив флажок **Удалить события аудита без возможности восстановления** при отключении журнала.

Отправка записей журнала аудита на Syslog-сервер

По умолчанию *журнал аудита* хранится в базе данных продукта Кибер Бэкап, однако для централизованного хранения и обработки можно настроить отправку записей журнала аудита на удаленный Syslog-сервер. Для отправки записей может использоваться протокол TCP, UDP или TLS.

Примечание

При *отключении* журнала аудита передача событий на Syslog-сервер прекращается. Настройки, указанные в этом разделе, становятся недоступны.

Предварительные требования для протокола TLS

Если для отправки записей планируется использовать протокол TLS, то перед настройкой должны быть выполнены следующие требования:

- Для сервера управления Кибер Бэкап подготовлены сертификат и закрытый ключ. Сертификат заверен корневым или промежуточным удостоверяющим центром (УЦ).
- Для Syslog-сервера подготовлены сертификат и закрытый ключ. Сертификат заверен корневым УЦ. В поле сертификата `IPAddress` указан IP-адрес Syslog-сервера, или в поле `DNSname` указано его DNS-имя.
- Сертификат и закрытый ключ Syslog-сервера загружены на Syslog-сервер и указаны в его настройках.
- Файл цепочки сертификатов для проверки сертификата сервера управления Кибер Бэкап загружен на Syslog-сервер и указан в его настройках.
- Подготовлен сертификат УЦ, которым был заверен сертификат Syslog-сервера.

Подробные сведения о подготовке сертификатов и настройке Syslog-сервера см. в документации используемого в вашем окружении Syslog-сервера.

Настройка отправки записей на Syslog-сервер

Для настройки выполните следующие действия:

1. Перейдите в раздел **Настройки** → **Аудит** → **Syslog** и переведите переключатель **Передавать журнал аудита на Syslog сервер** в состояние **Вкл**.
2. Укажите параметры подключения к Syslog-серверу:
   - **Адрес удаленного сервера**. IP-адрес или DNS-имя Syslog-сервера.
   - **Порт**. Порт Syslog-сервера.
   - **Протокол**. Протокол для подключения к Syslog-серверу. Можно указать **TCP**, **UDP** или **TLS**.
   - **Формат сообщения**. Формат, в котором будут отправляться сообщения. Можно указать **CEF (RFC 3164)** или **Syslog**.
   - [Только для протокола TLS] **TLS Certificate**. Сертификат сервера управления Кибер Бэкап в формате PEM. Этот сертификат будет использоваться Syslog-сервером для проверки подлинности сервера управления Кибер Бэкап.
   - [Только для протокола TLS] **TLS Key**. Закрытый ключ сертификата сервера управления Кибер Бэкап. Ключ должен быть указан в формате PEM.

- [Только для протокола TLS] **TLS CA Certificate**. Сертификат удостоверяющего центра (УЦ), которым заверен сертификат Syslog-сервера. Сертификат УЦ должен быть указан в формате PEM. Этот сертификат будет использоваться сервером управления Кибер Бэкап при проверке подлинности Syslog-сервера.

3. Нажмите **Отправить тестовое сообщение** и убедитесь, что сообщение получено Syslog-сервером.

> **Примечание**
>
> При использовании протокола UDP сообщение об ошибке отправки будет показано только в том случае, когда хост, на котором установлен Syslog-сервер, недоступен.

4. Нажмите **Сохранить**.

После настройки запись о каждом новом событии будет сохраняться в журнал аудита, а также отправляться на указанный Syslog-сервер.

Управление учетными записями пользователей и отделами организации

Функциональные возможности, описанные в этом разделе, доступны только для *администраторов организации*.

Чтобы получить доступ к этим настройкам, щёлкните **Настройки** → **Учетные записи**.

Отделы и административные учетные записи

Для управления отделами и административными учетными записями в веб-консоли Кибер Бэкап последовательно выберите пункты **Настройки** → **Учетные записи**. На панели **Учетные записи** отображается группа **Организация** с деревом отделов (при их наличии), а также список административных учетных записей на выбранном уровне иерархии.

