КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 26.03

Руководство пользователя

Редакция: 20.04.2026

Заявление об авторских правах

Содержание

1 Вас приветствует Кибер Бэкап Облачный

Кибер Бэкап Облачный – это комплексное решение для киберзащиты, в котором объединены функции резервного копирования и восстановления, контроля безопасности, мониторинга и отчетности.

Кибер Бэкап Облачный предоставляет один агент защиты, одну легкую в управлении консоль службы, а также один план защиты, охватывающий все аспекты безопасности и защиты данных.

1.1 Основные функции

Кибер Бэкап Облачный предоставляет следующие функции:

- Функции резервного копирования и восстановления позволяют создавать резервные копии физических машин, виртуальных машин и приложений, а также восстанавливать их.
- Автоматическое обнаружение машин предоставляет простой и автоматический способ зарегистрировать большое количество машин и установить агент защиты и дополнительные компоненты.

1.2 Что делает Кибер Бэкап Облачный особенным?

Кибер Бэкап Облачный имеет следующие уникальные функции:

- Защита от возможных проблем после применения исправления путем создания резервных копий перед обновлением.
- Список разрешений для всей компании, который основан на резервных копиях, позволяет избежать ложных выявлений. Эта функция позволяет исключить затратное по времени составление списка доверенных корпоративных приложений, обеспечивает более высокую производительность и повышает скорость обнаружения благодаря улучшенной эвристике.

2 Поддерживаемые функции Кибер Бэкап Облачный по операционным системам

Примечание
В этом разделе содержится информация обо всех функциях Кибер Бэкап Облачный и операционных системах, в которых они поддерживаются. В зависимости от примененной модели лицензирования для некоторых функций может требоваться дополнительное лицензирование.

Функции Кибер Бэкап Облачный поддерживаются в тех операционных системах, которые перечислены в разделе "Поддерживаемые операционные системы и среды" (стр. 16). Дистрибутивы Linux, отличающиеся от перечисленных, могут поддерживаться, но для них не выполнялось тестирование.

Внимание
Функции Кибер Бэкап Облачный поддерживаются только для машин, на которых установлен агент защиты. Для виртуальных машин, защищенных в режиме без использования агента (агент для Hyper-V, агент для VMware, агент для oVirt), поддерживается только резервное копирование.

Функции Кибер Бэкап Облачный	Windows	Linux
Планы защиты по умолчанию		
Сотрудники, которые работают удаленно	Да	Нет
Офисные сотрудники (сторонняя антивирусная программа)	Да	Нет
Офисные сотрудники (антивирусная программа Кибер Бэкап)	Да	Нет
Автоматическое обнаружение и удаленная установка		
Обнаружение на основе сети	Да	Нет
Обнаружение на основе Active Directory	Да	Нет
Обнаружение на основе шаблонов (импорт машин из файла)	Да	Нет
Добавление устройств вручную	Да	Нет
Active Protection		
Обнаружение внедрений в процесс	Да	Нет
Автоматическое обнаружение затронутых файлов из локального кэша	Да	Да
Управление доверенным/блокированным процессом	Да	Нет
Исключения процессов/папок	Да	Да

Защита внешних дисков (жесткие диски (HDD), флэш-накопители, SD-карты)	Да	Нет
Защита сетевых папок	Да	Да
Защита на стороне сервера	Да	Нет
Параметры управления		
Сценарии апсейла для продвижения выпусков Кибер Бэкап Облачный	Да	Да
Централизованная и удаленная веб-консоль управления	Да	Да
Параметры защиты		
Удаленная очистка данных (только в Windows 10)	Да	Нет
Кибер Бэкап Монитор		
Приложение Кибер Бэкап Монитор	Да	Нет

3 Требования к программному обеспечению

3.1 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Яндекс Браузер 21 или более поздней версии;
- Google Chrome 90 или более поздней версии;
- Opera 77 или более поздней версии;
- Mozilla Firefox 86 или более поздней версии;
- Microsoft Edge 112 или более поздней версии.

В других веб-браузерах (включая браузеры Safari, запущенные в других операционных системах) может неправильно отображаться интерфейс пользователя или могут быть недоступны некоторые функции.

3.2 Поддерживаемые операционные системы и среды

Внимание
Поддерживаются только 64-разрядные версии перечисленных операционных систем.

3.2.1 Агент для Windows

- Windows Server 2012 R2 – все выпуски,
- Windows Storage Server 2012 R2, 2016,
- Windows 10 – выпуски Home, Pro, Education, Enterprise, IoT Enterprise и LTSC (прежнее название LTSB),
- Windows 11,
- Windows Server 2016 – все выпуски, кроме Nano Server,
- Windows Server 2019 – все выпуски, кроме Nano Server,
- Windows Server 2022 – все выпуски, кроме Nano Server.

3.2.2 Агент для SQL, агент для Active Directory, агент для Exchange (для резервного копирования базы данных и резервного копирования с поддержкой приложений)

Каждый из этих агентов можно установить на машине с любой из перечисленных выше операционных систем и поддерживаемой версией соответствующего приложения.

3.2.3 Агент для Exchange (для резервного копирования почтового ящика)

- Windows Server 2012 R2 – все выпуски;
- Windows Storage Server 2012 R2, 2016;
- Windows 10 – выпуски Home, Pro, Education и Enterprise;
- Windows 11;
- Windows Server 2016 – все выпуски, кроме Nano Server;
- Windows Server 2019 – все выпуски, кроме Nano Server;
- Windows Server 2022 – все выпуски, кроме Nano Server.

3.2.4 Агент для Oracle

- Windows Server 2012 R2 – выпуски Standard, Enterprise, Datacenter и Web (x64),
- Linux – все ядра и дистрибутивы, которые поддерживаются агентом для Linux (перечислены ниже).

3.2.5 Агент для PostgreSQL

Поддерживаемые операционные системы Windows

- Windows Server 2012 R2
- Windows Server 2016, 2019, 2022
- Windows 10

Поддерживаемые операционные системы Linux с версией ядра от 3.0 и выше

- Astra Linux Special Edition 1.6 и выше
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9
- Альт Сервер 10
- Red Hat Enterprise Linux 7.x и выше
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS
- SUSE Linux Enterprise Server 12 и выше
- Debian 10 и выше
- CentOS 7.x и выше

Поддерживаемые системы управления базами данных

- PostgreSQL 11, 12, 13, 14, 15, 16
- Postgres Pro Standard 11, 12, 13, 14, 15, 16

- Postgres Pro Enterprise 11, 12, 13, 14, 15, 16
- Patroni 3.0-3.2.1
- Proxima DB 2.0, 3.0
- СУБД Jatoba (без поддержки подключения томов и гранулярного восстановления)
- СУБД Tantor

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

3.2.6 Агент для Linux

Linux с версией ядра от 3.0 до 6.14 и glibc версии 2.17 или более поздней, включая следующие дистрибутивы:

- Astra Linux Special Edition 1.6 – 1.7
- Astra Linux Common Edition 2.12
- Альт Сервер 9, 10
- Альт Рабочая станция 9, 10
- Альт 8 СП
- РЕД ОС 7.2, 7.3, 8
- РОСА «КОБАЛЬТ» 7.9, «ХРОМ» 12.5
- Red Hat Enterprise Linux 7.x, 8.0*, 8.1*, 8.2*, 8.3*
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS
- SUSE Linux Enterprise Server 12, 15 — поддерживается в файловых системах, за исключением Btrfs
- SUSE Linux Enterprise Server 15.5
- Debian 10, 11, 12
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3
- Oracle Linux 7.x, 8.0, 8.1, 8.2, 8.3 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel
- AlmaLinux 8.x*, 9.0 – 9.2
- AlterOS 7.5
- ОСнова 2.7 – 2.10

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 привилегированного пользователя): apt-get install rpm

* Конфигурации со Stratis не поддерживаются.

3.2.7 Агент для CommuniGate Pro

- Windows – все ОС, которые поддерживаются агентом для Windows.
- Linux – все ядра и дистрибутивы, которые поддерживаются агентом для Linux.

3.2.8 Агент для VK WorkMail

- Windows – все ОС, которые поддерживаются агентом для Windows.
- Linux – все ядра и дистрибутивы, которые поддерживаются агентом для Linux.

3.2.9 Агент для Kubernetes

Поддерживаемые операционные системы Linux с версией ядра от 3.0 до 6.12

- Astra Linux Special Edition 1.6 - 1.8;
- РЕД ОС 7.2, 7.3, 8;
- РОСА «КОБАЛЬТ» 7.9;
- Альт Сервер 9, 10;
- ОСнова 2.7 - 2.10, 3.0;
- Red Hat Enterprise Linux версии с 7.x по 8.x, кроме конфигураций со Stratis;
- Ubuntu 20.04 LTS, 22.04 LTS;
- SUSE Linux Enterprise Server 12, 15, 15.5 – поддерживается в файловых системах, за исключением Btrfs;
- Debian 10, 11, 12;
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3, 9 Stream, 10 Stream.

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.

3.2.10 Агент для VMware (виртуальное устройство)

Этот агент предоставляется в качестве виртуального устройства для запуска на хосте ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0, 8.0 Update 2

3.2.11 Агент для VMware (Windows)

Этот агент предоставляется в виде приложения Windows для работы в любой из перечисленных выше операционных систем для агента для Windows.

3.2.12 Агент для Hyper-V

- Windows Server 2012 R2 с ролью Hyper-V, включая Server Core
- Microsoft Hyper-V Server 2012 R2
- Windows 10 – выпуски Pro, Education и Enterprise с Hyper-V
- Windows Server 2016 с ролью Hyper-V – все выпуски, кроме Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 с ролью Hyper-V – все выпуски, кроме Nano Server
- Microsoft Hyper-V Server 2019

3.2.13 Агент для oVirt

Red Hat Virtualization 4.2, 4.3, 4.4

3.2.14 Агент для OpenStack (VK Cloud)

- OpenStack от Ussuri до Zed
- VK Cloud 4.0

3.3 Поддерживаемые версии Microsoft SQL Server

Microsoft SQL Server 2012–2019.

3.4 Поддерживаемые версии Microsoft Exchange Server

- **Microsoft Exchange Server 2013** – все выпуски, накопительный пакет обновления 1 (CU1) или более поздней версии.
- **Microsoft Exchange Server 2016** – все выпуски.
- **Microsoft Exchange Server 2019** – все выпуски.

3.5 Поддерживаемые версии Oracle Database

- Oracle Database 11g, все выпуски
- Oracle Database 12c, все выпуски

Поддерживаются только конфигурации с одним экземпляром.

3.6 Поддерживаемые версии SAP HANA

Версия HANA 2.0 SPS 03, установленная в RHEL 7.6 на физической машине 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.

3.7 Поддерживаемые платформы виртуализации

В следующей таблице приведены поддерживаемые платформы виртуализации.

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
Киберпротект		
Кибер Инфраструктура версии с 6.0 по 6.7	+	+
HOSTVM		
HOSTVM 4	+	+
РЕД СОФТ		
РЕД Виртуализация 7.2, 7.3	+	+
РОСА		
ROSA Virtualization 2.0, 2.1, 3.0*	+	+
РУСТЭК		
РУСТЭК 2.6	+	+
zVirt		
zVirt 3.0, 3.1, 3.2, 3.3, 4.0, 4.1, 4.2, Max	+	+
Basis DynamiX Enterprise		
Basis DynamiX Enterprise версии с 3.8.8 по 4.0.0	-	+
Proxmox Virtual Environment		
Proxmox Virtual Environment версии 7.2, 7.3, 7.4, 8.4.0, 9.0.3	+	+
ПК СВ "Брест"		

ПК СВ "Брест", основанный на версии OpenNebula 6.0.0.2	-	+
Альт Виртуализация		
Альт Виртуализация 10, основанная на версии OpenNebula 6.2.0.1	+	+
VK Cloud		
VK Cloud 4.0	+	+
VMware		
Версии VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0, 8.0 Update 2 **Выпуски VMware vSphere:** VMware vSphere Essentials** VMware vSphere Essentials Plus** VMware vSphere Standard** VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (бесплатная низкоуровневая оболочка ESXi)***		+
VMware Server (VMware Virtual Server) VMware Workstation VMware ACE VMware Player		+
Microsoft		
Windows Server 2012 R2 с Hyper-V Microsoft Hyper-V Server 2012 R2 Windows 10 с Hyper-V Windows Server 2016 с Hyper-V – все варианты установки, кроме Nano Server Microsoft Hyper-V Server 2016 Windows Server 2019 с Hyper-V – все варианты установки, кроме Nano Server Microsoft Hyper-V Server 2019	+	+

Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
oVirt		
oVirt 4.2, 4.3, 4.4, 4.5	+	+
OpenStack		
От Ussuri до Zed	+	+
OpenNebula		
OpenNebula версии 6.0.0.2	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		Только полностью виртуализированные (известные также как HVM) гостевые системы. Паравиртуализированные (известные также как PV) гостевые системы не поддерживаются.
Red Hat и Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization (RHV) 4.0, 4.1, 4.2, 4.3, 4.4		+
Виртуальные машины на основе ядра (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Только полностью виртуализированные (известные также как HVM) гостевые системы. Паравиртуализированные

		(известные также как PV) гостевые системы не поддерживаются.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x-20180425.x		+
Amazon		
Экземпляры Amazon EC2		+
Microsoft Azure		
Виртуальные машины Azure		+

* Для ROSA Virtualization 3.0 не поддерживается восстановление ВМ с ОС на основе CentOS в новую ВМ на платформу VMware.

** В этих редакциях транспорт HotAdd для виртуальных дисков поддерживается в vSphere 5.0 и более поздней версии. В версии 4.1 резервные копии могут выполняться медленнее.

*** Резервное копирование на уровне гипервизора не поддерживается для vSphere Hypervisor, так как в этом продукте доступ к удаленному интерфейсу командной строки (RCLI) возможен исключительно в режиме «только для чтения». Агент работает в течение пробного периода vSphere Hypervisor до введения серийного ключа. После введения серийного ключа агент перестает работать.

3.7.1 Ограничения

- **Отказоустойчивые машины**

  Агент для VMware выполняет резервное копирование отказоустойчивой машины, только если в VMware vSphere 6.0 и более поздней версии 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 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** (эта функциональная возможность представлена в VMware vSphere 6.5)
  - 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** (эта функциональная возможность представлена в VMware vSphere 6.5)

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.

3.8 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 на лету. 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.

3.8.1 Типичные правила установки

Настоятельно рекомендуется установить программу шифрования перед установкой агентов защиты.

3.8.2 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.

3.8.3 Общее правило резервного копирования

Позволяет выполнить резервное копирование на уровне дисков операционной системы.

3.8.4 Процедуры восстановления для конкретных программ

3.8.4.1 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.

3.8.4.2 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, как описано в статье базы знаний Майкрософт.

4 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 (загрузочные носители поддерживают только восстановление). Ограничения применяются как к агентам, так и к загрузочным носителям.

<table>
<tr><th rowspan="2">Файловая система</th><th colspan="2">Поддержка</th><th rowspan="2">Ограничения</th></tr>
<tr><th>Агенты</th><th>Загрузочные носители для Windows и Linux</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Все агенты</td><td>+</td><td rowspan="3">Без ограничений</td></tr>
<tr><td>NTFS</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td></tr>
<tr><td>JFS</td><td rowspan="3">Агент для Linux</td><td>+</td><td rowspan="2">• Файлы невозможно исключить из резервной копии диска
• Невозможно включить быстрое инкрементное/дифференциальное резервное копирование</td></tr>
<tr><td>ReiserFS3</td><td>+</td></tr>
<tr><td>ReiserFS4</td><td>+</td><td rowspan="3">• Файлы невозможно исключить из резервной копии диска
• Невозможно включить быстрое инкрементное/дифференциальное резервное копирование
• Невозможно изменить размер томов при выполнении восстановления</td></tr>
<tr><td>ReFS</td><td rowspan="2">Все агенты</td><td>+</td></tr>
<tr><td>XFS</td><td>+</td></tr>
<tr><td>Linux SWAP</td><td>Агент для Linux</td><td>+</td><td>Без ограничений</td></tr>
<tr><td>exFAT</td><td>Все агенты</td><td>+
Если резервная копия хранится в файловой системе exFAT, загрузочный носитель невозможно использовать для восстановления.</td><td>• Поддерживается только резервное копирование дисков/томов
• Файлы невозможно исключить из резервной копии
• Отдельные файлы невозможно восстановить из резервной копии</td></tr>
</table>

Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами (например, Btrfs). 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.

4.0.1 Дедупликация данных

ОС Windows Server 2012 и более поздних версий 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 с резервной копии диска запустите виртуальную машину с резервной копии или подключите резервную копию на машине под управлением Windows Server 2012 или более поздней версии и скопируйте файлы с подключенного тома.

Функциональные средства дедупликации данных Windows Server не имеют никакого отношения к функциональным средствам дедупликации ПО Кибер Бэкап Облачный.

5 Активация учетной записи

После того как администратор создаст для вас учетную запись, на ваш адрес электронной почты будет отправлено сообщение. Это сообщение содержит следующую информацию:

- **Ваше имя для входа.** Имя пользователя, которое используется для входа в службу. Имя входа также отображается на странице активации учетной записи.
- **Кнопка активации учетной записи.** Щелкните эту кнопку и задайте пароль для учетной записи. Убедитесь, что пароль содержит не менее девяти символов.

  Если администратор включил двухфакторную проверку подлинности, вам будет предложено настроить двухфакторную проверку подлинности для своих учетных записей.

5.1 Двухфакторная проверка подлинности

Двухфакторная проверка подлинности обеспечивает дополнительную защиту от несанкционированного доступа к учетной записи. Если настроена двухфакторная проверка подлинности, то для входа в консоль службы сначала необходимо ввести пароль (первый фактор), а затем – одноразовый код (второй фактор). Одноразовый пароль генерируется в специальном приложении, которое необходимо установить на мобильный телефон или другое устройство, которое вам принадлежит. Даже если кто-то найдет ваше имя входа и пароль, они не смогут выполнить вход без устройства второго фактора.

Одноразовый код генерируется на основе текущего времени на устройстве, а секретный ключ предоставляется службой Кибер Бэкап Облачный в виде QR-кода или буквенно-цифрового кода. При первом входе необходимо ввести этот секретный ключ в приложение проверки подлинности.

Порядок настройки двухфакторной проверки подлинности для вашей учетной записи

1. Выберите устройство второго фактора.

   Обычно это мобильный телефон, однако для этой можно использовать планшет, ноутбук или настольный ПК.
2. Убедитесь, что время на устройстве установлено правильно и соответствует фактическому. Убедитесь, что устройство блокируется по истечении определенного периода неактивности.
3. Установите приложение проверки подлинности на устройство. Рекомендуется использовать приложения Google Authenticator или Microsoft Authenticator.
4. Откройте страницу входа в консоль службы и задайте пароль.

   В консоли службы отображается QR-код и буквенно-цифровой код.
5. Сохраните QR-код и буквенно-цифровой код любым удобным способом (например, распечатайте снимок экрана, запишите код или сохраните снимок экрана в облачном хранилище данных). При утрате устройства второго фактора эти коды позволят вам сбросить двухфакторную проверку подлинности.
6. Откройте приложение проверки подлинности и выполните одно из следующих действий:
   - Отсканируйте QR-код.
   - Вручную введите буквенно-цифровой код в приложение.

Приложение проверки подлинности генерирует одноразовый код. Новый код генерируется каждые 30 секунд.

7. Вернитесь на страницу входа в консоль службы и введите сгенерированный вход.

   Одноразовый код действует в течение 30 секунд. По истечении 30 секунд используйте следующий сгенерированный код.

При следующем входе можно установить флажок **Сделать браузер доверенным**. После этого одноразовый код не потребуется для входа с использованием браузера на этой машине.

5.1.1 Что если...

5.1.1.1 ...потеряно устройство второго фактора?

Если есть доверенный браузер, с него можно выполнить вход. Тем не менее, на новом устройстве повторите действия 1-3 и 6-7 описанной выше процедуры и сохраните QR-код или буквенно-цифровой код.

Если вы не сохранили код, обратитесь к администратору или поставщику услуг с просьбой сбросить двухфакторную проверку подлинности для вашей учетной записи, а затем повторите шаги 1-3 и 6-7 вышеуказанной процедуры, используя новое устройство.

5.1.1.2 ...мне нужно использовать другое устройство второго фактора?

При входе щелкните ссылку **Сбросить настройки двухфакторной проверки подлинности**, подтвердите операцию вводом одноразового пароля, а затем повторите описанную выше процедуру на новом устройстве.