Отделы

Группа **Организация** автоматически создается при установке сервера управления. При наличии лицензии Кибер Бэкап Расширенная можно создать дочерние группы, называемые отделами, которые, как правило, соответствуют отделам или подразделениям организации, и добавить в них административные учетные записи. Таким способом можно делегировать управление защитой другим пользователям, для которых разрешения на доступ явным образом ограничены соответствующими отделами. Информацию о том, как создать отдел, см. в разделе *Создание отделов*.

Каждый отдел может иметь дочерние отделы. Учетные записи родительского отдела имеют одинаковые права во всех дочерних отделах. Группа **Организация** — это родительская группа верхнего уровня. Учетные записи на этом уровне имеют одинаковые права во всех ее отделах.

Административные учетные записи

Если учетная запись пользователя позволяет ему войти в веб-консоль Кибер Бэкап, то такая учетная запись является административной (управляющей).

В веб-консоли Кибер Бэкап любой пользователь с административной учетной записью может просматривать все элементы на уровне иерархии своего отдела, а также управлять ими. Например, административная учетная запись в *организации* имеет доступ к верхнему уровню, а соответственно, и доступ ко всем отделам этой организации. Напротив, административная учетная запись в определенном *отделе* может получить доступ только к данному отделу и своим дочерним отделам.

Если на машине установлен сервер управления, любому локальному пользователю, пользователю домена или группе пользователей можно предоставить административную учетную запись (поддерживаемые службы каталогов приведены в разделе *Поддерживаемые интеграции со службами каталогов*).

Информацию о добавлении административной учетной записи на сервере управления см. в разделе *Добавление административных учетных записей*.

Роли административной учетной записи

Каждой административной учетной записи назначается роль с предварительно определенными правами, которые необходимы для выполнения определенных заданий. Роли административной учетной записи перечислены ниже:

Администратор

Роль предоставляет полный административный доступ к организации или отделу.

Оператор мониторинга

Роль предоставляет доступ к инструментам мониторинга системы Кибер Бэкап. Роль позволяет создавать виджеты, просматривать уведомления о сбоях, действиях в системе, детали запущенных процессов, список агентов и узлов хранения, разрешает собирать данные диагностики Кибер Бэкап. Эта роль не позволяет изменять или запускать планы резервного копирования и восстанавливать резервные копии.

Только для чтения

Роль предоставляет доступ только для чтения по отношению к веб-консоли Кибер Бэкап. Эта роль позволяет только собирать диагностические данные, такие как системные отчеты. Роль **Только для чтения** не позволяет выполнять обзор резервных копий.

Аудитор

Роль предоставляет доступ только для чтения по отношению к вкладке **Действия** и разделу **Журнал аудита** в веб-консоли Кибер Бэкап. Дополнительную информацию об этом см. в разделах *Панель мониторинга "Действия"* и *Журнал аудита*. Эта роль не позволяет собирать или экспортировать какие-либо данные, включая системную информацию сервера управления.

Все изменения, внесенные в роли, отображаются на вкладке **Действия**.

Наследование ролей

Роли в родительском отделе наследуются дочерними отделами. Если для одной учетной записи пользователя назначены разные роли в родительском и дочернем отделах, эта учетная запись будет иметь обе роли.

Кроме того, роли можно явно назначить определенной учетной записи пользователя или наследовать от

группы пользователей. Таким образом, учетная запись пользователя может иметь специально назначенную роль и наследованную роль.

Если учетная запись пользователя имеет различные роли (назначенные и (или) наследованные), такой пользователь может получить доступ и выполнять действия, разрешенные одной из этих ролей. Например, учетная запись пользователя с назначенной ролью ”Только для чтения” и наследованной ролью **Администратор** будет иметь права администратора.

Важно

В веб-консоли Кибер Бэкап показаны только роли, которые явно назначены для текущего отдела. Никакие возможные отличия от наследованных ролей не отображаются. Во избежание возможных проблем с наследованными ролями настоятельно рекомендуем назначать роли **Администратор**, **Только для чтения** и **Аудитор** отдельным учетным записям или группам.

Администраторы по умолчанию

В ОС Windows

При установке сервера управления на машине происходит следующее:

- Группа пользователей **Acronis Centralized Admins** создается на машине.