6 Доступ к службе Кибер Бэкап Облачный

После активации учетной записи можно войти в службу Кибер Бэкап Облачный.

Порядок входа в службу Кибер Бэкап Облачный

1. Перейдите на страницу входа в службу Кибер Бэкап Облачный. Адрес страницы входа был указан в сообщении электронной почты со сведениями об активации.
2. Введите имя пользователя и щелкните **Далее**.
3. Введите пароль и щелкните **Далее**.
4. Если в службе Кибер Бэкап Облачный вы имеете роль администратора, щелкните **Кибер Бэкап**.

   Пользователи без роли администратора входят непосредственно на эту консоль службы.

Время ожидания для консоли службы составляет 24 часа для активных сеансов и 1 час для неактивных сеансов.

Порядок сброса пароля

1. Перейдите на страницу входа в службу Кибер Бэкап Облачный.
2. Введите учетные данные и щелкните **Далее**.
3. Щелкните **Забыли пароль?**
4. Подтвердите запрос дальнейших инструкций, щелкнув **Отправить**.
5. Следуйте инструкциям в полученном электронном письме.
6. Задайте новый пароль. Убедитесь, что пароль содержит не менее восьми символов.

Можно изменить язык веб-интерфейса, щелкнув значок учетной записи в правом верхнем углу.

Если у вас есть подписка на другие службы, кроме **Кибер Бэкап**, переключаться между ними можно с помощью значка  в правом верхнем углу. Администраторы также могут использовать этот значок для переключения на портал управления.

Если у вас есть подписка на любой из выпусков Кибер Бэкап Облачный, в консоли службы можно отправить отзыв о продукте. В левом меню навигации щелкните **Отправить отзыв**, заполните поля, вложите файлы (если есть) и щелкните **Отправить**.

7 Установка программного обеспечения

7.1 Какой агент необходим?

Выбор агента зависит от того, для какого именно объекта нужно создать резервную копию. В таблице ниже приведены основные сведения, которые помогут вам принять решение.

Обратите внимание, что в ОС Windows агент для Exchange, агент для SQL, агент для Active Directory и агент для Oracle требуют установленного агента для Windows. Например, установив агент для SQL, вы также сможете создавать резервные копии всей машины, на которой установлен агент.

Рекомендуется установить агент для Windows, если вы решите установить агент для VMware (Windows) и агент для Hyper-V.

В ОС Linux для агента для Oracle требуется установленный агент для Linux (64-разрядная версия). Для всех трех агентов используется один установщик.

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?
Физические машины		
Физические машины под управлением Windows	Агент для Windows	На машину, резервная копия которой будет создана.
Физические машины под управлением ОС Linux	Агент для Linux	
Приложения		
Базы данных PostgreSQL	Агент для PostgreSQL	На машину с сервером PostgreSQL или на другую машину.
Базы данных SQL	Агент для SQL	На машину с сервером Microsoft SQL Server.
Базы данных Exchange	Агент для Exchange	На машине с ролью почтового ящика Microsoft Exchange Server.*
Машины с доменными службами Active Directory	Агент для Active Directory	На контроллер домена.
Машины под управлением Oracle Database	Агент для Oracle	На машине с запущенной Oracle Database.
Виртуальные машины		
Виртуальные машины VMware ESXi	Агент для VMware (Windows)	На машине Windows с сетевым доступом к vCenter Server и хранилищу виртуальных

		машин.**
	Агент для VMware (виртуальное устройство)	На хосте ESXi.
Виртуальные машины Hyper-V	Агент для Hyper-V	На хост Hyper-V.
Виртуальные машины Red Hat Virtualization (с управлением oVirt)	Агент для oVirt (виртуальное устройство)	На хосте Red Hat Virtualization.
Виртуальные машины на хосте Citrix XenServer		
Red Hat Virtualization (RHV/RHEV)		
Виртуальные машины на основе ядра (KVM)		
Виртуальные машины Oracle		
Виртуальные машины Nutanix AHV		

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

**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 «Агент для VMware – резервное копирование без использования локальной сети».

7.2 Системные требования для агентов

Агент	Для установки необходимо место на диске
Агент для Windows	1,2 ГБ
Агент для Linux	2 ГБ
Агент для SQL и агент для Windows	1,2 ГБ
Агент для Exchange и агент для Windows	1,3 ГБ
Агент службы предотвращения утечки данных	500 МБ

Агент для Active Directory и агент для Windows	2 ГБ
Агент для VMware и агент для Windows	1,5 ГБ
Агент для Hyper-V и агент для Windows	1,5 ГБ
Агент для Oracle и агент для Windows	2,2 ГБ
Агент для Oracle и агент для Linux	2 ГБ

Для выполнения операций резервного копирования требуется 1 ГБ ОЗУ на каждый терабайт резервной копии. Потребление памяти может меняться в зависимости от объема и типа данных, обрабатываемых агентами.

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

7.3 Подготовка

7.3.1 Шаг 1

Выберите агент в зависимости от того, для какого именно объекта нужно создать резервную копию. Дополнительную информацию о возможных вариантах выбора см. в разделе Какой агент необходим?

7.3.2 Шаг 2

На жестком диске должно быть достаточно свободного пространства для установки агента. Более подробную информацию о необходимом объеме пространства см. в разделе "Системные требования для агентов" (стр. 34).

7.3.3 Шаг 3

Загрузите программу установки. Чтобы найти ссылки загрузки, последовательно выберите пункты **Все устройства** > **Добавить**.

На странице **Добавить устройства** есть ссылки на веб-установщики для всех агентов, которые устанавливаются в ОС Windows. Веб-установщик – это небольшой исполняемый файл, который загружает основную программу установки из Интернета и сохраняет ее в качестве временного файла. Этот файл удаляется сразу же после установки.

Чтобы сохранить программы установки локально, загрузите пакет со всеми агентами для установки в Windows по ссылке в нижней части страницы **Добавить устройства**. Эти пакеты позволяют настроить список компонентов для установки. С помощью этих пакетов также можно настроить автоматическую установку (например, с использованием групповой политики). Этот расширенный сценарий описан в разделе "Развертывание агентов с использованием групповой политики" (стр. 105).

Установка в ОС Linux выполняется с помощью обычных программ установки.

Всем программам установки необходимо подключение к Интернету для регистрации машины в службе Кибер Бэкап Облачный. Если подключение отсутствует, выполнить установку не удастся.

7.3.4 Шаг 4

Для работы функций Кибер Бэкап Облачный требуется распространяемый пакет Microsoft Visual C++ 2017. Проверьте наличие этого компонента на машине или установите его перед установкой агента. После установки Microsoft Visual C++ может потребоваться перезагрузка. Распространяемый пакет Microsoft Visual C++ можно скачать по ссылке.

7.3.5 Шаг 5

Убедитесь, что брандмауэры и другие компоненты системы безопасности сети (например, прокси-сервер) не блокируют входящие и исходящие подключения через следующие TCP-порты:

- **443** и **8443** – эти порты используются для доступа к консоли службы, регистрации агентов, скачивания сертификатов, авторизации пользователей, а также скачивания файлов из облачного хранилища данных;
- **7770...7800** – агенты используют эти порты для обмена данными с сервером управления резервным копированием;
- **44445 и 55556**: агенты используют эти порты для передачи данных при выполнении резервного копирования и восстановления.

Если в вашей сети включен прокси-сервер, см. раздел Настройки прокси-сервера, который поможет понять, нужно ли задавать эти настройки на каждой машине с запущенным агентом защиты.

Для управления установленным в облаке агентом скорость подключения к Интернету должна быть не меньше 1 Мбит/с (не путать со скоростью передачи данных, приемлемой для резервного копирования в облако). Примите это во внимание при использовании технологии подключения с небольшой пропускной способностью (например, ADSL).

7.3.5.1 Для резервного копирования и репликации виртуальных машин VMware необходимы порты TCP

- **TCP 443**. Агент для VMware (как в ОС Windows, так и на виртуальном устройстве) подключается к этому порту на хосте ESXi (сервере vCenter) для выполнения операций управления виртуальной машиной, таких как создание, обновление и удаление виртуальных машин в vSphere при выполнении операций резервного копирования, восстановления и репликации виртуальных машин.
- **TCP 902**. Агент для VMware (как в ОС Windows, так и на виртуальном устройстве) подключается к этому порту на хосте ESXi для установки подключения через NFC для чтения/записи данных на дисках виртуальной машины при выполнении операций резервного копирования, восстановления и репликации виртуальных машин.

- **TCP 3333**. Если агент для VMware (виртуальное устройство) выполняется на целевом хосте (в целевом кластере) ESXi для репликации виртуальной машины, трафик операции репликации виртуальной машины не поступает непосредственно на порт 902 хоста ESXi. Вместо этого трафик поступает с исходного агента для VMware на TCP-порт 3333 на агенте для VMware (виртуальном устройстве) на целевом хосте (кластере) ESXi.

  Исходный агент для VMware, который считывает данные с оригинальных дисков виртуальной машины, может быть в любом ином месте. Он может работать как на виртуальном устройстве, так и в ОС Windows.

  Служба, которая отвечает за прием данных репликации виртуальной машины на целевом агенте для VMware (виртуальном устройстве), называется "Replica disk server" ("Сервер диска реплики"). Эта служба отвечает за методы оптимизации глобальной сети, такие как сжатие трафика и дедупликация при репликации виртуальной машины, включая заполнение реплики. Если на целевом хосте не выполняется агент для VMware (виртуальное устройство), эта служба недоступна, поэтому сценарий заполнение реплики не поддерживается.

7.3.6 Шаг 6

Проверьте, что локальные порты машины, на которой вы планируете установить агент Кибер Бэкап, не используются другими процессами.

- 127.0.0.1:9999
- 127.0.0.1:43234
- 127.0.0.1:9850

Примечание
Не нужно открывать их в брандмауэре.

Служба Active Protection использует TCP-порт 6109. Убедитесь, что он не используется другим процессом.

7.3.6.1 Изменение портов, используемых агентом Кибер Бэкап

Некоторые порты, необходимые для агента Кибер Бэкап, могут использоваться другими приложениями в вашей среде. Во избежание конфликтов можно изменить порты, которые по умолчанию используются агентом Кибер Бэкап. Для этого внесите изменения в указанные ниже файлы.

- В ОС Linux: /opt/Acronis/etc/aakore.yaml
- В ОС Windows: \ProgramData\Acronis\Agent\etc\aakore.yaml

7.4 Пакеты 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.
- Библиотеки libelf-dev, libelf-devel или elfutils-libelf-devel для сборки ядер не ниже 4.15 и настроены с параметром CONFIG_UNWINDER_ORC=y. Для некоторых дистрибутивов, например Fedora 28, их необходимо установить отдельно от заголовков ядра.

Имена этих пакетов зависят от используемого дистрибутива Linux.

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

7.4.1 Установлены ли необходимые пакеты?

Чтобы проверить, установлены ли пакеты, сделайте 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 следующую команду, 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, CentOS и Fedora 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. В Red Hat Enterprise Linux, CentOS и Fedora 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.

7.4.2 Установка пакетов из репозитория

В следующей таблице указано, как установить необходимые пакеты в различных дистрибутивах Linux.

Дистрибутив Linux	Имена пакетов	Как установить
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Программа установки загрузит и установит пакеты автоматически по вашей подписке на Red Hat.
	perl	Выполните следующую команду: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	Программа установки загрузит и установит пакеты автоматически.
	perl	Выполните следующую команду: `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		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 gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux OpenSUSE	**kernel-source** **gcc** **make** **perl**	sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper install perl

Пакеты будут загружены из репозитория дистрибутива и установлены.

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

7.4.3 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, CentOS и Fedora выполните следующую команду как привилегированный пользователь:

  ```
  rpm -ivh ФАЙЛ_ПАКЕТА1 ФАЙЛ_ПАКЕТА2 ФАЙЛ_ПАКЕТА3
  ```

- В Ubuntu выполните следующую команду:

  ```
  sudo dpkg -i ФАЙЛ_ПАКЕТА1 ФАЙЛ_ПАКЕТА2 ФАЙЛ_ПАКЕТА3
  ```

7.5 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.

Поскольку на этапе установки агент регистрируется в облаке, во время установки или заранее необходимо указать параметры прокси-сервера.

7.5.1 В ОС 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 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.
9. Откройте файл **%programdata%\Acronis\Agent\etc\aakore.yaml** в текстовом редакторе.
10. 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
```

11. Вместо proxy_login и proxy_password укажите учетные данные прокси-сервера, а вместо proxy_address:port – адрес и номер порта прокси-сервера.
12. В меню **Пуск** щелкните **Выполнить**, введите **cmd** и щелкните **OK**.
13. Перезапустите службу aakore, выполнив следующие команды:

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

14. Перезапустите агент, выполнив следующие команды:

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

7.5.2 В ОС 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.

Именение 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 туда следующие строки:

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

8. Вместо proxy_login и proxy_password укажите учетные данные прокси-сервера, а вместо proxy_address:port — адрес и номер порта прокси-сервера.
9. Перезапустите службу aakore, выполнив следующую команду:

   ```
   sudo service aakore restart
   ```

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

    ```
    sudo service acronis_mms restart
    ```

7.5.3 На загрузочном носителе

Если используется загрузочный носитель, вам может потребоваться доступ к облачному хранилищу с использованием прокси-сервера. Чтобы указать настройки прокси-сервера, выберите пункты **Инструменты** > **Прокси-сервер** и укажите имя хоста или IP-адрес, порт и учетные данные прокси-сервера.

7.6 Установка агентов

Агенты можно установить на машинах под управлением любой операционной системы, указанной в разделе Поддерживаемые операционные системы и среды. Операционные системы, которые поддерживают функции Кибер Бэкап Облачный, указаны в разделе Поддерживаемые функции Кибер Бэкап Облачный по операционным системам.

Перед установкой агента убедитесь в соответствии машины системным требованиям.

7.6.1 В Windows

Для установки агента на машине с ОС Windows выполните следующие действия:

1. Убедитесь в том, что машина подключена к Интернету.
2. Войдите как администратор и запустите программу установки.
3. [Необязательно] Щёлкните **Настройка параметров установки** и внесите изменения (при необходимости):
   - Отметьте флажками те компоненты, которые необходимо установить:
     - **Агент для Windows**;
     - **Агент для VMware (Windows)**;
     - **Агент для Exchange**;
     - **Агент для Oracle**;
     - **Агент для PostgreSQL**;
     - **Агент для VK WorkMail**;
     - **Агент для CommuniGate Pro**;
     - **LDAP Коннектор**;
     - **Мастер создания загрузочных носителей;**
     - **Программа командной строки**;
     - **Мониторинг Защиты Данных**.
   - Выберите метод регистрации машины в службе Кибер Бэкап Облачный. Можно изменить параметр **Использовать консоль службы** (по умолчанию) на **Использовать учётные данные** или **Использовать маркер регистрации** (см. раздел "Управление маркерами регистрации" (стр. 113)).

- Укажите путь установки.
- Укажите учётную запись, с которой будет запускаться служба агента. Дополнительную информацию см. в разделе "Изменение учетной записи входа на машинах Windows" (стр. 46).
- Проверьте или измените имя хоста или IP-адрес, порт и учётные данные прокси-сервера. Если прокси-сервер включён в Windows, он определяется и используется автоматически.

4. Нажмите **Установить**.
5. [Только при установке агента для VMware] Укажите адрес и учётные данные доступа для сервера vCenter Server или автономного хоста ESXi, для которых агент будет создавать резервные копии виртуальных машин, и нажмите кнопку **Готово**. Рекомендуем использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями на хосте vCenter Server или ESXi.
6. [Только при установке на контроллер домена] Укажите учётную запись пользователя, под которой будет работать служба агента, и нажмите кнопку **Готово**. В целях безопасности программа установки не может автоматически создавать учётные записи на контроллере домена.
7. Если на шаге 3 вы не меняли способ регистрации по умолчанию **Использовать консоль службы**, дождитесь появления экрана регистрации и перейдите к следующему шагу. Если нет, дополнительных действий не требуется.

7.6.2 В ОС Linux

7.6.2.1 Подготовка к установке в ОС Astra Linux SE

Перед установкой агента в ОС Astra Linux SE выполните следующие шаги:

Примечание
Предполагается, что включён режим замкнутой программной среды.

1. Распакуйте дистрибутив:

```
tar --xattrs --xattrs-include=* -xvf Backup_AgentForLinux_x86_64.bin.tar
```

2. Запустите файл установки с правами привилегированного пользователя:

```
./Backup_AgentForLinux_x86_64.bin
```

3. Обновите образы initramfs:

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

4. Перезагрузите систему.

7.6.2.2 Установка

Для установки агента для Linux выполните следующие шаги:

1. Убедитесь в том, что машина подключена к Интернету.
2. Запустите файл установки от имени суперпользователя.

   Если в сети включен прокси-сервер, при запуске файла укажите имя хоста или IP-адрес и порт сервера в следующем формате: --http-proxy-host=АДРЕС --http-proxy-port=ПОРТ --http-proxy-login=ИМЯ ВХОДА--http-proxy-password=ПАРОЛЬ.

   Чтобы изменить метод регистрации машины в службе Кибер Бэкап Облачный, используемый по умолчанию, запустите установочный файл с одним из следующих параметров:

   - --register-with-credentials: запрашивать имя пользователя и пароль при установке;
   - --token=STRING: использовать маркер регистрации;
   - --skip-registration: пропустить регистрацию.
3. Отметьте флажками те компоненты, которые необходимо установить:
   - **Агент для Linux**;
   - **Агент для CommuniGate Pro**;
   - **Агент для Oracle**;
   - **Агент для PostgreSQL**;
   - **Агент для VK WorkMail**;
   - **Агент для Kubernetes**;
   - **LDAP Коннектор**.

   Для агентов для Oracle, PostgreSQL, VK WorkMail, CommuniGate Pro также требуется установленный агент для Linux.
4. Если вы оставили метод регистрации по умолчанию в шаге 2, перейдите к следующему шагу. В противном случае введите имя пользователя и пароль для службы Кибер Бэкап Облачный или дождитесь регистрации машины с использованием маркера.
5. 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.
6. 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.**

7.6.3 Изменение учетной записи входа на машинах Windows

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 в контроллере 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.

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 (в Windows XP и Server 2003, %ALLUSERSPROFILE%\Application Data\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 оборудования

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 **Администрирование** (или щелкните Win+R, введите **control admintools** и нажмите клавишу "ВВОД"), затем откройте **Локальная политика безопасности**.
3. Разверните **Локальные политики** и щелкните **Назначение прав пользователя**.
4. В правой панели щелкните правой кнопкой мыши **Вход в качестве службы** и выберите **Свойства**.
5. Чтобы добавить нового пользователя, нажмите кнопку **Добавление пользователя или группы...**.
6. В окне **выбора пользователей, компьютеров, учетных записей служб или групп** найдите пользователя, которого необходимо ввести, и щелкните **OK**.
7. Чтобы сохранить изменения, щелкните **OK** в разделе "Свойства" (**Вход в качестве службы**).

Внимание
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.

7.7 Автоматическая установка или автоматическое удаление

7.7.1 Автоматическое установка или автоматическое удаление в Windows

В этом разделе показано, как установить или удалить агенты защиты 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 «Установка агентов с помощью 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.

7.7.1.1 Создание MST-преобразования и извлечение пакетов установки

1. Войдите как администратор и запустите программу установки.
2. Щелкните **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. В разделе **Настройки регистрации** выберите **Использовать учетные данные** или **Использовать маркер регистрации**. Дополнительную информацию о создании маркера регистрации см. в разделе "Управление маркерами регистрации" (стр. 113).
5. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл.
6. Щелкните **Продолжить**, а затем выберите папку, в которой будет создан файл преобразования .mst и распакованы пакеты установки .msi и .cab.
7. Нажмите кнопку **Создать**.

7.7.1.2 Установка продукта с использованием преобразования MST

В командной строке выполните указанную ниже команду.

Шаблон команды:

```
msiexec /i <имя пакета> TRANSFORMS=<имя преобразования>
```

В этой формуле:

- <имя пакета> – это имя MSI-файла.
- <имя преобразования> – это имя преобразования.

Пример команды:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

7.7.1.3 Установка или удаление продукта с указанием параметров вручную

В командной строке выполните указанную ниже команду.

Шаблон команды (установка):

```
msiexec /i <имя пакета><ПАРАМЕТР 1>=<значение 1> ... <ПАРАМЕТР N>=<значение n>
```

<имя пакета> – это имя MSI-файла. Все доступные параметры и их значения описаны в разделе "Параметры автоматической установки или автоматического удаления".

Шаблон команды (удаление):