  На контроллере домена группе присваивается имя **DCNAME $ Acronis Centralized Admins**. **DCNAME** означает имя NetBIOS контроллера домена.

- Все члены группы **Администраторы** добавляются в группу **Acronis Centralized Admins**. Если данная машина входит в домен, но не является контроллером домена, локальные пользователи (не входят в домен) исключаются. В контроллере домена нет пользователей, не принадлежащих к данному домену.

Acronis Centralized Admins и Администраторы добавляются к серверу управления как **администраторы организации**. Если данная машина входит в домен, но не является контроллером домена, группа **Администраторы** не добавляется. Это необходимо, чтобы локальные пользователи (не входят в домен) не стали администраторами организации.

Можно удалить группу **Администраторы** из списка администраторов организации. Однако группу **Acronis Centralized Admins** невозможно удалить. В том маловероятном случае, когда удалены все администраторы организации, в Windows можно добавить учетную запись в группу **Acronis Centralized Admins**, а затем войти в веб-консоль Кибер Бэкап, используя эту учетную запись.

В ОС Linux

При установке сервера управления на машину пользователь **root** добавляется на сервер управления в качестве **администратора организации**.

Можно добавить других пользователей Linux в список администраторов сервера управления, как описано далее, а затем удалить пользователя **root** из этого списка. В том маловероятном случае, когда удалены все администраторы организации, можно перезапустить службу `acronis_asm`. В результате пользователь **root** будет автоматически заново добавлен в качестве администратора организации.

В Linux вы можете также добавлять пользователей и назначать им роли (подробнее о добавлении пользователей см. раздел *Добавление административных учетных записей*).

Административная учетная запись в нескольких отделах

Для учетной записи можно предоставить права на управление в любом количестве отделов. Для такой учетной записи, а также для административных учетных записей на уровне организации в веб-консоли Кибер Бэкап отображается селектор отдела. Этот селектор позволяет пользователю с этой учетной записью по отдельности просмотреть каждый отдел и выполнить управление.

Учетная запись, которая имеет разрешения на все отделы в организации, не имеет разрешений для организации. Административные учетные записи на уровне организации необходимо явно добавить в группу **Организация**.

Добавление машин в отделы

Когда администратор добавляет машину с помощью веб-интерфейса, она добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, машина добавляется в отдел, выбранный с помощью селектора. Следовательно, администратору необходимо выбрать отдел перед тем, как щёлкнуть **Добавить**.

При локальной установке агентов администратор предоставляет свои учетные данные. Машина добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, установщик попросит выбрать, в какой отдел добавить машину.

См. также

- *Создание отделов*
- *Добавление административных учетных записей*
- *Добавление машин через веб-интерфейс*
- *Установка агентов*

Добавление административных учетных записей

> **Примечание**
>
> Эта функция недоступна в Стандартной редакции.

Порядок добавления учетных записей

1. Щёлкните **Настройки** → **Учетные записи**.

   В веб-консоли отобразится список администраторов сервера управления и дерево отделов (при его наличии).