```
msiexec /x <package name> <ПАРАМЕТР 1>=<значение 1> ... <ПАРАМЕТР N>=<значение n>
```

Пакет .msi должен иметь ту же версию, что и продукт, который необходимо удалить.

7.7.1.4 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 в документации Майкрософт.

Параметры установки

Базовые параметры

ADDLOCAL=<список компонентов>

Компоненты для установки, разделенные запятыми и без символов пробела. Все указанные компоненты необходимо извлечь из программы установки до установки.

Полный список компонентов приведен ниже:

Компонент	Необходимо установить вместе с	Разрядность	Имя / описание компонента
MmsMspComponents		64-разрядная	Компоненты Core для агентов
BackupAndRecoveryAgent	MmsMspComponents	64-разрядная	Агент для Windows
ArxAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для Exchange
ArsAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для SQL
ArsAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для Exchange
ARADAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для Active Directory
ActiveProtection	MmsMspComponents	64-разрядная	Агент службы активной зщиты
OracleAgentFeature	BackupAndRecoveryAgent	64-разрядная	Агент для

			Oracle
PostgreSqlAgentFeature	MmsMspComponents	64-разрядная	Агент для PostgreSQL
AcronisESXSupport	MmsMspComponents	64-разрядная	Агент для VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	64-разрядная	Агент для Hyper-V
CommunigateAgentFeature	MmsMspComponents	64-разрядная	Агент для Communigate Pro
WorkmailAgentFeature	MmsMspComponents	64-разрядная	Агент для WorkMail
CommandLineTool		64-разрядная	Программа командной строки
TrayMonitor	BackupAndRecoveryAgent	64-разрядная	Cyber Protection Monitor
BackupAndRecoveryBootableComponents;		64-разрядная	Мастер создания загрузочных носителей

TARGETDIR=<путь>

Папка, в которую будет установлен продукт. По умолчанию используется следующая папка: C:\Program Files\BackupClient.

REBOOT=ReallySuppress

Если данный параметр указан, перезапуск машины запрещен.

/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.

CURRENT_LANGUAGE=<ИД языка>

Язык продукта. Доступные значения: en, ru
Если этот параметр не указан, язык продукта определяется языком, который используется в системе, при условии, что он указан в списке выше. В противном случае будет использоваться английский (en).

Параметры регистрации

REGISTRATION_ADDRESS

Это URL-адрес для службы Кибер Бэкап Облачный. Этот параметр можно использовать с параметрами REGISTRATION_LOGIN и REGISTRATION_PASSWORD или с параметром REGISTRATION_TOKEN.

- Если REGISTRATION_ADDRESS используется с параметрами REGISTRATION_LOGIN и REGISTRATION_PASSWORD, укажите адрес, который используется **для входа** в службу Кибер Бэкап Облачный. Например, https://cloud.company.com:

- Если REGISTRATION_ADDRESS используется с параметром REGISTRATION_TOKEN, укажите точный адрес центра обработки данных. Это URL-адрес, который отображается **после входа в** службу Кибер Бэкап Облачный. Например, https://eu2-cloud.company.com.

  Не используйте формат https://cloud.company.com here.

REGISTRATION_LOGIN и REGISTRATION_PASSWORD

Учетные данные учетной записи, под которой агент будет зарегистрирован в службе Кибер Бэкап Облачный. Для этого нельзя использовать учетную запись администратора партнера.

REGISTRATION_PASSWORD_ENCODED

Пароль учетной записи, под которой агент будет зарегистрирован в службе Кибер Бэкап Облачный, закодированный в base64. Инструкции о том, как зашифровать пароль, см. в разделе "Регистрация машин вручную".

REGISTRATION_TOKEN

Маркер регистрации – это последовательность из 12 символов, разделенных дефисами на три части. Его можно создать в консоли службы, как указано в разделе "Управление маркерами регистрации" (стр. 113).

REGISTRATION_REQUIRED={0,1}

Определяет способ завершения установки в случае сбоя регистрации. Если задано значение 1, установка также завершается сбоем. По умолчанию задано значение 0, поэтому если не указать этот параметр, установка завершается успешно, даже если агент не зарегистрирован.

Дополнительные параметры

Чтобы определить учетную запись входа для службы агента в Windows, используйте один из следующих параметров:

- MMS_USE_SYSTEM_ACCOUNT={0,1}
  Если задано значение 1, агент будет запускаться под учетной записью **Локальная система**.
- MMS_CREATE_NEW_ACCOUNT={0,1}
  Если задано значение 1, агент будет запускаться под новой созданной учетной записью **Cyber Agent User**.
- MMS_SERVICE_USERNAME=<имя пользователя> и MMS_SERVICE_PASSWORD=<пароль>
  Используйте эти параметры, чтобы указать существующую учетную запись, под которой будет запускаться агент.

Дополнительную информацию об учетных записях входа см. в разделе "Изменение учетной записи входа на машинах Windows".

SET_ESX_SERVER={0,1}

- Если задано значение 0, устанавливаемый агент для VMware не будет подключаться к vCenter Server или хосту ESXi. Если задано значение 1, укажите следующие параметры:
  - ESX_HOST=<имя хоста>
    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.

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}

Если значение равно 0 или данный параметр не указан, агент будет использовать прокси-сервер только для резервного копирования и восстановления из облака. Если значение равно 1, агент также подключится к серверу управления через прокси-сервер.

Параметры удаления

REMOVE={<список компонентов>|ALL}

Компоненты для удаления, разделенные запятыми и без символов пробела. 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.

ANTI_TAMPER_PASSWORD=<пароль>

Для удаления защищенного паролем агента для Windows или изменения его компонентов требуется пароль.

Примеры

- Установка агента для Windows, программы командной строки и Cyber Protection Monitor. Регистрация машины в службе Кибер Бэкап Облачный с использованием имени пользователя и пароля.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_
SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD=johnspassword
```

- Установка агента для Windows, программы командной строки и Cyber Protection Monitor. Создание новой учетной записи входа для службы агента в Windows. Регистрация машины в службе Кибер Бэкап Облачный с использованием маркера.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_
NEW_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C
```

- Установка агента для Windows, программы командной строки, агента для Oracle и Cyber Protection Monitor. Регистрация машины в службе Кибер Бэкап Облачный с использованием имени пользователя и пароля, закодированного в base64.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgent
Feature,TrayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress
CURRENT_LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_
ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe REGISTRATION_
PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Установка агента для Windows, программы командной строки и Cyber Protection Monitor. Регистрация машины в службе Кибер Бэкап Облачный с использованием маркера. Настройка прокси-сервера HTTP

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
```

```
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- Удаление всех агентов с их журналами, задачами и параметрами конфигурации.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_SETTINGS=1 REBOOT=ReallySuppress
```

7.7.2 Автоматическое установка или автоматическое удаление в Linux

В этом разделе описан порядок установки или удаления агентов защиты в автоматическом режиме на машинах под управлением Linux с использованием командной строки.

Порядок установки или удаления агента защиты

1. Откройте приложение терминала.

2. Выполните одно из следующих действий:

- Чтобы запустить установку указанных параметров в командной строке, выполните следующую команду:

  ```
  <имя пакета> -a <параметр 1> ... <параметр N>
  ```

  Здесь <имя пакета> – это имя пакета установки (файла .x86_64). Все доступные параметры и их значения описаны в разделе Параметры автоматической установки или автоматического удаления.

- Чтобы запустить установку с параметрами, которые указаны в отдельном текстовом файле, выполните следующую команду:

  ```
  <имя пакета> -a --options-file=<путь к файлу>
  ```

  Этот подход можно использовать, чтобы не вводить конфиденциальную информацию в командную строку. В этом случае можно указать параметры конфигурации в отдельном текстовом файле и разрешить к нему доступ только для себя. В каждой строке может быть только один параметр, после которого необходимо указать нужное значение. Пример:

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  или

  ```
  -C
  https://cloud.company.com
  ```

```
-g
johndoe
-w
johnspassword
-a
--language
en
```

Если в командной строке и текстовом файле указан одинаковый параметр, значение, указанное в командной строке, имеет приоритет.

3. Если на машине включена безопасная загрузка UEFI, выводится сообщение о том, что необходимо перезагрузить систему после установки. Запомните, какой пароль необходимо использовать (суперпользователя или пользователя "acronis"). 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.

7.7.2.1 Параметры автоматической установки или автоматического удаления

В этом разделе описаны параметры, которые используются при автоматической установке или автоматическом удалении в Linux.

В минимальную конфигурацию для автоматической установки входит параметр -a и параметры регистрации (например, параметры --login и --password; --rain и --token). Для более точной настройки установки можно использовать дополнительные параметры.

Параметры установки

Базовые параметры

{-i |--id=}<список компонентов>

Компоненты для установки, разделенные запятыми и без символов пробела. В пакете установки .x86_64 доступны следующие компоненты:

Компонент	Описание компонента
BackupAndRecoveryAgent	Агент для Linux
CommunigateAgentFeature	Агент для Communigate Pro
K8sAgentFeature	Агент для Kubernetes
OracleAgentFeature	Агент для Oracle

PostgreSqlAgentFeature	Агент для PostgreSQL
WorkmailAgentFeature	Агент для WorkMail

Если данный параметр не указан, устанавливаются все перечисленные ниже компоненты.

Для агента для Oracle требуется установленный агент для Linux.

Пакет установки .i686 содержит только BackupAndRecoveryAgent.

{-a|--auto}

Процесс установки и регистрации завершится без какого-либо вмешательства пользователя. При использовании этого параметра необходимо указать учетную запись, под которой агент будет зарегистрирован в службе Кибер Бэкап Облачный. Для этого можно использовать параметр --token или параметры --login и --password.

{-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}

Отсутствие требуемых пакетов Linux не будет принято во внимание при установке.

{-d|--debug}

Позволяет вести журнал установки в режиме подробного протоколирования.

--options-file=<хранилище>

Параметры установки будут считываться из текстового файла, а не из командной строки.

--language=<ИД языка>

Язык продукта. Доступные значения: en, ru.
Если этот параметр не указан, язык продукта определяется языком, который используется в системе, при условии, что он указан в списке выше. В противном случае будет использоваться английский (en).

Параметры регистрации

Укажите один из следующих параметров:

- {-g|--login=}<имя пользователя> и {-w|--password=}<пароль>

Учетные данные учетной записи, под которой агент будет зарегистрирован в службе Кибер Бэкап Облачный. Для этого нельзя использовать учетную запись администратора партнера.

- --token=<маркер>

  Маркер регистрации — это последовательность из 12 символов, разделенных дефисами на три части. Его можно создать в консоли службы, как указано в разделе "Управление маркерами регистрации" (стр. 113).

  Невозможно использовать параметр --token вместе с параметрами --login, --password и --register-with-credentials.

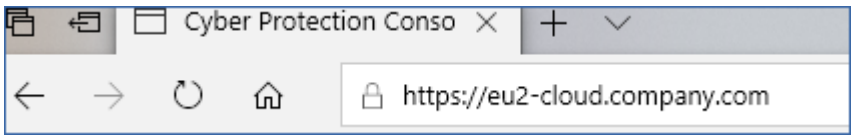
  - {-C|--rain=}<адрес службы>

    URL-адрес службы Кибер Бэкап Облачный.

    Если не нужно включить этот параметр явно при использовании параметров --login и --password для регистрации из-за того, что установщик использует правильный адрес по умолчанию — это адрес, используемый для **входа в** службу Кибер Бэкап Облачный. Пример:

    Но если {-C|--rain=} используется с параметром --token, необходимо указать точный адрес центра обработки данных. Это URL-адрес, который отображается **после входа в** службу Кибер Бэкап Облачный. Пример:

- --register-with-credentials

Если указан этот параметр, запустится графический интерфейс установщика. Чтобы завершить регистрацию, введите имя пользователя и пароль для учетной записи, под которой агент будет зарегистрирован в службе Кибер Бэкап Облачный. Для этого нельзя использовать учетную запись администратора партнера.

- --skip-registration

Используйте этот параметр, когда необходимо установить агент, но вы планируете зарегистрировать его в службе Кибер Бэкап Облачный позже. Инструкции о том, как это сделать, см. в разделе "Регистрация машин вручную".

Дополнительные параметры

--http-proxy-host=<IP-адрес> и --http-proxy-port=<порт>

Прокси-сервер HTTP, который агент будет использовать для резервного копирования и восстановления из облака и для подключения к серверу управления. 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.

--tmp-dir=<хранилище>

Указывает папку, в которую сохраняются временные файлы при установке. По умолчанию используется папка **/var/tmp**.

{-s|--disable-native-shared}

При установке используются свободно распространяемые библиотеки, даже если они уже есть в вашей системе.

--skip-prereq-check

Не будет выполняться проверка на предмет того, установлены ли пакеты, требуемые для компиляции модуля snapapi.

--force-weak-snapapi

Установщик не будет компилировать модуль snapapi. Вместо этого будет использоваться готовый модуль, который может в точности не соответствовать ядру Linux. Не рекомендуется использовать этот параметр.

--skip-svc-start

Служба не будет запускаться автоматически после установки. В большинстве случаев этот параметр используется с параметром --skip-registration.

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.

--snapapi-list

Показывает доступные готовые модули snapapi.

--components-list

Показывает компоненты установщика.

Параметры для устаревших функций

Эти параметры относятся к устаревшему компоненту agent.exe.

{-e|--ssl=}<путь>

Указывает путь к файлу настраиваемого сертификата для обмена данными SSL.

{-p|--port=}<порт>

Укажите порт, на котором agent.exe будет ожидать передачи данных. По умолчанию используется порт 9876.

Параметры удаления

{-u|--uninstall}

Удаляет продукт.

--purge

Удаляет продукт вместе с журналами, задачами и настройками конфигурации. Нет необходимости явно указывать параметр --uninstall, когда используется параметр --purge.

Примеры

- Установка агента для Linux без его регистрации.

```
./Cloud_Backup_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Установка агента для Linux, агента для Oracle и их регистрация с использованием учетных записей.

```
./Cloud_Backup_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- Установка агента для Oracle и агента для Linux и их регистрация с использованием маркера регистрации.

```
./Cloud_Backup_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature
-a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- Установка агента для Linux, агента для Oracle с настройками конфигурации в отдельном текстовом файле.

```
./Cloud_Backup_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_
file
```

- Установка агента для Linux, агента для Oracle и удаление всех их журналов, задач и настроек конфигурации.

```
./Cloud_Backup_Agent_for_Linux_x86_64.bin -a --purge
```

7.8 Регистрация машин вручную

Помимо регистрации машины в службе Кибер Бэкап Облачный при установке агента, можно также зарегистрировать её 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 учётной записью.

7.8.1 Регистрация машины с агентом в ОС Windows

7.8.1.1 Регистрация с использованием маркера

Данный способ является рекомендуемым. Маркер регистрации представляет собой уникальную последовательность из 12 цифро-буквенных символов (например, 7A85-70B2-445F). Его можно создать для пользователя и затем указать при развёртывании агента или виртуального устройства, не указывая и не сохраняя при этом имя учётной записи и пароль соответствующего пользователя. Подробнее о маркерах регистрации см. в разделе "Управление маркерами регистрации" (стр. 113).

Для регистрации машины с использованием маркера выполните команду:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a <адрес службы> --token <маркер>
```

Пример команды:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

7.8.1.2 Регистрация с использованием данных учётной записи

Для регистрации машины с использованием данных текущей учётной записи выполните команду:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud --update
```

Для регистрации машины с использованием данных другой учётной записи выполните команду:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a <адрес службы> -u <имя пользователя> -p <пароль>
```

Пример команды:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Примечание

Если пароль содержит специальные символы или пробелы, заключите его в кавычки при вводе в командной строке. Пароль рекомендуется указывать в формате base64, используя параметр --base64.

Предупреждение
Не рекомендуется вводить данные учётной записи, в том числе пароль, в открытом виде.

7.8.2 Регистрация машины с агентом в ОС Linux

7.8.2.1 Регистрация с использованием маркера

Данный способ является рекомендуемым. Маркер регистрации представляет собой уникальную последовательность из 12 цифро-буквенных символов (например, 7A85-70B2-445F). Его можно создать для пользователя и затем указать при развёртывании агента или виртуального устройства, не указывая и не сохраняя при этом имя учётной записи и пароль соответствующего пользователя. Подробнее о маркерах регистрации см. в разделе "Управление маркерами регистрации" (стр. 113).

Для регистрации машины с использованием маркера выполните команду:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <адрес службы> --token <маркер>
```

Пример команды:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

7.8.2.2 Регистрация с использованием данных учётной записи

Для регистрации машины с использованием данных текущей учётной записи выполните команду:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud --update
```

Для регистрации машины с использованием данных другой учётной записи выполните команду:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <адрес службы> -u <имя пользователя> -p <пароль>
```

Пример команды:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Примечание
Если пароль содержит специальные символы или пробелы, заключите его в кавычки при вводе в командной строке. Пароль рекомендуется указывать в формате base64, используя параметр --base64.

Предупреждение
Не рекомендуется вводить данные учётной записи, в том числе пароль, в открытом виде.

7.8.3 Удаление регистрации

Чтобы удалить регистрацию машины с агентом, выполните следующую команду:

- в ОС Windows:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

- в ОС Linux:

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

7.9 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.

Внимание
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 пакете с установленным агентом не было никаких машин, то функция автоматического обнаружения будет скрыта: раздел **Несколько устройств** будет скрыт в мастере добавления нового устройства.

После добавления машин в консоль службы 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.

7.9.1 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)

При выполнении сканирования AD агент пытается получить для каждой машины практически такие же параметры, которые перечислены выше. Отличие состоит в том, что в этом случае агент пытается дополнительно получить параметр "Подразделение", а также более полную информацию об имени и операционной системе и не запрашивает IP-адрес и MAC-адрес.

7.9.2 Предварительные требования

Прежде чем запустить обнаружение машин, необходимо установить агент защиты хотя бы на одной машине в локальной сети, 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 домене AD. Этот агент будет использоваться как агент обнаружения при сканировании AD.

Примечание
Агент для Windows невозможно установить на удаленной машине с Windows XP.
Для установки агента для Windows на машине с Windows Server 2012 R2, на этой машине должно быть установлено обновление Windows KB2999226.

7.9.3 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:
   - Путем сканирования Active Directory
   - Путем сканирования локальной сети
   - Вручную: добавление машины по 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 консоли службы.
- Машины регистрируются в консоли службы (если они уже имеют установленный агент).
- Машины добавляются в консоль службы со статусом **Неуправляемое** без установки каких-либо агентов или компонентов.

Если для добавления машины вы используете один из первых двух методов, можно также выбрать план защиты из существующих планов и применить его к машинам.

4. Укажите учетные данные пользователя, который имеет права администратора для управления машинами.
5. Проверьте возможность подключения к машинам, используя предоставленные учетные данные.

В следующих темах вы получите более подробную информацию о процедуре обнаружения.

7.9.4 Автоматическое и ручное обнаружение

Прежде чем запустить обнаружение, убедитесь, что соблюдены предварительные требования.

Обнаружение машин

1. В консоли службы последовательно выберите пункты **Устройства** > **Все устройства**.
2. Нажмите кнопку **Добавить**.
3. В **Несколько устройств** щелкните **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.
6. Выберите метод обнаружения:
   - **Поиск в Active Directory**. Машина с агентом для Windows должна состоять в домене Active Directory. Установить агент на контроллер домена, доступный только для чтения (RODC), можно по инструкции из базы знаний.
   - **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 действия, которые необходимо выполнить после обнаружения:
   - **Установить агенты и зарегистрировать машины**. Компоненты для установки на машинах можно выбрать, щелкнув **Выбор компонентов**. Дополнительную информацию см. в разделе "Выбор компонентов для установки" (стр. 69)

     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 в контроллере 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.

     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 Облачный. 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 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] **Пользователь, для которого регистрируются машины**: выберите пользователя вашего отдела или подчиненных отделов, для которых 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.

Внимание

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 "Включение удаленной установки агента для настраиваемого администратора", который приведен ниже.

11. 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**).

7.9.4.1 Подготовка машины для удаленной установки

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 > Центр управления сетями и общим доступом > Изменить дополнительные параметры общего доступа**.
4. Кибер Бэкап Облачный 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.

7.9.4.2 Требования к контролю учетных записей пользователей (UAC)

На машине с ОС Windows Vista или более поздней версии, 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.

Как отключить UAC

Выберите один из следующих вариантов в зависимости от операционной системы.

- **В ОС Windows более ранней версии, чем Windows 8:**

  Выберите **Панель управления > Просмотр по: Мелкие значки > Учетные записи пользователей > Изменение параметров контроля учетных записей** и передвиньте ползунок на пункт **Никогда не уведомлять**. Перезапустите машину.
- **В любой операционной системе Windows**:

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 Майкрософт.

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

7.9.4.3 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 службы предотвращения утечки данных	Этот агент позволят ограничить доступ пользователей к локальным и перенаправленным периферийным устройствам, портам и буферу на машинах, для которых применены планы защиты. Он устанавливается на машинах с Oracle Database. Если этот компонент выбран, он будет установлен.
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.
Кибер Бэкап Облачный Monitor	Этот компонент позволяет пользователю отслеживать выполнение запущенных заданий в области уведомлений. Он устанавливается на машинах Windows. Если этот компонент выбран, он будет установлен. Поддерживается в Windows 7 с пакетом обновления 1 (SP1) и более поздних версий, Windows 2008 R2 с пакетом обновления 1 (SP1) и более поздних версий.
Программа командной строки	Кибер Бэкап Облачный 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 Облачный – агентов и сервера управления. Если этот компонент выбран, он будет установлен.

7.9.5 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 щелкните **Добавить в исключения**. Чтобы удалить машину из раздела **Исключения**, выберите пункты **Необслуживаемые машины** > **Исключения**, выберите машину и щелкните **Удалить из исключений**.

Для установки агента защиты и регистрации группы обнаруженных машин в Кибер Бэкап Облачный можно выбрать их в списке и щелкнуть **Установить и зарегистрировать**. В открытом мастере также можно назначить план защиты группе машин.

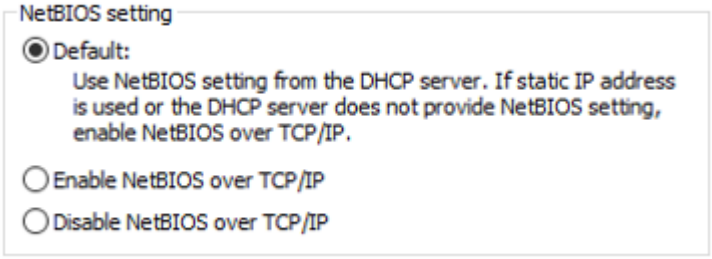
Те машины, на которых установлен агент защиты, отображаются в разделе **Устройства** > **Машины с агентами**.

Чтобы проверить статус защиты, откройте раздел **Панель мониторинга** > **Обзор** и добавьте виджет Статус защиты или виджет Обнаруженная машина.

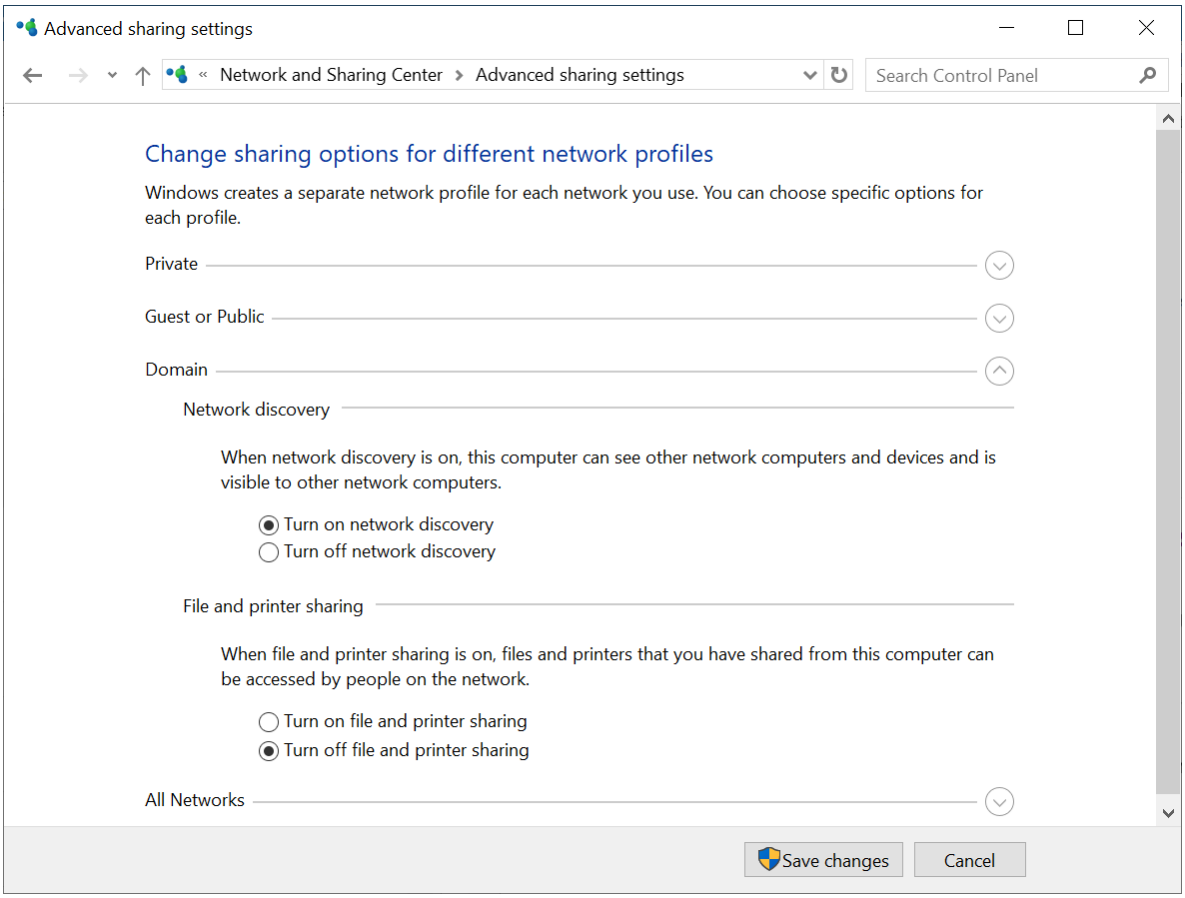
7.9.6 Устранение неисправностей

Если есть какие-либо проблемы с функциональностью автоматического обнаружения, выполните указанные ниже действия.

- Проверьте, что протокол "NetBIOS over TCP/IP" включен или задан по умолчанию.



- В разделе "Панель управления\Центр управления сетями и общим доступом\Дополнительные параметры общего доступа" включите обнаружение сети.



- Проверьте, что служба "Хост поставщика функции обнаружения" запущена на машине, которая выполняет обнаружение и на машинах, которые должны быть доступны для обнаружения.
- Проверьте, что служба "Публикация ресурсов обнаружения функции" запущена на машинах, которые должны быть доступны для обнаружения.

7.10 Развертывание агента для VMware (виртуальное устройство)

7.10.1 Перед началом

7.10.1.1 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 ТБ. Формат диска («толстый» или «тонкий») не влияет на производительность устройства.

7.10.1.2 Сколько агентов необходимо?

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».

7.10.1.3 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**.

7.10.2 Развертывание шаблона OVF

1. Последовательно выберите пункты **Все устройства** > **Добавить** > **VMware ESXi** > **Virtual Appliance (OVF)**.
   ZIP-архив загрузится на машину.
2. Распакуйте ZIP-архив. Папка содержит один OVF-файл и два VMDK-файла.
3. Убедитесь в том, что эти файлы доступны с машины с клиентом vSphere.
4. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
5. 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 убедитесь, что выбранная сеть позволяет подключиться к Интернету. Это необходимо, чтобы агент мог зарегистрироваться в облаке.

7.10.3 Настройка виртуального устройства

1. **Запуск виртуального устройства**

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

2. **Прокси-сервер**

   Если в вашей сети есть прокси-сервер:

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

   b. Откройте файл **/etc/Acronis/Global.config** в текстовом редакторе.

   c. 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>.

   d. Замените АДРЕС новым именем хоста или IP-адресом прокси-сервера, а ПОРТ — номером порта в десятичном формате.

   e. 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.

   f. Сохраните файл.

   g. Откройте файл **/opt/acronis/etc/aakore.yaml** в текстовом редакторе.

   h. 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
      ```

   i. Вместо proxy_login и proxy_password укажите учетные данные прокси-сервера, а вместо proxy_address:port — адрес и номер порта прокси-сервера.

   j. 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**

   a. На **сервере управления** в разделе **Параметры агента** щелкните **Изменить**.

   b. В поле **Имя/IP-адрес сервера** выберите **Облако**. В программе отображается адрес службы Кибер Бэкап Облачный. Не меняйте этот адрес, если иное не указано в инструкции.