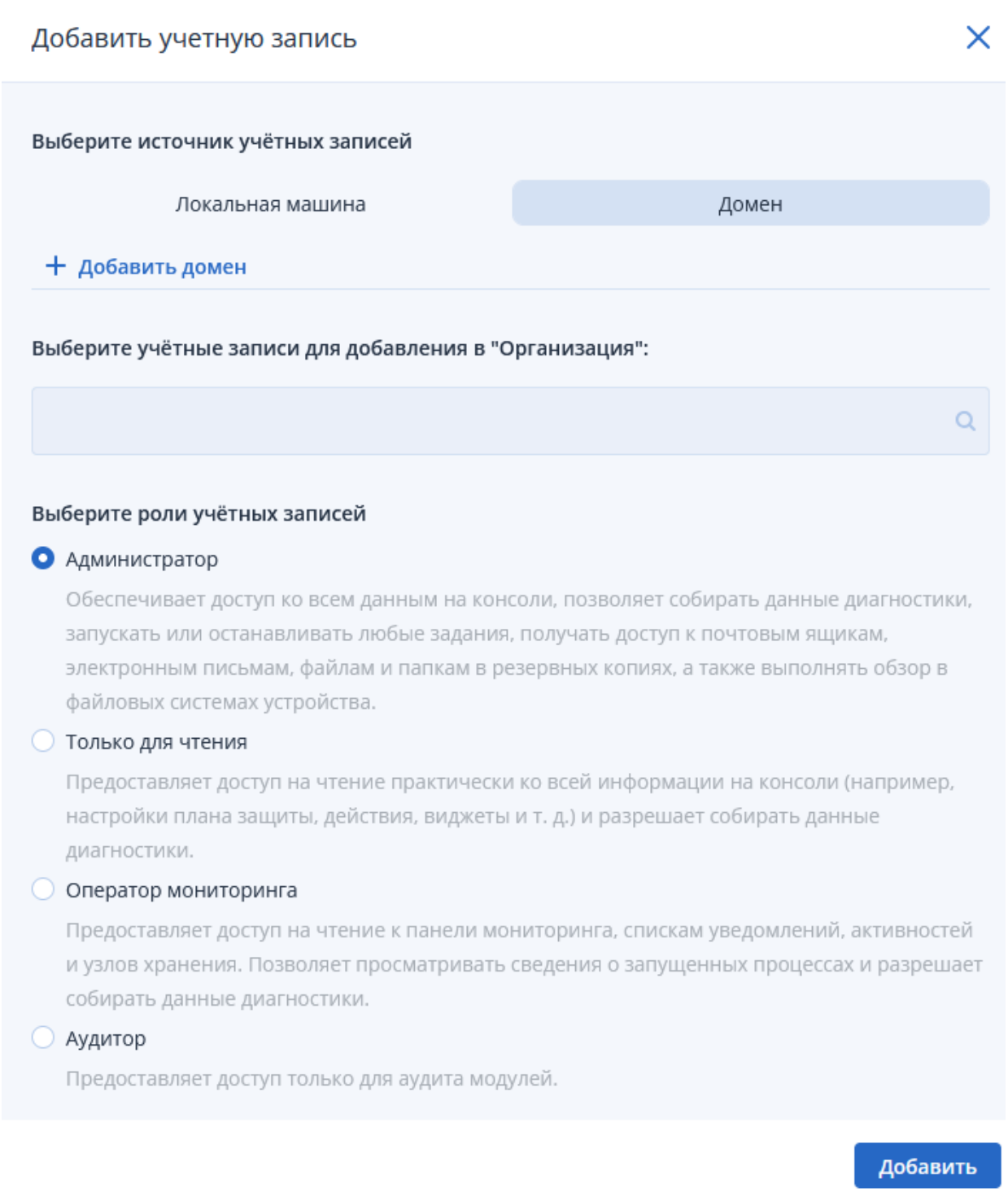
2. Выберите **Организация** или выберите отдел, в котором необходимо добавить административную учетную запись.

3. Нажмите кнопку **Добавить учетную запись**. Вы можете добавить пользователей домена следующих служб каталогов: Active Directory, Samba DC, FreeIPA, ALD Pro, РЕД АДМ.

4. Выберите локальную машину или домен, содержащий учетные записи, которые необходимо добавить.

   > **Примечание**
   >
   > Для добавления учетных записей из домена необходимо сначала добавить сам домен.

   На вкладке **Домен** нажмите **Добавить домен**.



Для добавления домена необходимо создать LDAP-подключение (или LDAPS-подключение). Укажите параметры этого подключения:

- **Имя домена**. Введите полное имя домена службы каталогов, например: `company.ru`.
- **Имя контроллера домена**. Укажите полное DNS-имя или IP-адрес сервера, на котором работает контроллер домена, например: `dc1.company.ru` или `192.168.1.10`.