   c. В полях **Имя пользователя** и **Пароль** укажите имя пользователя и пароль для службы Кибер Бэкап Облачный. Агент и виртуальные машины, управляемые агентом, будут зарегистрированы с этой учетной записью.

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.

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. Щелкните эту ссылку, выберите диск и задайте для него метку.

7.11 Развертывание агента для oVirt (виртуальное устройство)

7.11.1 Перед началом

Этот программно-аппаратный комплекс представляет собой предварительно настроенную виртуальную машину, которая развертывается в центре обработки данных Red Hat Virtualization/oVirt. В ее состав входит агент защиты, который позволяет вам администрировать киберзащиту для всех виртуальных машин в центре обработки данных.

7.11.1.1 Системные требования для агента

По умолчанию виртуальная машина с агентом использует 2 виртуальных ЦП и 4 ГиБ ОЗУ. Эти настройки достаточны для большинства операций, но при необходимости их можно изменить на портале администрирования Red Hat Virtualization/oVirt. 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 и использовать 4 виртуальных ЦП и повысить объем ОЗУ до 8 ГиБ.

Размер виртуального диска программно-аппаратного комплекса составляет 8 ГиБ.

7.11.1.2 Сколько агентов необходимо?

Одного агента достаточно для защиты всего центра обработки данных. Однако можно использовать несколько агентов в центре обработки данных, если нужно распределить нагрузку на сеть, которую создает трафик резервного копирования.

Если в центре обработки данных несколько агентов, виртуальные машины автоматически распределяются между агентами таким образом, что каждый агент управляет почти одинаковым количеством машин.

Автоматическое перераспределение происходит, когда дисбаланс нагрузки между агентами достигает 20 процентов. Это может происходить при добавлении или удалении машины или агента. Например, когда становится очевидно, что для повышения пропускной способности требуется больше агентов, вы развертываете в центре обработки данных дополнительное виртуальное устройство. Сервер управления назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится. При удалении агента машины, назначенные этому агенту, перераспределяются между оставшимися агентами. Однако этого не происходит, если агент повреждается или вручную удаляется с портала администрирования Red Hat Virtualization/oVirt. Перераспределение начнется только после удаления такого агента из консоли службы Кибер Бэкап Облачный.

Порядок получения информации об агенте, управляющем конкретной машиной

1. В консоли службы Кибер Бэкап Облачный щелкните **Устройства**, а затем выберите **oVirt**.
2. Щелкните значок шестерни в верхнем правом углу таблицы и в области **Система** установите флажок **Агент**.
3. Имя агента отобразится в появившемся столбце.

7.11.1.3 Ограничения

Следующие операции не поддерживаются для виртуальных машин Red Hat Virtualization/oVirt:

- Резервное копирование с поддержкой приложений
- Запуск виртуальной машины из резервной копии
- Репликация виртуальных машин
- Технология отслеживания измененных блоков (CBT)

7.11.2 Развертывание шаблона OVA

1. Войдите в учетную запись Кибер Бэкап Облачный.
2. Щелкните **Устройства** > **Все устройства** > **Добавить** > **Red Hat Virtualization (oVirt)**.
   ZIP-архив загрузится на машину.
3. Распакуйте ZIP-архив. В нем содержится файл .ova.
4. Передайте файл .ova на хост в центре обработки данных Red Hat Virtualization/oVirt, который необходимо защитить.
5. Войдите на портал администрирования Red Hat Virtualization/oVirt с учетной записью администратора. Дополнительную информацию о ролях, которые необходимы для выполнения операций с виртуальными машинами, см. в разделе "Агент для oVirt: требуемые роли и порты" (стр. 79).
6. В меню навигации выберите пункты **Вычисления** > **Виртуальные машины**.
7. Над основной таблицей щелкните значок в виде вертикального эллипса  , а затем щелкните **Импорт**.
8. В окне **Import Virtual Machine(s)** (Импорт виртуальных машин) выполните следующие действия:
   a. В области **Центр обработки данных** выберите центр обработки данных, для которого нужно обеспечить защиту.
   b. В области **Источник** выберите **Виртуальное устройство (OVA)**.
   c. В области **Хост** выберите хост, на который вы передали файл .ova.
   d. В области **Путь к файлу** укажите путь к каталогу, который содержит файл .ova.
   e. Щелкните **Загрузить**.
      На панели **Virtual Machines on Source** (Виртуальные машины в источнике) появится шаблон виртуального устройства oVirt из файла .ova.
      Если шаблон не появится на этой панели, убедитесь, что указан правильный путь к файлу, файл не поврежден, а хост доступен.

f. На панели **Virtual Machines on Source** (Виртуальные машины в источнике) выберите шаблон виртуального устройства oVirt, а затем щелкните значок со стрелкой вправо.
Шаблон появится на панели **Виртуальные машины для импорта**.

g. Нажмите кнопку **Далее**.

9. В новом окне щелкните имя программно-аппаратного комплекса и настройте следующие параметры:
   - На вкладке **Сетевые интерфейсы** настройте сетевые интерфейсы.
   - [Необязательно] На вкладке **Общие** измените имя по умолчанию для виртуальной машины с агентом.

Развертывание готово. После этого необходимо настроить виртуальное устройство. Инструкции о том, как это сделать, см. в разделе "Настройка виртуального устройства" (стр. 78)

Примечание
Если в центре обработки данных нужно использовать несколько виртуальных устройств, повторите указанные выше шаги и разверните дополнительные виртуальные устройства. Не клонируйте существующее виртуальное устройство, используя параметр **Clone VM** (Клонировать ВМ) на портале администрирования Red Hat Virtualization/oVirt.

Чтобы исключить виртуальное устройство из резервных копий динамической группы, необходимо также исключить его из списка виртуальных машин в консоли службы Кибер Бэкап Облачный. Чтобы исключить его, на портале администрирования Red Hat Virtualization/oVirt выберите виртуальную машину с агентом, а затем назначьте ему тег cyberprotect_virtual_appliance.

7.11.3 Настройка виртуального устройства

После развертывания виртуального устройства необходимо настроить его таким образом, чтобы у него был доступ как ядру oVirt, так и к службе Кибер Бэкап Облачный.

Для настройки виртуального приложения

1. Войдите на портал администрирования Red Hat Virtualization/oVirt.
2. Выберите виртуальную машину с агентом для настройки и щелкните значок **Консоль**.
3. В поле **eth0** настройте сетевые интерфейсы программно-аппаратного комплекса.
   Убедитесь, что автоматически назначенные адреса DHCP (если есть) действительны в сетях, которые использует ваша виртуальная машина, или назначьте их вручную. Для настройки может быть доступен один интерфейс или несколько интерфейсов. Это зависит от количества сетей, которые использует программно-аппаратный комплекс.
4. В поле **oVirt** щелкните **Изменить**, укажите адрес ядра oVirt и учетные данные для доступа к нему:
   a. В поле **Имя/IP-адрес сервера** введите DNS-имя или IP-адрес ядра.
   b. В полях **Имя пользователя** и **Пароль** введите учетные данные администратора для этого ядра.

Убедитесь, что учетная запись этого администратора имеет роли, необходимые для выполнения операций с виртуальными машинами Red Hat Virtualization/oVirt. Дополнительную информацию об этих ролях см. в разделе "Агент для oVirt: требуемые роли и порты" (стр. 79).

c. [Необязательно] Щелкните **Проверить подключение**, чтобы проверить правильность указанных учетных данных.

d. Нажмите кнопку **OK**.

5. В поле **Сервер управления** щелкните **Изменить** и укажите адрес и учетные данные службы Кибер Бэкап Облачный для доступа к ней.

   a. В поле **Имя/IP-адрес сервера** выберите **Облако**, а затем укажите адрес службы Кибер Бэкап Облачный.

   b. В полях **Имя пользователя** и **Пароль** введите учетные данные для учетной записи в службе Кибер Бэкап Облачный.

   c. Нажмите кнопку **OK**.

6. [Необязательно] В поле **Имя** щелкните **Изменить** и измените имя виртуального устройства по умолчанию (**localhost**). Это имя показано в консоли службы Кибер Бэкап Облачный.

7. [Необязательно] В поле **Время** щелкните **Изменить**, а затем выберите часовой пояс, чтобы запланированные операции выполнялись в правильное время.

Чтобы защитить виртуальную машину в центре обработки данных Red Hat Virtualization/oVirt

1. Войдите в учетную запись Кибер Бэкап Облачный.
2. Откройте **Устройства** > **oVirt** > <ваш кластер> или найдите машины в разделе **Устройства** > **Все устройства**.
3. Выберите нужные машины и примените к ним план защиты.

7.11.4 Агент для oVirt: требуемые роли и порты

7.11.4.1 Требуемые роли

Для развертывания и работы агента для oVirt требуется учетная запись администратора, для которой назначены указанные ниже роли.

oVirt/Red Hat Virtualization 4.2 и 4.3

- DiskCreator
- UserVmManager
- TagManager
- UserVmRunTimeManager
- VmCreator

oVirt/Red Hat Virtualization 4.4

- SuperUser

7.11.4.2 Необходимые порты

Агент для oVirt подключается к ядру oVirt по URL-адресу, который указан при настройке виртуального устройства. Как правило, URL-адрес ядра имеет следующий формат: https://ovirt.company.com. В этом случае используется протокол HTTPS и порт 443.

Если настройки oVirt отличаются от тех, которые заданы по умолчанию, может потребоваться другой порт. Точный порт можно узнать в формате URL-адреса. Пример:

URL-адрес ядра oVirt	Порт	Протокол
https://ovirt.company.com/	443	HTTPS
http://ovirt.company.com/	80	HTTP
https://ovirt.company.com:1234/	1234	HTTPS

Для операций чтения с диска/записи на диск не требуется дополнительных портов, поскольку резервная копия выполняется в режиме HotAdd.

7.12 Развертывание агента для OpenStack (виртуальное устройство)

Для развертывания агента для OpenStack вам понадобится установленная и настроенная платформа виртуализации OpenStack (выпуск от Ussuri до Zed).

Агент для OpenStack можно установить вручную в панели управления OpenStack, как описано далее.

7.12.1 Установка агента для OpenStack вручную

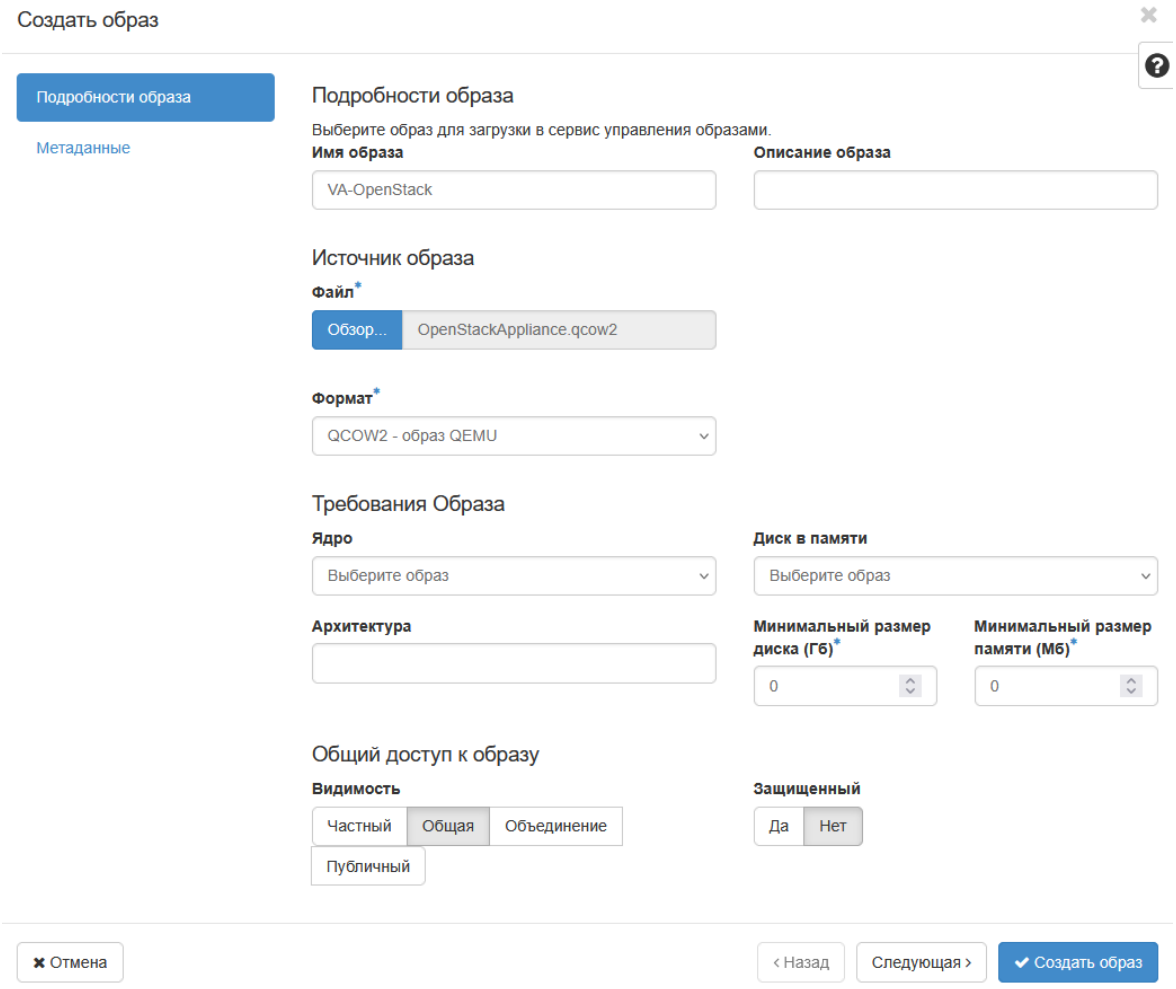
Чтобы установить агент для OpenStack вручную, выполните следующие шаги:

1. В консоли службы перейдите в раздел **Устройства** > **Все устройства** и нажмите **Добавить**.
2. В области **ХОСТЫ ВИРТУАЛИЗАЦИИ** щелкните **OpenStack** и загрузите архив с образом виртуального устройства.
3. Распакуйте образ виртуального устройства OpenStackAppliance.qcow2.
4. Импортируйте образ виртуального устройства в OpenStack:
   a. В панели управления OpenStack перейдите в раздел **Вычислительные ресурсы** > **Образы** и нажмите **Создать образ**.
   b. В поле **Имя образа** задайте имя образа.

c. В поле **Файл** укажите путь к распакованному образу виртуального устройства.

d. В поле **Формат** выберите **QCOW2 - образ QEMU**.

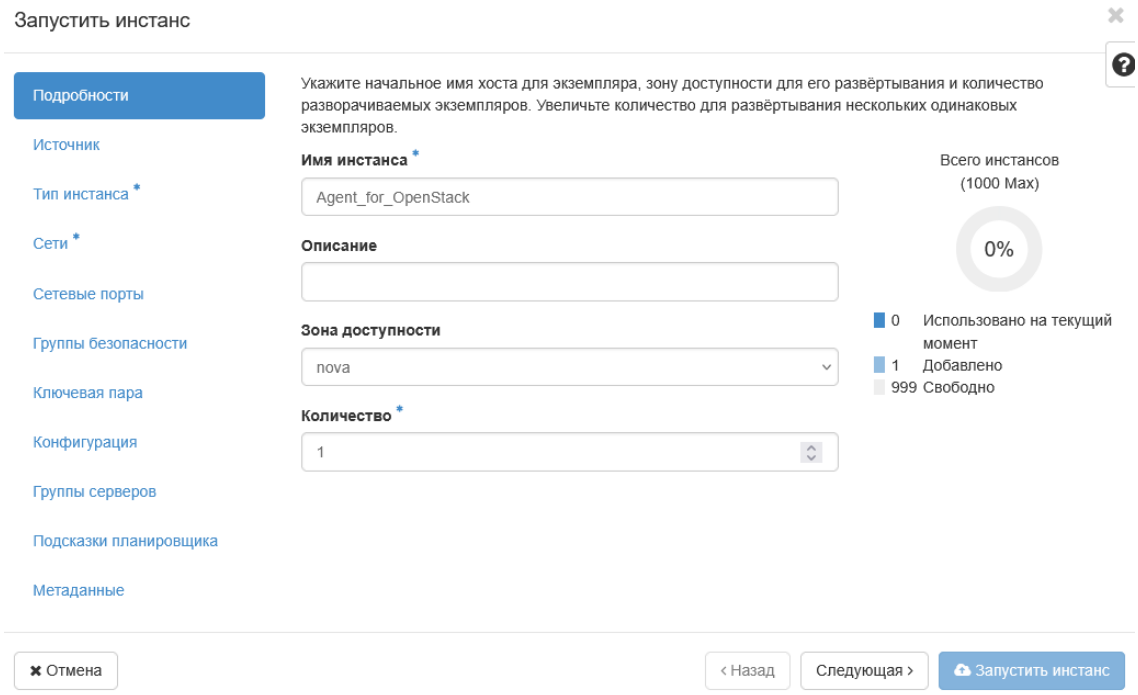
e. По окончании ввода данных нажмите **Создать образ**.



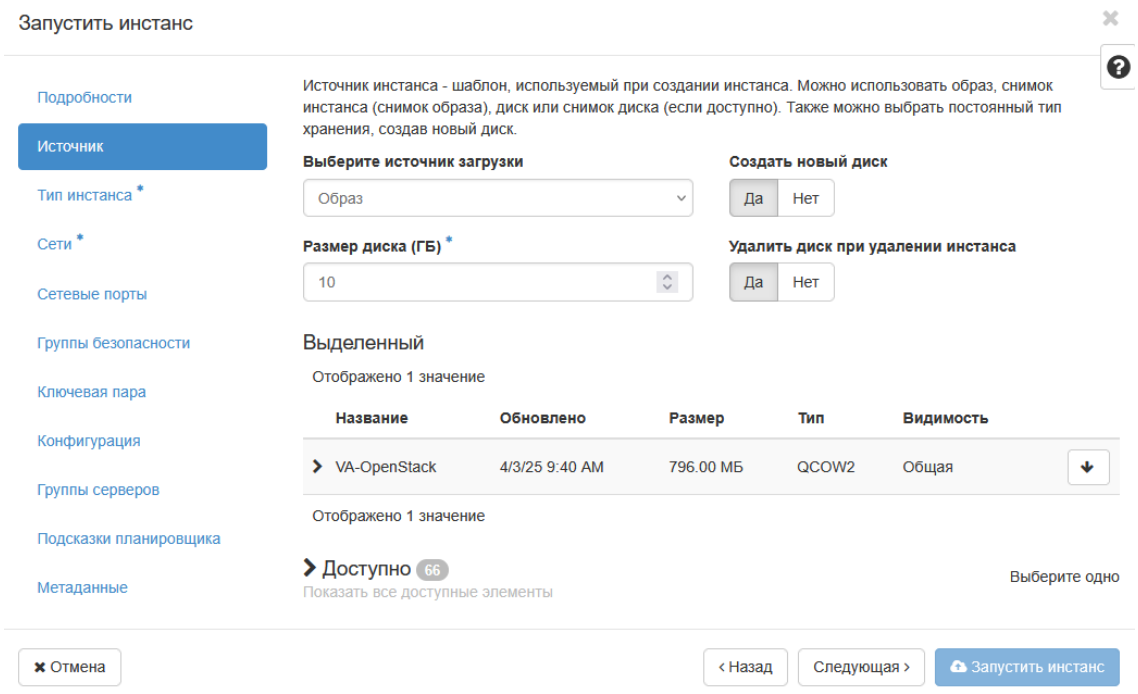
5. Создайте виртуальную машину в OpenStack на основе импортированного образа:

a. Перейдите в раздел **Вычислительные ресурсы** > **Инстансы** и нажмите **Запустить инстанс**.

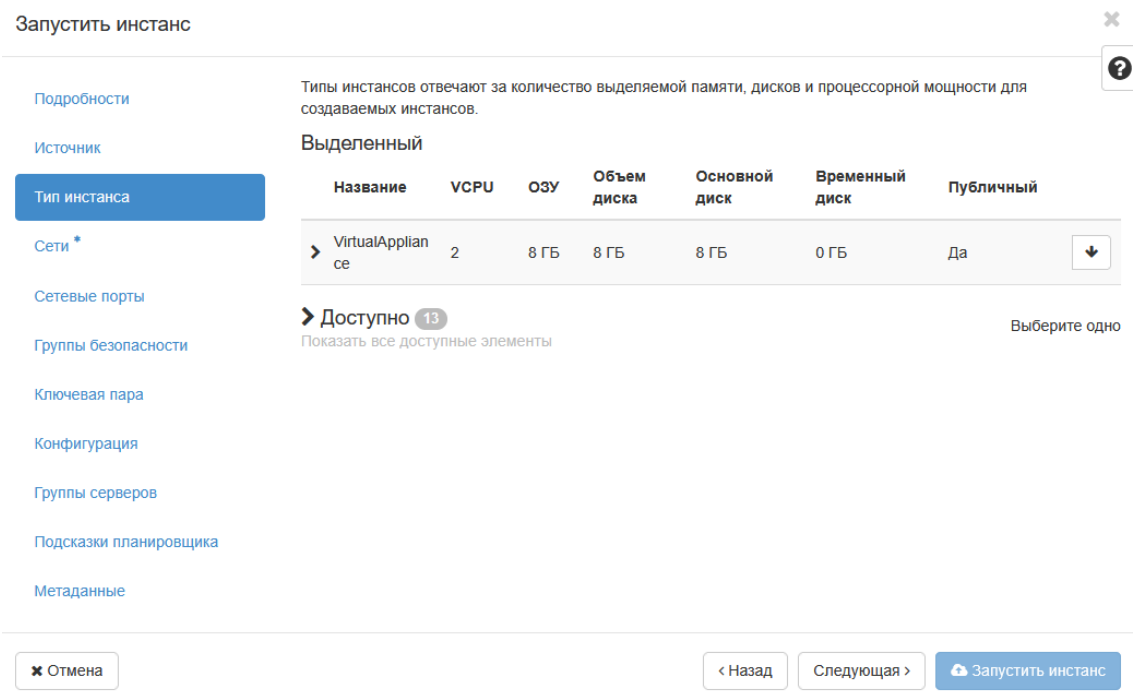
b. На вкладке **Подробности** укажите имя ВМ и зону доступности.



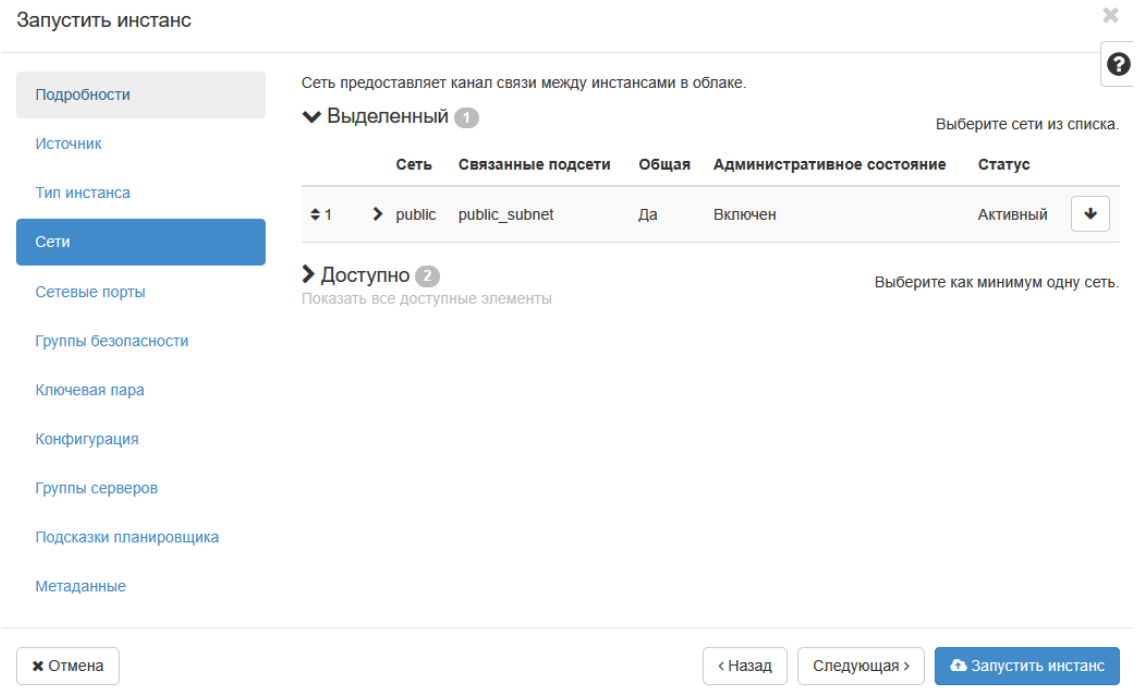
c. На вкладке **Источник** выберите источник загрузки **Образ** и укажите образ виртуального устройства.



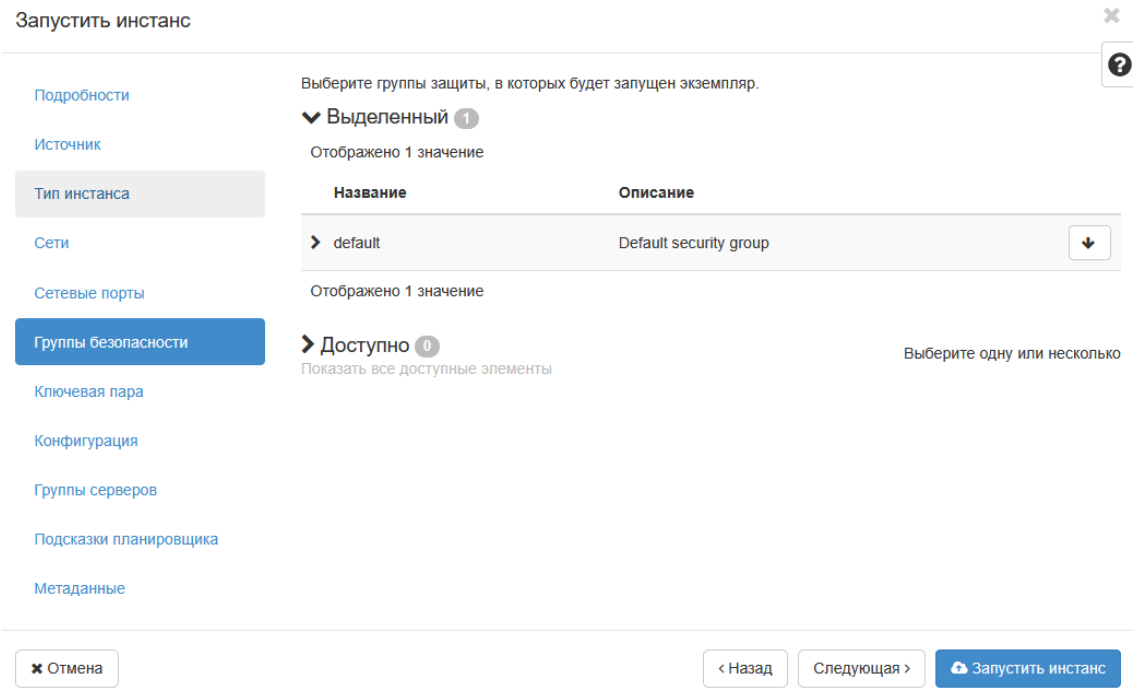
d. На вкладке **Тип инстанса** укажите параметры виртуальной машины. Для промышленной среды рекомендуется указывать не менее 2 ЦП и не менее 4 ГБ памяти.



e. На вкладке **Сети** укажите подходящую сеть. Сеть должна обеспечивать связь виртуального устройства с продуктом Кибер Бэкап Облачный и с контроллером OpenStack.



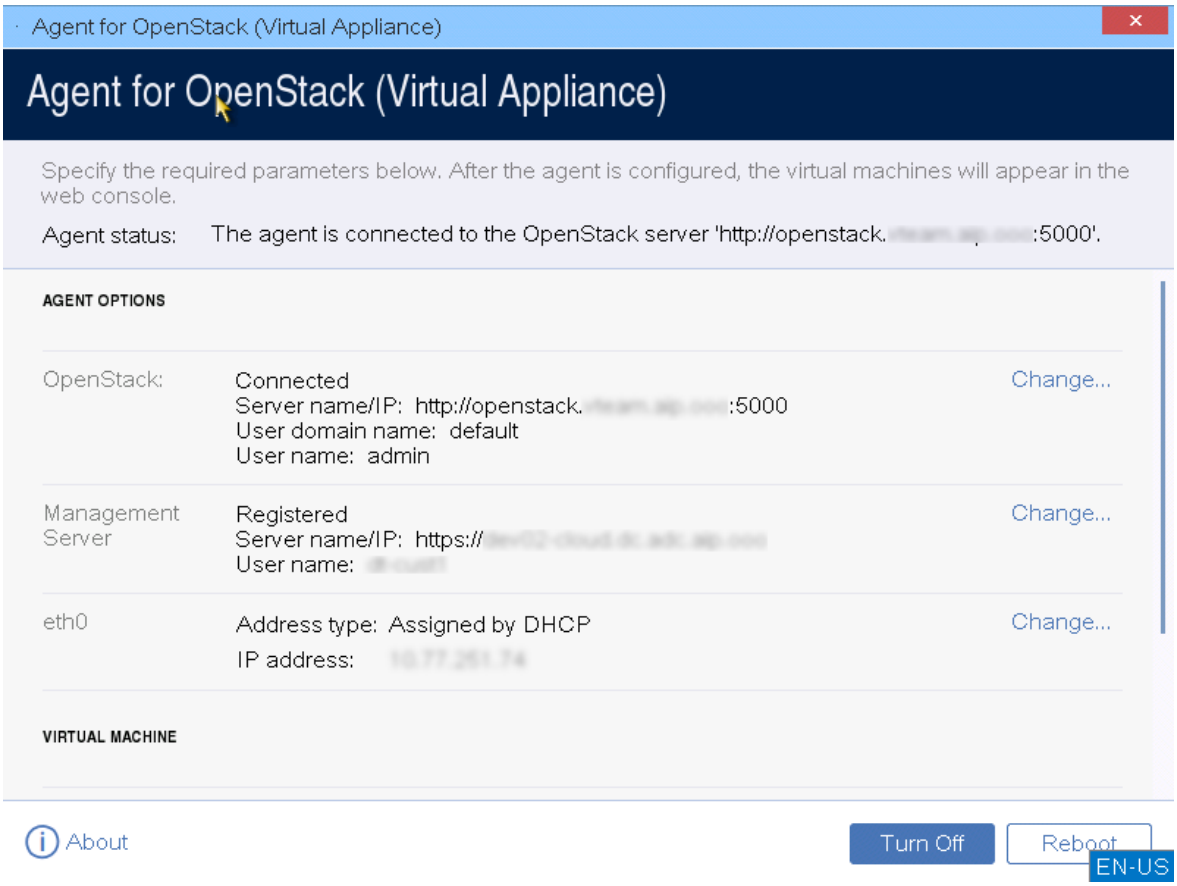
f. На вкладке **Группы безопасности** укажите подходящие группы безопасности. Группы безопасности должны разрешать связь виртуального устройства с продуктом Кибер Бэкап Облачный и с контроллером OpenStack.



g. По окончании ввода данных нажмите **Запустить инстанс**.

6. Перейдите в раздел **Вычислительные ресурсы** > **Инстансы** и убедитесь, что имя машины с агентом появилось в списке виртуальных машин.
7. Дождитесь запуска ВМ, откройте ее консоль и задайте параметры агента:
   - **OpenStack**. Укажите URL-адрес контроллера OpenStack, например: https://openstack.example.com:5000.

     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 URL-адрес службы Кибер Бэкап Облачный, 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 консоли службы.
   - **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 **Устройства** появится подраздел **OpenStack**;
- в разделе **Настройки** > **Агенты** отобразится агент для OpenStack.

7.13 Развертывание агента для VK Cloud (виртуальное устройство)

Для развертывания агента для VK Cloud вам понадобится установленная и настроенная платформа виртуализации VK Cloud версии 4.0.

Перед установкой агента для VK Cloud требуется предварительная настройка пользователя VK Cloud в зависимости от типа облачной платформы.

7.13.1 Предварительная настройка VK Cloud

7.13.1.1 Настройка для публичной облачной платформы

В панели администратора VK Cloud убедитесь, что включен доступ к API у пользователя, от лица которого виртуальное устройство будет взаимодействовать с VK Cloud.

См. также документацию разработчика.

7.13.1.2 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 ролью 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.

7.13.2 Установка агента для VK Cloud

Для установки обратитесь к разделу "Установка агента для VK Cloud вручную" (стр. 86).

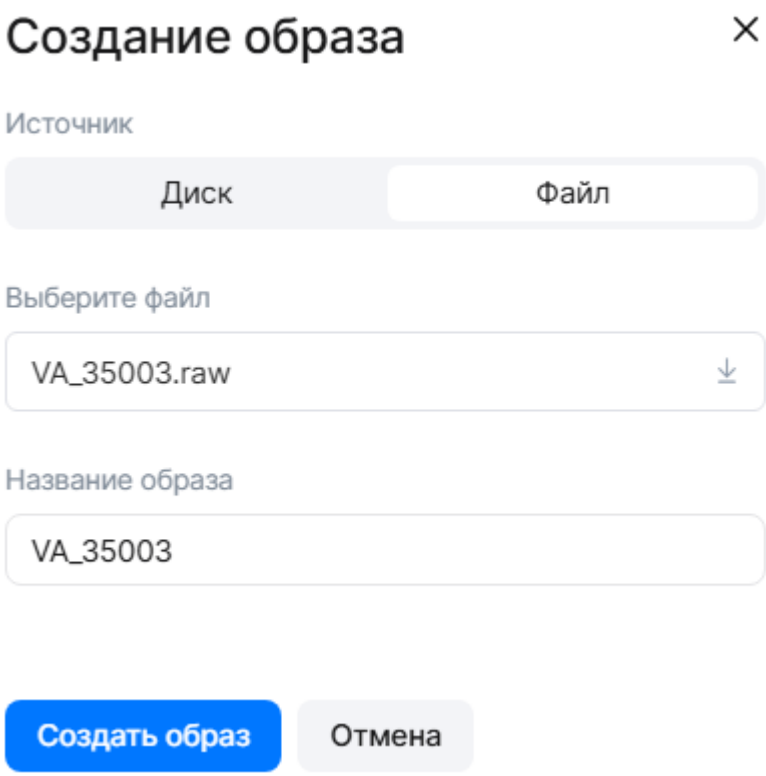
7.13.3 Установка агента для VK Cloud вручную

Чтобы установить агент для VK Cloud вручную, выполните следующие шаги:

1. В консоли службы перейдите в раздел **Устройства** > **Все устройства** и нажмите **Добавить**.
2. В области **ХОСТЫ ВИРТУАЛИЗАЦИИ** щелкните **OpenStack** и загрузите архив с образом виртуального устройства.
3. Подготовьте образ виртуального устройства в формате RAW с помощью утилиты qemu-img:

   ```
   qemu-img convert -f qcow2 -O raw OpenStackAppliance.qcow2 OpenStackAppliance.raw
   ```

4. Войдите в личный кабинет VK Cloud.
5. Импортируйте подготовленный образ в VK Cloud:
   a. Перейдите в раздел **Облачные вычисления** > **Образы** и нажмите **Создать**.
   b. В окне **Создание образа** укажите параметры импортируемого образа:
      i. В поле **Источник** выберите **Файл**.
      ii. В поле **Выберите файл** укажите путь к файлу образа в формате RAW.
      iii. В поле **Название образа** введите имя образа.

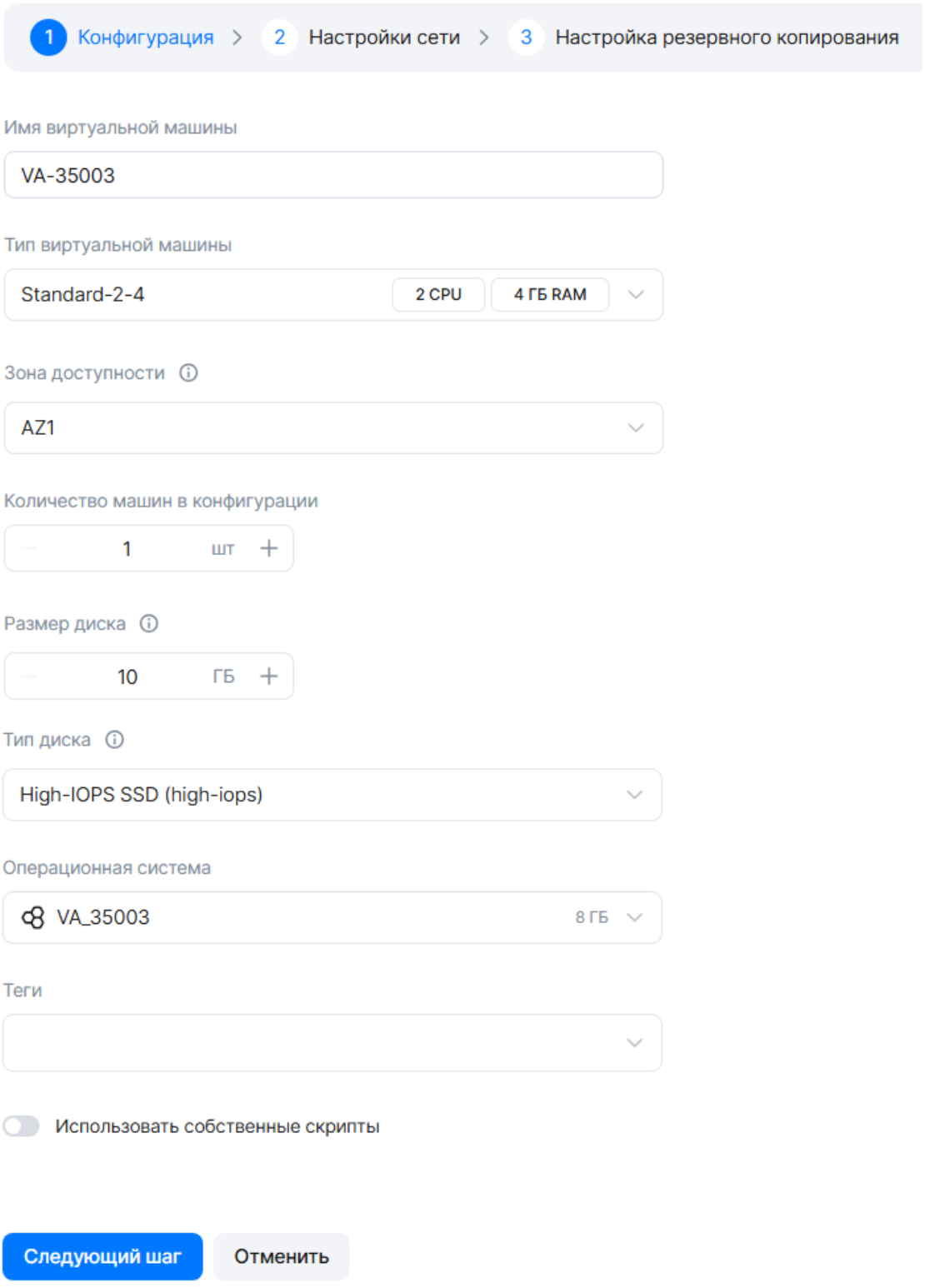


   c. Нажмите **Создать образ**.
6. Создайте ВМ на основе импортированного ранее образа:
   a. Перейдите в раздел **Облачные вычисления** > **Образы**, щелкните значок многоточия рядом с образом и выберите **Создать ВМ из образа** в появившемся меню. Откроется мастер создания ВМ.
   b. На шаге **Конфигурация** укажите конфигурационные параметры ВМ:
      i. В поле **Имя виртуальной машины** введите имя ВМ.
      ii. 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.
      iii. В поле **Зона доступности** выберите необходимую зону.
      iv. В поле **Количество машин в конфигурации** укажите значение 1.
      v. В поле **Размер диска** задайте размер диска ВМ.

vi. В поле **Тип диска** выберите тип диска ВМ.

vii. Убедитесь, что в поле **Операционная система** выбран образ ВМ, который был импортирован ранее.

По окончании ввода нажмите **Следующий шаг**.



c. На шаге **Настройки сети** задайте сетевую конфигурацию ВМ:

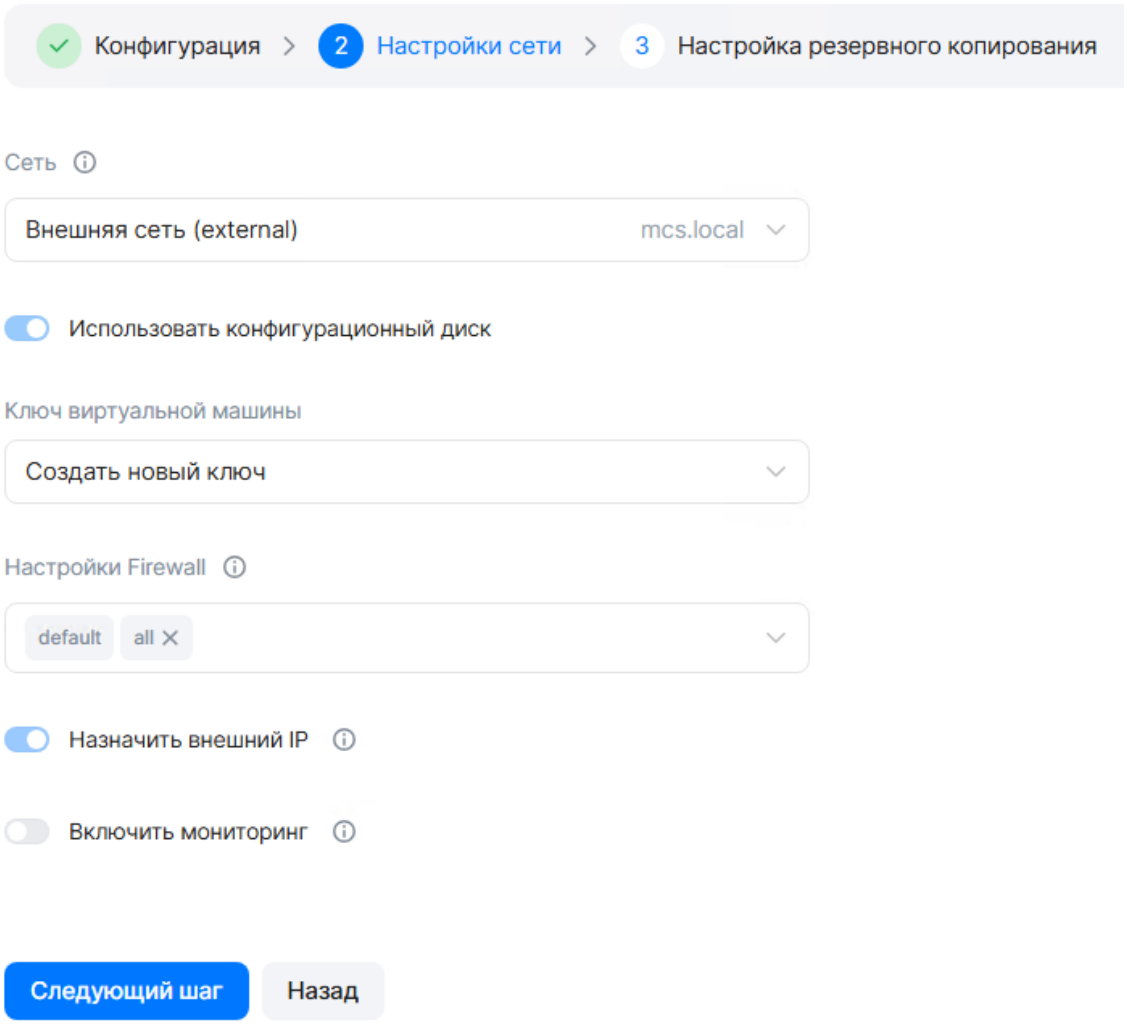
   i. В поле **Сеть** выберите сеть, к которой будет подключена ВМ. Сеть должна обеспечивать связь виртуального устройства с продуктом Кибер Бэкап Облачный и с контроллером VK Cloud.

   ii. В поле **Ключ виртуальной машины** укажите SSH-ключ для доступа к ВМ.

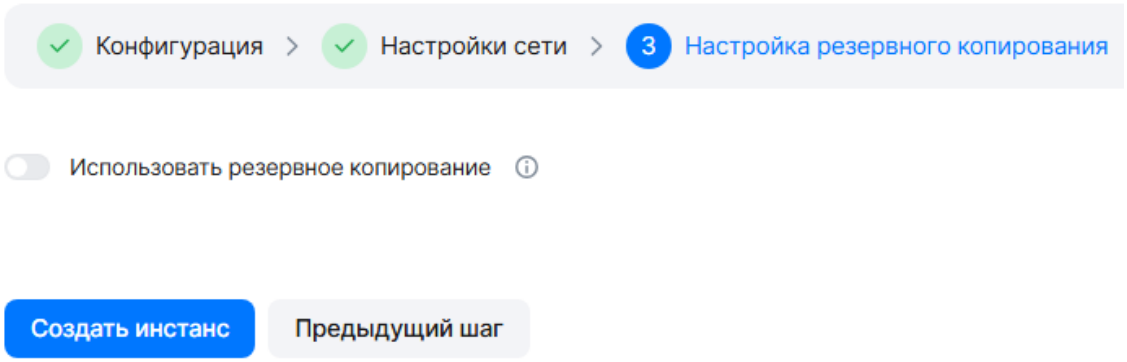
   iii. В поле **Настройки Firewall** выберите группы безопасности. Группы безопасности должны разрешать связь виртуального устройства с продуктом Кибер Бэкап Облачный и с контроллером VK Cloud.

   iv. При необходимости передвиньте переключатель **Назначить внешний IP** в положение "вкл".

   По окончании ввода нажмите **Следующий шаг**.

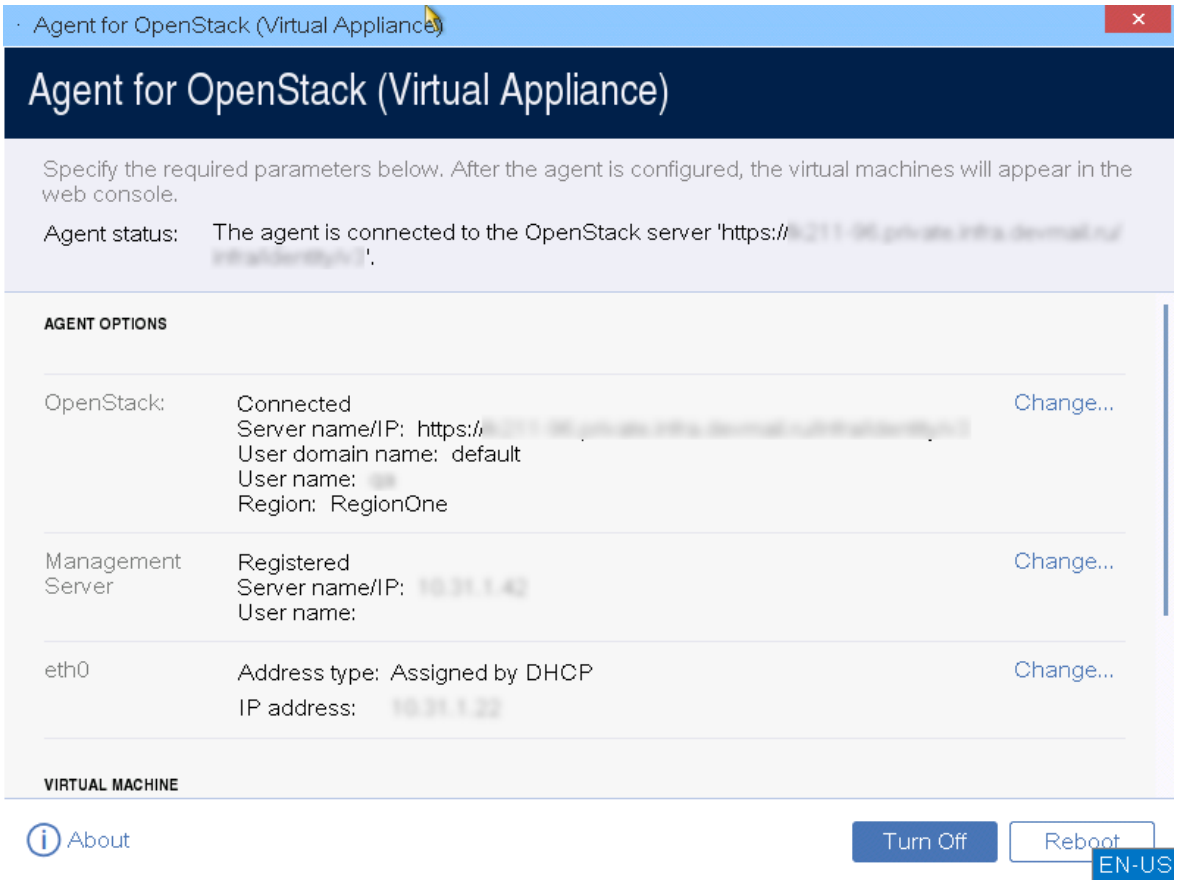


d. На шаге **Настройка резервного копирования** нажмите **Создать инстанс**.



e. Перейдите в раздел **Облачные вычисления** > **Виртуальные машины** и убедитесь, что имя машины с агентом появилось в списке виртуальных машин.

7. Получите URL-адрес API для аутентификации, который будет использоваться виртуальным устройством для взаимодействия с VK Cloud:
   a. Щелкните имя пользователя вверху справа и выберите **Настройки проекта**.
   b. Перейдите на вкладку **Доступ по API**.
   c. Запомните или запишите значение поля **Auth URL**.
8. 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 URL-адрес службы Кибер Бэкап Облачный, 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 консоли службы.
   - **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 **Устройства** появится подраздел **OpenStack (VK Cloud)**;
- в разделе **Настройки** > **Агенты** отобразится агент для OpenStack (VK Cloud).

7.14 Развертывание агента для Basis DynamiX Enterprise

Для резервного копирования данных Basis DynamiX Enterprise понадобятся установленные и настроенные продукты:

- Кибер Бэкап Облачный с лицензией Кибер Бэкап Облачный Виртуальный хост;
- Basis DynamiX Enterprise версии с 3.8.8 по 4.1.

Для корректной работы Кибер Бэкап Облачный и Basis DynamiX Enterprise виртуальное устройство должно отвечать следующим минимальным требованиям:

- Количество центральных процессоров (CPU): 2;
- Объем ОЗУ: 4 ГБ;
- Объем диска: 8 ГБ.

7.14.1 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.

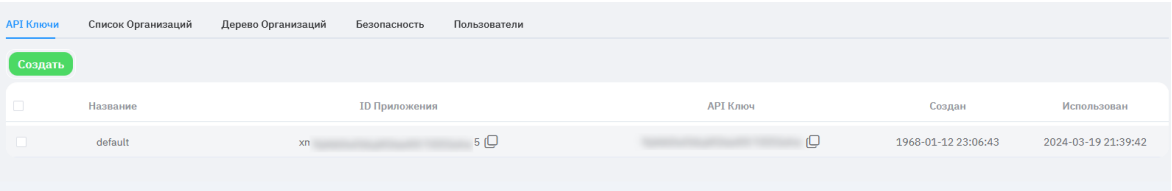
7.14.2 Установка агента для Basis DynamiX Enterprise вручную

Для установки агента понадобится ID приложения Basis DynamiX и ключ API. Чтобы их получить, 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.

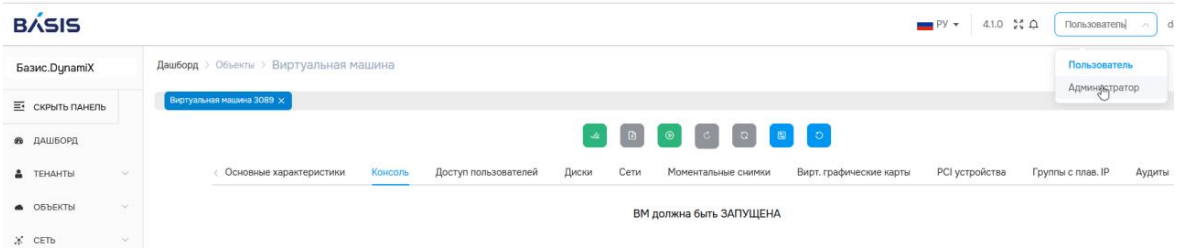
3. Перейдите на вкладку **API Ключи** и нажмите **Создать**.
4. Введите название ключа и нажмите **Enter**.



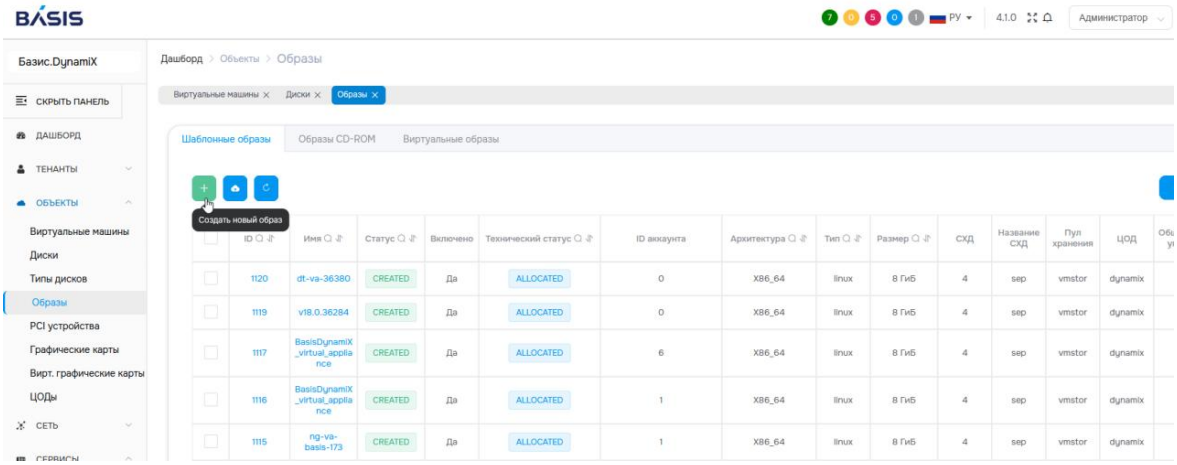
Чтобы установить агент для Basis DynamiX, выполните следующие действия:

1. Щелкните **Устройства** > **Все устройства** > **Добавить** > **Basis DynamiX**.
   Скачайте ZIP-архив с образом агента.
2. Распакуйте ZIP-архив и поместите файл QCOW2 на хост Basis DynamiX, который необходимо защитить.

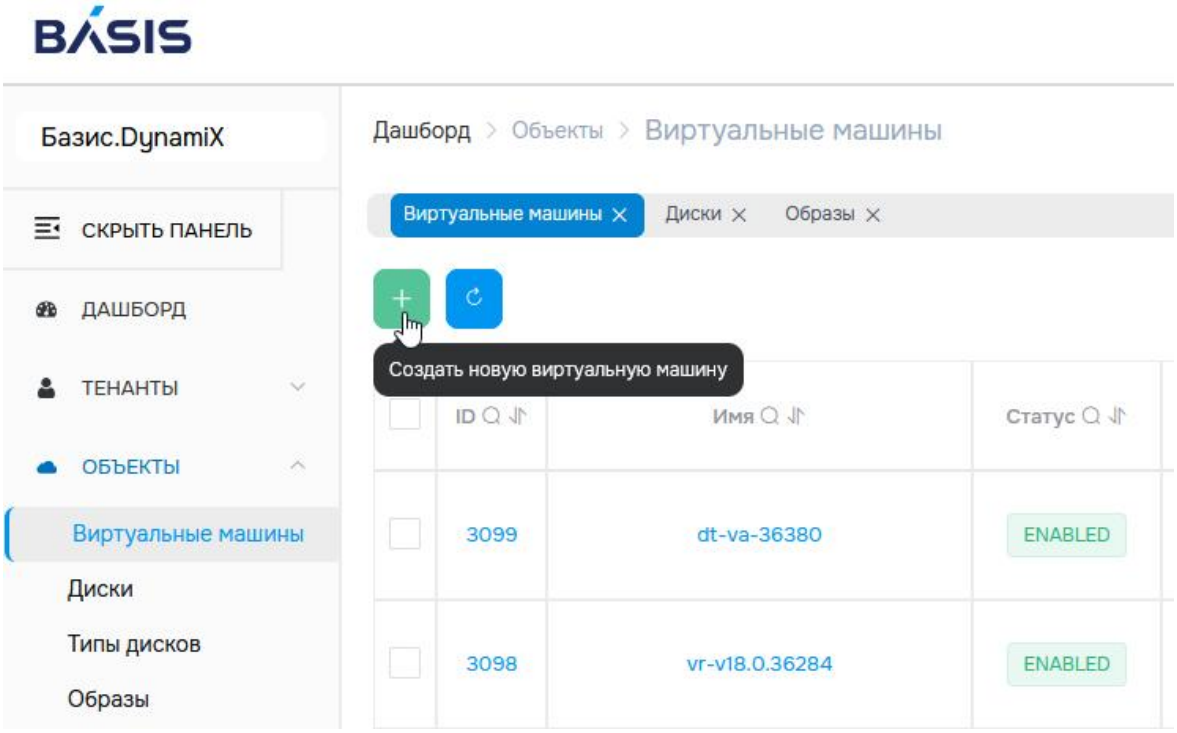
3. В панели управления системой виртуализации Basis DynamiX перейдите в режим администратора.



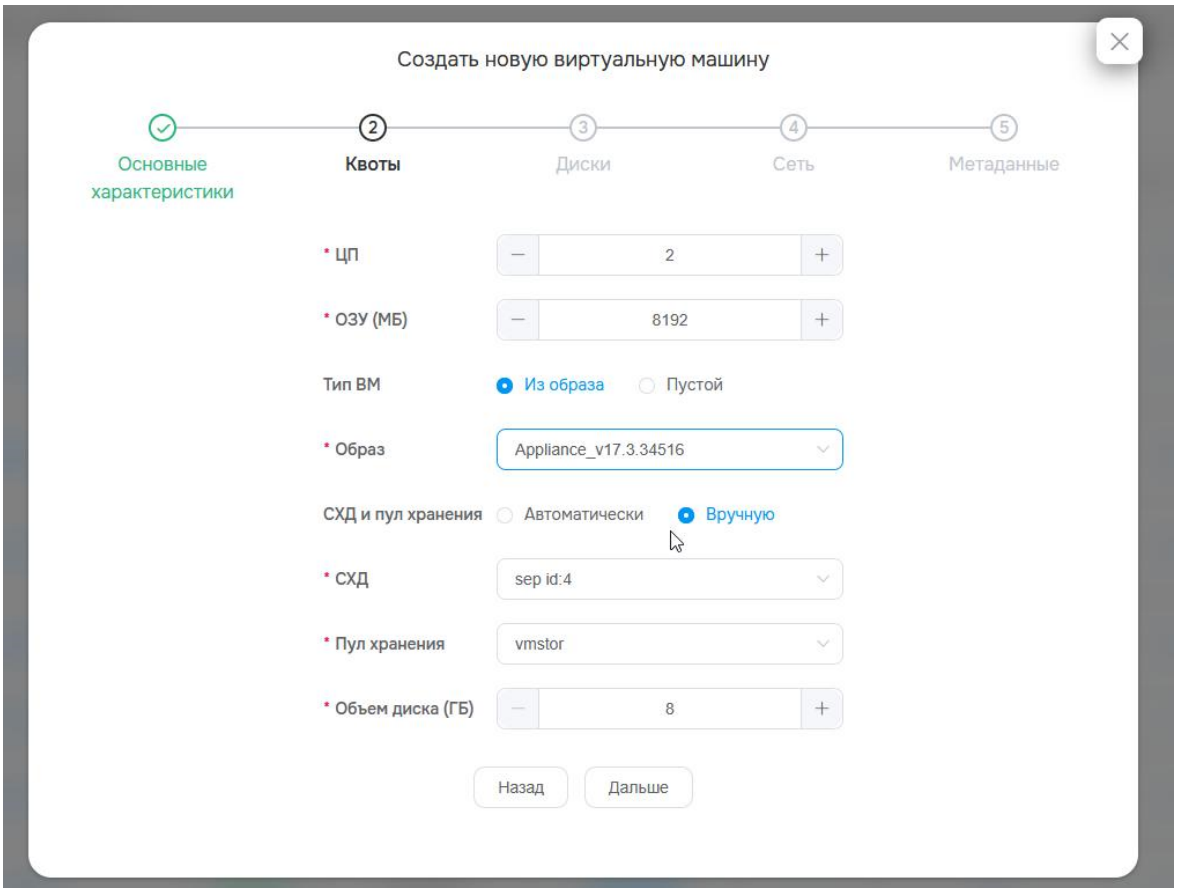
4. Перейдите в раздел **Объекты** > **Образы** и нажмите **Создать новый образ**.



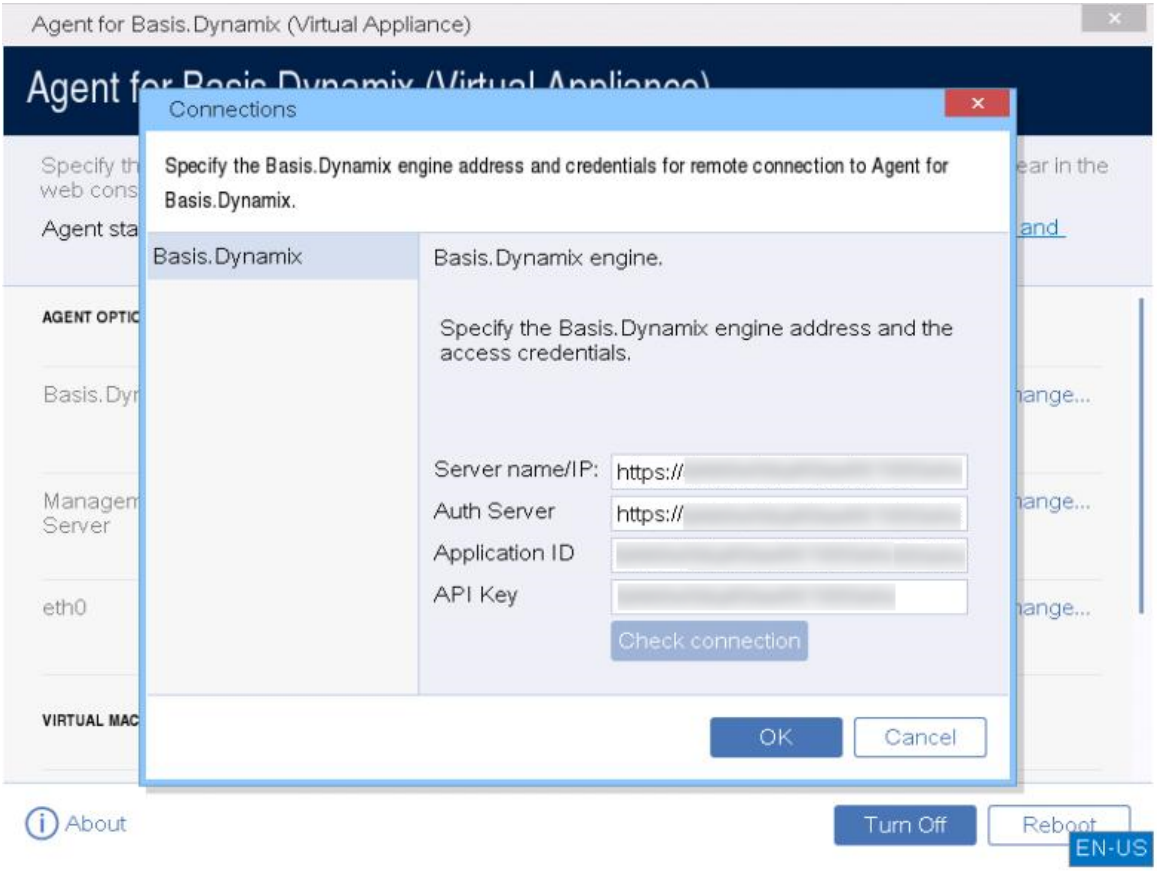
5. В окне создания образа укажите путь к пакету установки агента Basis DynamiX (подробнее см. в документации Basis DynamiX).
6. Перейдите в раздел **Виртуальные машины** и нажмите **Создать новую виртуальную машину**.



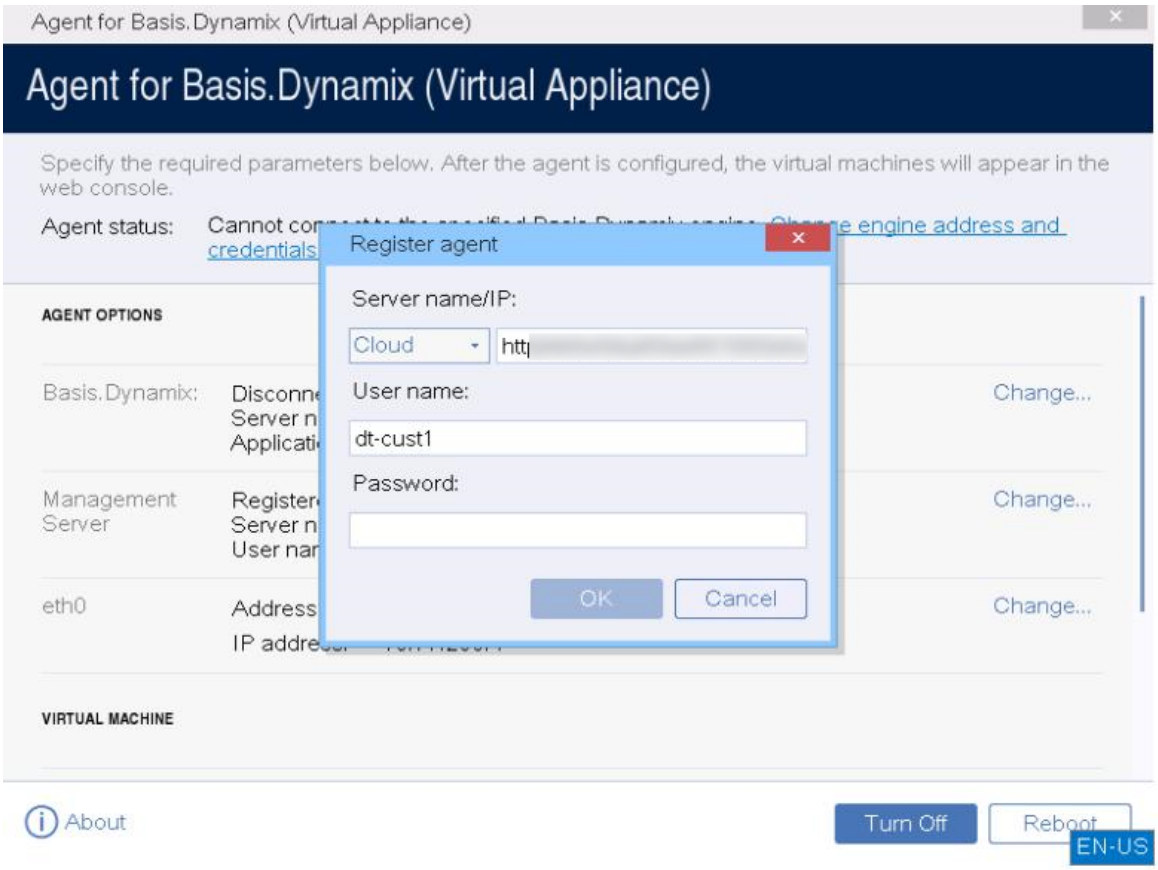
7. В окне создания виртуальной машины на шаге **Квоты** укажите созданный ранее образ ВМ.



8. Укажите остальные настройки для создания шаблона на основе образа виртуального устройства согласно документации Basis DynamiX.
9. Подключитесь к консоли виртуальной машины.
10. В разделе **Basis.Dynamix** нажмите **Change** и укажите IP-адрес сервера платформы виртуализации, ID приложения Basis DynamiX и ключ API.



11. В разделе **Management Server** нажмите **Change** и укажите IP-адрес сервера управления Кибер Бэкап Облачный и учетные данные для подключения к нему.



12. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап Облачный отображаются устройства Basis DynamiX.

7.15 Развертывание агента для Кибер Инфраструктуры (виртуальное устройство)

Для развертывания агента для Кибер Инфраструктуры вам понадобится установленная и настроенная система Кибер Инфраструктура версии 6.0 и выше.

Установка проводится в несколько этапов:

- Создание и регистрация пользователя в Кибер Инфраструктуре.
- Создание виртуального устройства.
- Подключение виртуального устройства к службе Кибер Бэкап Облачный.

7.15.1 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:
   a. Создайте RC-файл для OpenStack, в котором указаны учетные данные администратора системы.

   ```
   su - vstoradmin
   kolla-ansible post-deploy
   exit
   ```

   b. 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     |
+--------------+-----------------+-------+-----------------+---------+--------+-----------+
```