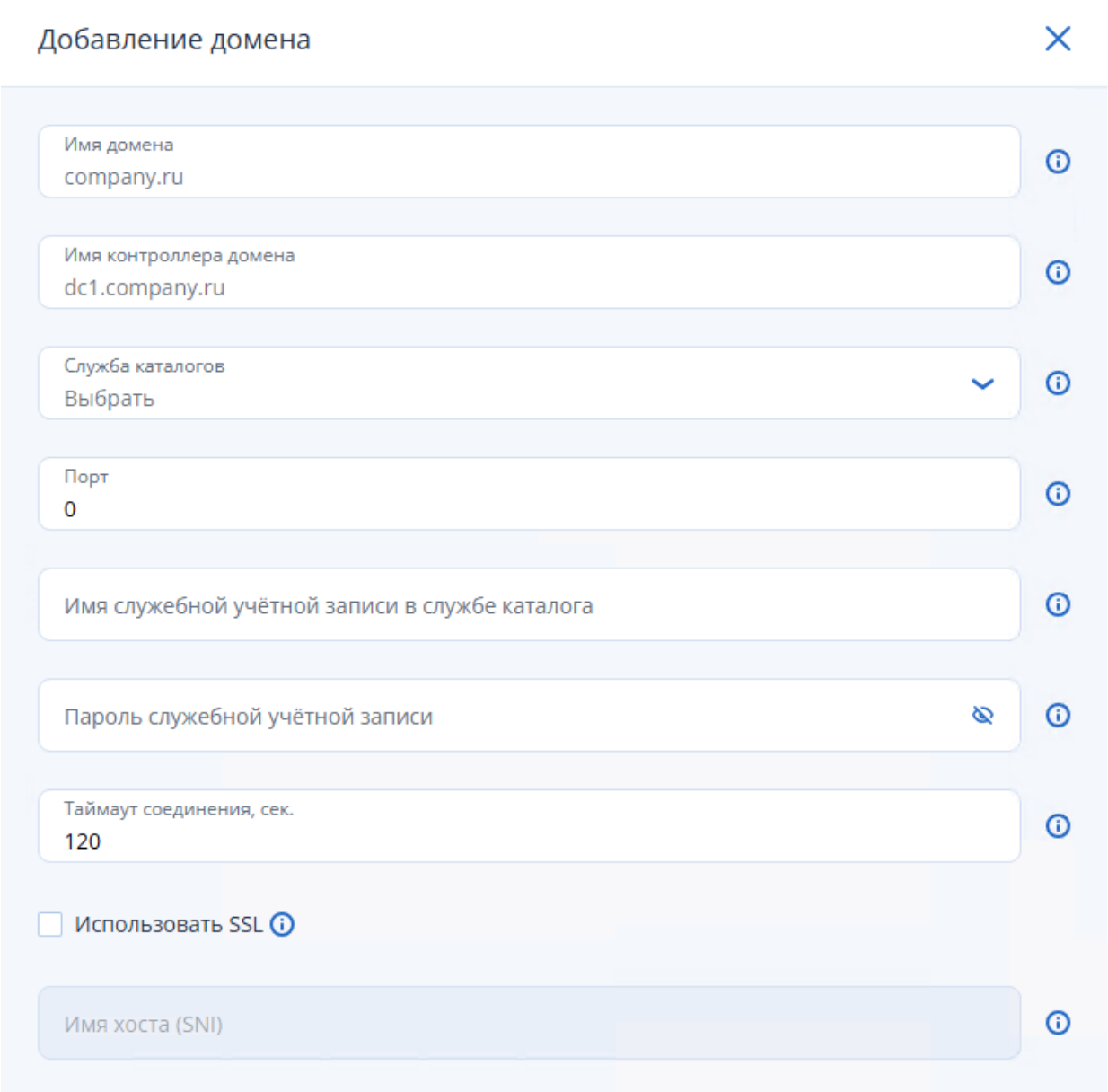
- **Служба каталогов**. Выберите **Active Directory**, **FreeIPA** или **Samba DC**. Для ALD Pro выберите **FreeIPA**, для РЕД АДМ — **Samba DC**.
- **Порт**. Укажите порт подключения к службе каталогов. Для обычного подключения порт по умолчанию — 389. Для подключения, защищенного посредством протокола SSL (LDAPS), порт по умолчанию — 636. Если указать значение `0`, то будет автоматически использован порт по умолчанию в зависимости от типа подключения.
- **Имя служебной учетной записи в службе каталога**. Введите имя учетной записи пользователя (с учетом регистра) для подключения к службе каталогов:
  - для FreeIPA или ALD Pro укажите имя в DN-формате, например: `uid=ivanivanov,cn=users,cn=accounts,dc=company,dc=ru`;
  - для Active Directory, РЕД АДМ или Samba DC укажите имя в формате `COMPANYRU\User` или `User@company.ru`, где `COMPANYRU` — NetBIOS-имя домена службы каталогов, `company.ru` — полное DNS-имя домена службы каталогов, `User` — имя учетной записи пользователя домена службы каталогов.