7.15.2 Создание виртуального устройства для Кибер Инфраструктуры

Для создания виртуального устройства:

1. Скачайте дистрибутив для резервного копирования с Кибер Инфраструктурой (архив формата ZIP, например CIAppliance.zip), 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. В поле **Имя** введите наименование виртуальной машины.
5. В поле **Выберите дистрибутив ОС** укажите нужный дистрибутив для виртуальной машины.
6. Перейдите на вкладку **Виртуальные машины** и выберите **Создать виртуальную машину**.
7. В поле **Образ** укажите нужный образ виртуальной машины.
8. Укажите параметры виртуальной машины на вкладке **Тип ВМ**. Для промышленных сборок рекомендуется указывать не менее 2-х ЦП и не менее 4 ГБ памяти.
9. На вкладке **Сетевые интерфейсы** укажите подходящий сетевой интерфейс. Нажмите **Добавить** и выберите нужный сетевой интерфейс. Убедитесь, что сеть виртуального устройства имеет доступ к внутренним интерфейсам кластера (это можно сделать в меню

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.

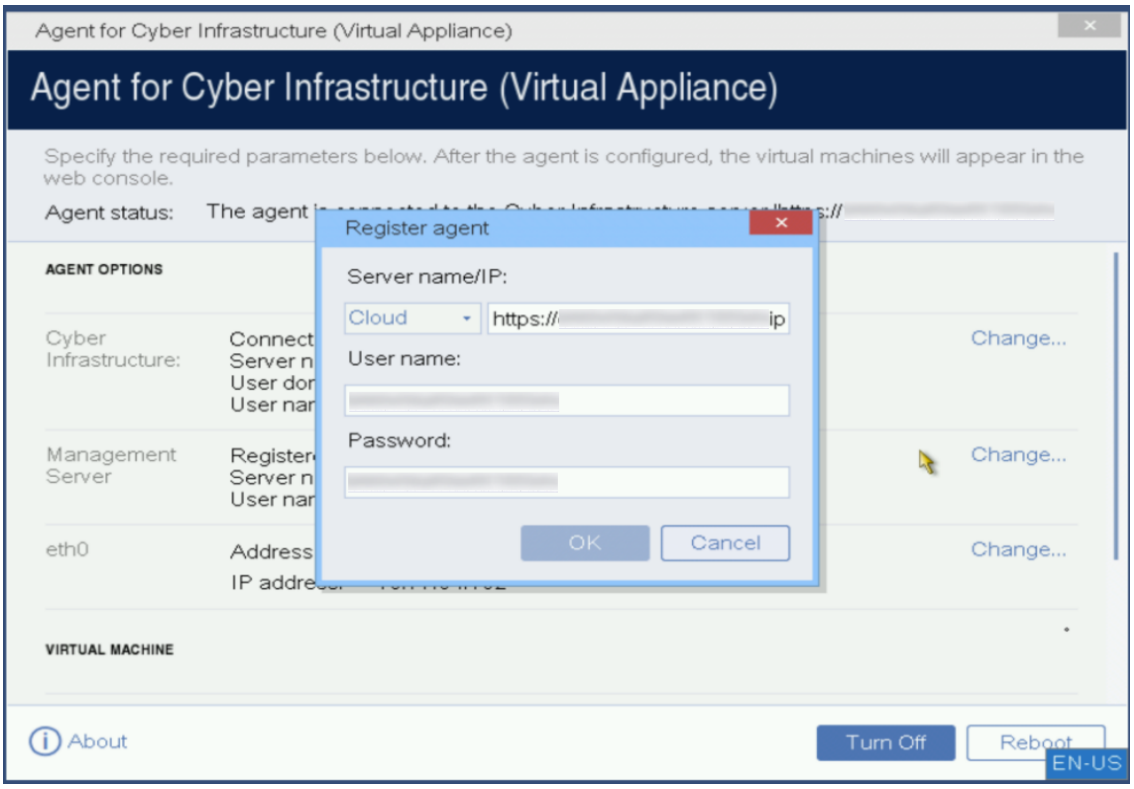
10. Введите имя виртуальной машины и по окончании ввода данных нажмите **Развернуть**.
11. Перейдите снова в **Виртуальные машины** и убедитесь, что имя виртуальной машины появилось в списке виртуальных машин.