> **Важно**
>
> Пользователь должен обладать правами на чтение объектов каталога и их свойств.

- **Пароль служебной учетной записи**. Введите пароль от учетной записи для подключения к службе каталогов.
- [Необязательно] **Таймаут соединения, сек**. Введите значение промежутка времени в секундах, в течение которого будет выполняться попытка подключения. По умолчанию это время составляет 120 с.
- **Использовать SSL**. Установите этот флажок, если необходимо использовать протокол SSL для подключения к службе каталогов (LDAPS-подключение).

> **Примечание**
>
> Чтобы использовать это подключение, необходимо настроить SSL-сертификат.

При установке этого флажка также появляется поле **Имя хоста (SNI)**. С его помощью можно задать указанное в сертификате имя хоста (SNI), с которым осуществляется TLS-соединение.

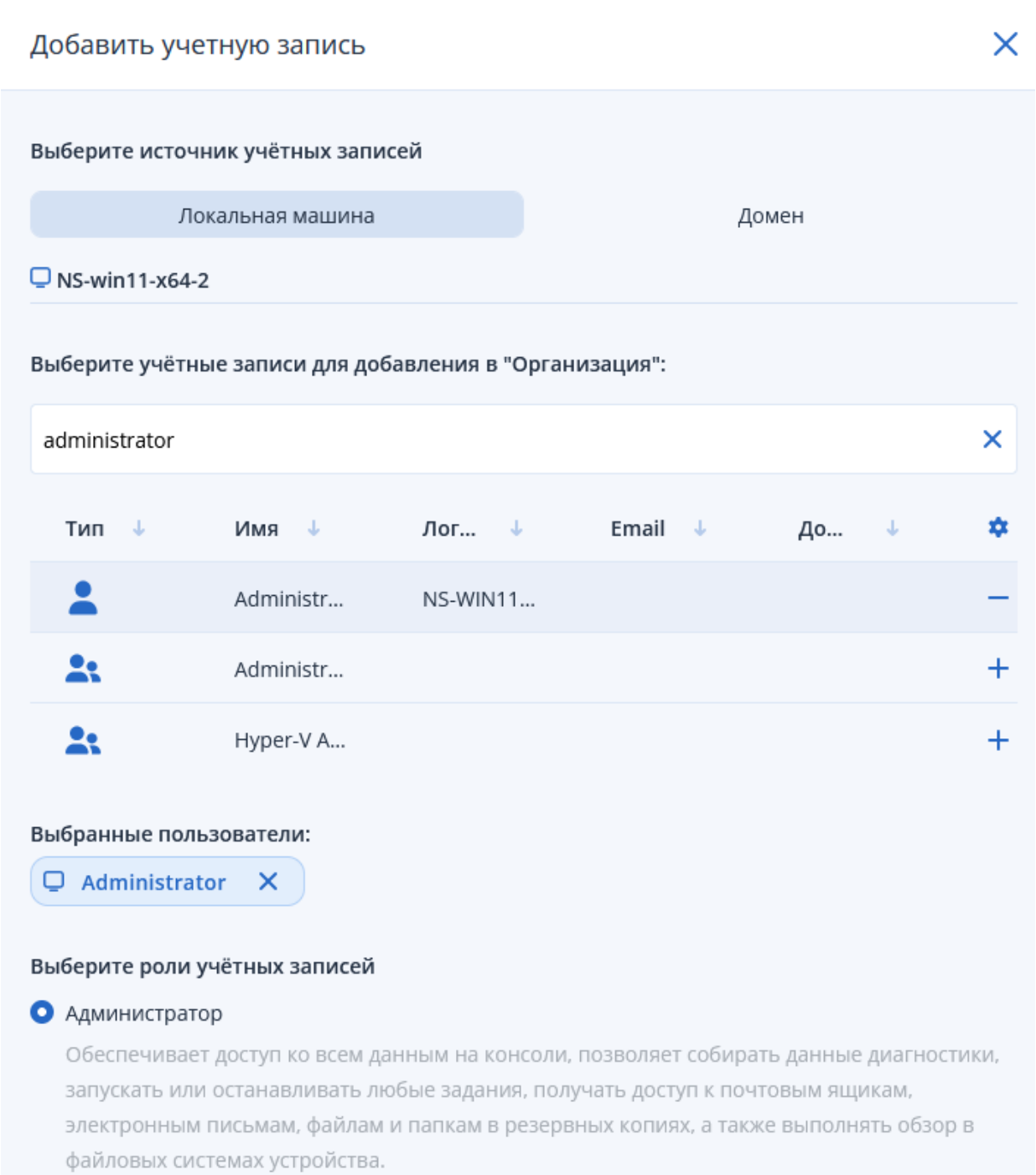


По окончании заполнения полей нажмите **Добавить** и дождитесь завершения процедуры добавления домена. Если процесс добавления не удается завершить успешно, проверьте настройки подключения.

5. Выполните поиск пользователя или группы пользователей. Поиск можно выполнять по следующим данным пользователя: имя пользователя, имя учетной записи, адрес электронной почты.
6. Нажмите ”+” рядом с именем пользователя или группы.

> **Примечание**
>
> Из больших доменов (более 10 000 пользователей) или из доменов с группами высокого уровня вложенности (третьего уровня и выше) рекомендуется добавлять пользователей по одному.

Или просто добавьте группу, в которую входят все необходимые пользователи.



7. Выберите роль для учетной записи. Подробнее о ролях учетной записи см. в разделе *Отделы и административные учетные записи*.
8. Повторите шаги 4-7 для всех пользователей или групп, которые необходимо добавить.
9. По окончании нажмите **Добавить**.
10. [Только в Linux для локальных пользователей] Добавьте имена пользователей в Linux Pluggable

Authentication Module (PAM), как описано ниже.

Порядок добавления имен пользователя в Linux PAM

1. На машине, где работает сервер управления, в текстовом редакторе откройте файл `/etc/security/acronisagent.conf` от имени привилегированного пользователя.
2. В этом файле введите имена пользователей, которые добавлены как администраторы сервера управления. В каждой строке должно быть по одному имени.

   > **Примечание**
   >
   > Указывайте в файле только имена локальных пользователей.

3. Сохраните и закройте файл.

После этого выполните настройку PAM-модуля, как описано в разделе *Настройка PAM-модуля*.

Создание отделов

1. Щёлкните **Настройки** → **Учетные записи**.
2. В веб-консоли отобразится список администраторов сервера управления и дерево отделов (при его наличии).
3. Выберите **Организация** или выберите родительский отдел для нового отдела.
4. Нажмите **Создать отдел**.
5. Укажите имя нового отдела и затем нажмите **Создать**.

Диагностика неполадок

В этом разделе объясняется, как сохранить журналы агента и сервера управления в ZIP-файлы. Эти журналы помогут сотрудникам сопровождения ПО определить проблему в случае неудачного резервного копирования или других операций, не удавшихся по неясной причине.

Получение журналов агентов

1. Выполните одно из следующих действий:
   - В разделе **Устройства** выберите машину, на которой необходимо собрать журналы, и нажмите кнопку **Действия**.
   - В разделе **Настройки** → **Агенты** выберите машину, на которой необходимо собрать журналы, и нажмите кнопку **Сведения**.
2. Нажмите кнопку **Сбор сведений о системе**.
3. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

Получение журналов сервера управления

Выполните следующие действия:

1. В разделе **Панель мониторинга** → **Действия** нажмите кнопку **Собрать сведения о системе сервера управления** в нижней части экрана.
2. В открывшемся окне **Требуется подтверждение** нажмите кнопку **Собрать**.
3. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

Получить журнал сервера управления возможно без установки агентов.