Примечание
Убедитесь, что в системе установлено корректное время. При необходимости установите часовой пояс. После изменения часового пояса необходимо перезагрузить систему.

7.15.3 Подключение виртуального устройства к службе Кибер Бэкап Облачный

1. Перейдите в раздел **Вычисления** > **Виртуальные машины**.
2. В списке виртуальных машин щелкните по имени виртуальной машины, а затем нажмите **Консоль**.
3. В разделе **Cyber Infrastructure** нажмите **Change** и укажите следующие данные:
   - В поле **Server name/IP** введите адрес сервера управления Кибер Инфраструктуры в формате https://<address>:5000.
   - В поле **User domain name** укажите имя системного домена.
   - В полях **User name** и **Password** укажите учетные данные специального пользователя для подключения к серверу управления Кибер Инфраструктуры (см. раздел "Создание и регистрация пользователя" (стр. 96)).

   Нажмите **Check connection**, чтобы проверить соединение и затем нажмите **OK**.
4. В разделе **Management Server** нажмите **Change** и укажите данные для подключения к службе Кибер Бэкап Облачный и нажмите **OK**.



5. В разделе **VIRTUAL MACHINE** > **Name** нажмите **Change**, в открывшемся окне **Rename Agent for Cyber Infrastructure** введите имя агента Кибер Инфраструктуры и нажмите **OK**.
6. По окончании настроек откройте веб-консоль Кибер Бэкап Облачный и выберите вкладку **Устройства**. Убедитесь, что в подменю слева появилась вкладка **Cyber Infrastructure**.
7. Перейдите в **Настройки** > **Агенты** и убедитесь, что в списке агентов появился агент для резервного копирования Кибер Инфраструктуры.

7.16 Развертывание агента для Proxmox

Для работы с виртуальными машинами на хосте Proxmox необходимо развернуть виртуальное устройство – виртуальную машину с агентом Кибер Бэкап Облачный.

7.16.1 Общие сведения

1. Для резервного копирования и восстановления данных Proxmox VE понадобятся установленные и настроенные продукты:
   - Кибер Бэкап Облачный с лицензией Кибер Бэкап Облачный Виртуальный хост;
   - Агент для Proxmox версии 18.1;
   - Система управления виртуализацией.
2. Поддерживаются следующие системы управления виртуализацией:
   - Proxmox VE версии 7.2, 7.3, 7.4;
   - Альт Виртуализация PVE версии 10.2;

- Альт Виртуализация PVE версии 11.

3. Для корректной работы Кибер Бэкап Облачный и Proxmox VE виртуальное устройство должно отвечать следующим минимальным требованиям:
   - Количество центральных процессоров (CPU): 2;
   - Объем ОЗУ: 4 ГБ;
   - Объем диска: 8 ГБ.

7.16.2 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.

7.16.3 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 Облачный. В таких случаях необходимо вручную изменить идентификаторы на уникальные.

7.16.4 Установка агента для Proxmox вручную

Чтобы установить вручную агент для Proxmox, выполните следующие действия:

1. Щелкните **Устройства** > **Все устройства** > **Добавить** > **Proxmox VE**.
   Скачайте ZIP-архив с образом агента.
2. Распакуйте ZIP-архив и поместите файл QCOW2 на хост Proxmox VE, который необходимо защитить.
3. Войдите как администратор в панель управления системы виртуализации Proxmox VE.
4. Создайте виртуальную машину без подключенных дисков:
   a. В верхнем левом углу панели управления нажмите **Create VM**.
   b. Укажите следующие данные в окне создания ВМ:
      i. На вкладке **General** задайте имя ВМ.
      ii. На вкладке **OS** выберите пункт **Do not use any media**.

iii. На вкладке **System** в поле **SCSI Controller** выберите один из поддерживаемых контроллеров: VirtIO SCSI, VirtIO SCSI Single, LSI 53C895A, VMware PVSCSI.

iv. На вкладке **Disks** удалите диск, который предлагается создать вместе с ВМ.

v. На вкладке **CPU** в поле **Cores** укажите минимум 2 ядра процессора.

vi. 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).

5. Загрузите диск установки агента на сервер системы виртуализации Proxmox VE. Например, выполните команду:

```
cd /mnt/pve/nfsproxmox/template
wget адрес_архива/ProxmoxAppliance.qcow2
```

6. Подключите диск агента для ранее созданной ВМ. Например, выполните команду:

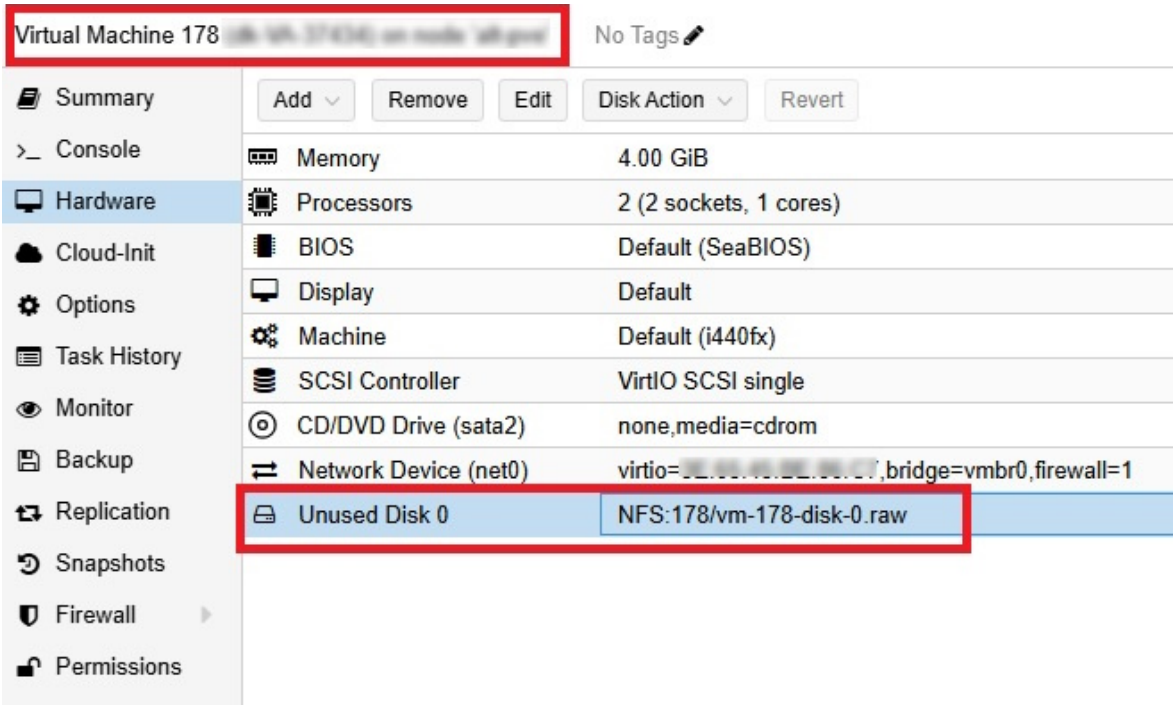
```
qm importdisk 178 ProxmoxAppliance.qcow2 NFS
```

Где:

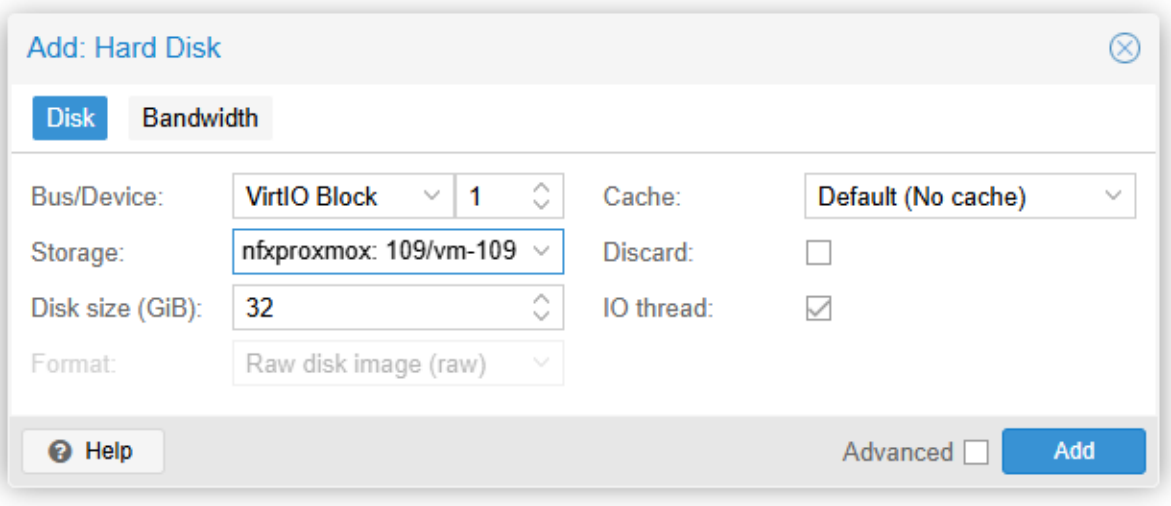
- 178 – ID виртуальной машины, созданной на шаге 3 данной инструкции;
- ProxmoxAppliance.qcow2 – имя пакета установки агента;
- NFS – имя хранилища в Proxmox, куда будет помещён диск.

7. Выберите в списке созданную виртуальную машину и перейдите в раздел **Hardware**.

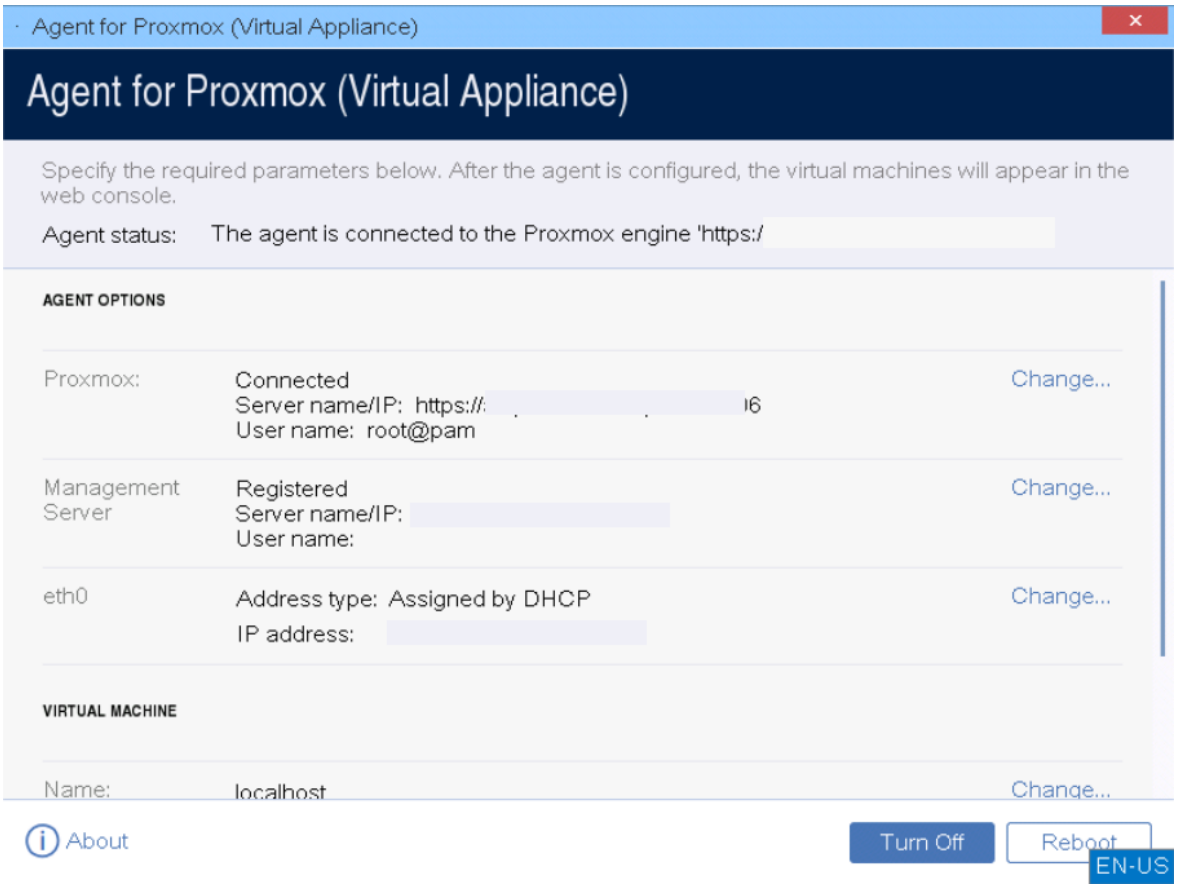
8. Откройте подключенный диск с именем **Unused Disk 0**.



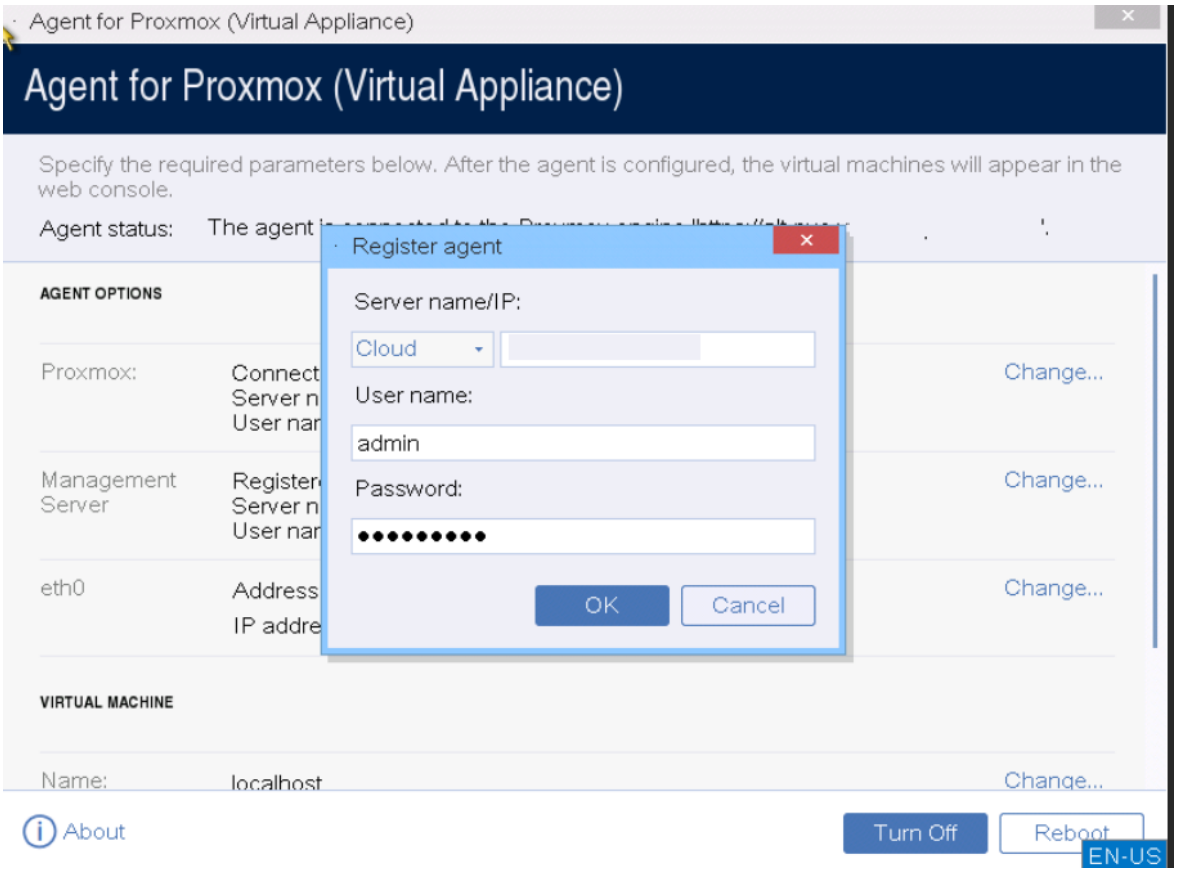
9. В поле **Bus/Device** выберите **VirtIO Block**.



10. Установите для нового диска первый приоритет в порядке загрузки:
    a. Выберите в списке виртуальную машину и нажмите **Options**.
    b. Выберите **Boot Order** и нажмите **Edit**.
    c. Перенесите диск, импортированный из пакета установки, на первое место в списке и поставьте для него галочку **Enabled**.
11. Подключитесь к консоли виртуальной машины.
12. 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.



13. В разделе **Management Server** нажмите **Change** и укажите адрес и учетные данные службы Кибер Бэкап Облачный для доступа к ней.
    a. В поле **Server name/IP** выберите **Cloud**, а затем укажите адрес службы Кибер Бэкап Облачный.
    b. В полях **User name** и **Password** введите учетные данные для учетной записи в службе Кибер Бэкап Облачный.
    c. Нажмите кнопку **OK**.



14. [Необязательно] В поле **Name** щелкните **Change** и измените имя виртуального устройства по умолчанию (**localhost**). Это имя показано в консоли службы Кибер Бэкап Облачный.
15. [Необязательно] В поле **Time zone** щелкните **Change**, а затем выберите часовой пояс, чтобы запланированные операции выполнялись в правильное время.
16. Перезапустите виртуальную машину.
17. Убедитесь, что в разделе **Устройства** веб-консоли Кибер Бэкап Облачный отображаются устройства Proxmox VE.

7.17 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.

7.17.1 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 2003 или более позднего выпуска.
- Вы входите в состав группы **Администраторы домена**.
- Вы скачали программу установки **Все агенты для Windows**. Ссылка для скачивания доступна на странице **Добавить устройства** в консоли службы.

7.17.2 Шаг 1. Формирование маркера регистрации

Сформируйте маркер регистрации согласно описанию в разделе "Управление маркерами регистрации" (стр. 113).

7.17.3 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. Щелкните **Создать MST- и MSI-файлы для автоматической установки**.
5. Щелкните **Указать** рядом с пунктом **Настройки регистрации** и введите созданный маркер. Можно изменить способ регистрации машины в службе Кибер Бэкап Облачный с **Использовать маркер регистрации** (по умолчанию) на **Использовать учетные данные** или **Пропустить регистрацию**. Выбор параметра **Пропустить регистрацию** предполагает, что вы зарегистрируете машину позже.
6. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **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.

7.17.4 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 щелкните **Пользователи и компьютеры Active Directory** (в ОС Windows Server 2003) или **Управление групповой политикой** (в Windows Server 2008 или более поздних версий).

4. В Windows Server 2003:
   - Правой кнопкой мыши щелкните имя домена или организационной единицы и выберите пункт **Свойства**. В диалоговом окне перейдите на вкладку **Групповая политика** и нажмите кнопку **Создать**.

   В Windows Server 2008 или более поздних версий:
   - Правой кнопкой мыши щелкните имя домена или организационной единицы, а затем щелкните **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 с помощью описанных ниже действий:
   - В Windows Server 2003 щелкните объект групповой политики, а затем выберите **Изменить**.
   - В Windows Server 2008 или более поздних версий в разделе **Объекты групповой политики** щелкните правой кнопкой мыши объект групповой политики, а затем щелкните **Изменить**.
7. В оснастке «Редактор объектов групповой политики» разверните узел **Конфигурация компьютера**.
8. В Windows Server 2003 и Windows Server 2008:
   - Разверните узел **Конфигурация программ**.

   В Windows Server 2012 или более поздних версий:
   - Разверните узел **Политики** > **Конфигурация программ**.
9. Щелкните правой кнопкой мыши узел **Установка программ**, выберите пункт **Создать**, затем щелкните **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 **OK**.
12. На вкладке **Изменения** нажмите кнопку **Добавить** и выберите созданное ранее MST-преобразование.
13. Нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Развертывание программ**.

7.18 Обновление агентов

Агенты версии, предшествующей 17.1.33712

Агенты обновляются до последней версии при условии, что они включены. Выключенные агенты не будут автоматически обновлены после включения.

Агенты версии 17.1.33712 и более поздней

Включенные агенты обновляются до последней версии. Выключенные агенты будут автоматически обновлены после включения.

7.18.1 Предварительные требования

Для работы функций Кибер Бэкап Облачный на машинах Windows требуется распространяемый компонент Microsoft Visual C++ 2017. 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.

7.18.2 Порядок обновления агента через консоль службы

1. Щелкните **Настройки** > **Агенты**.

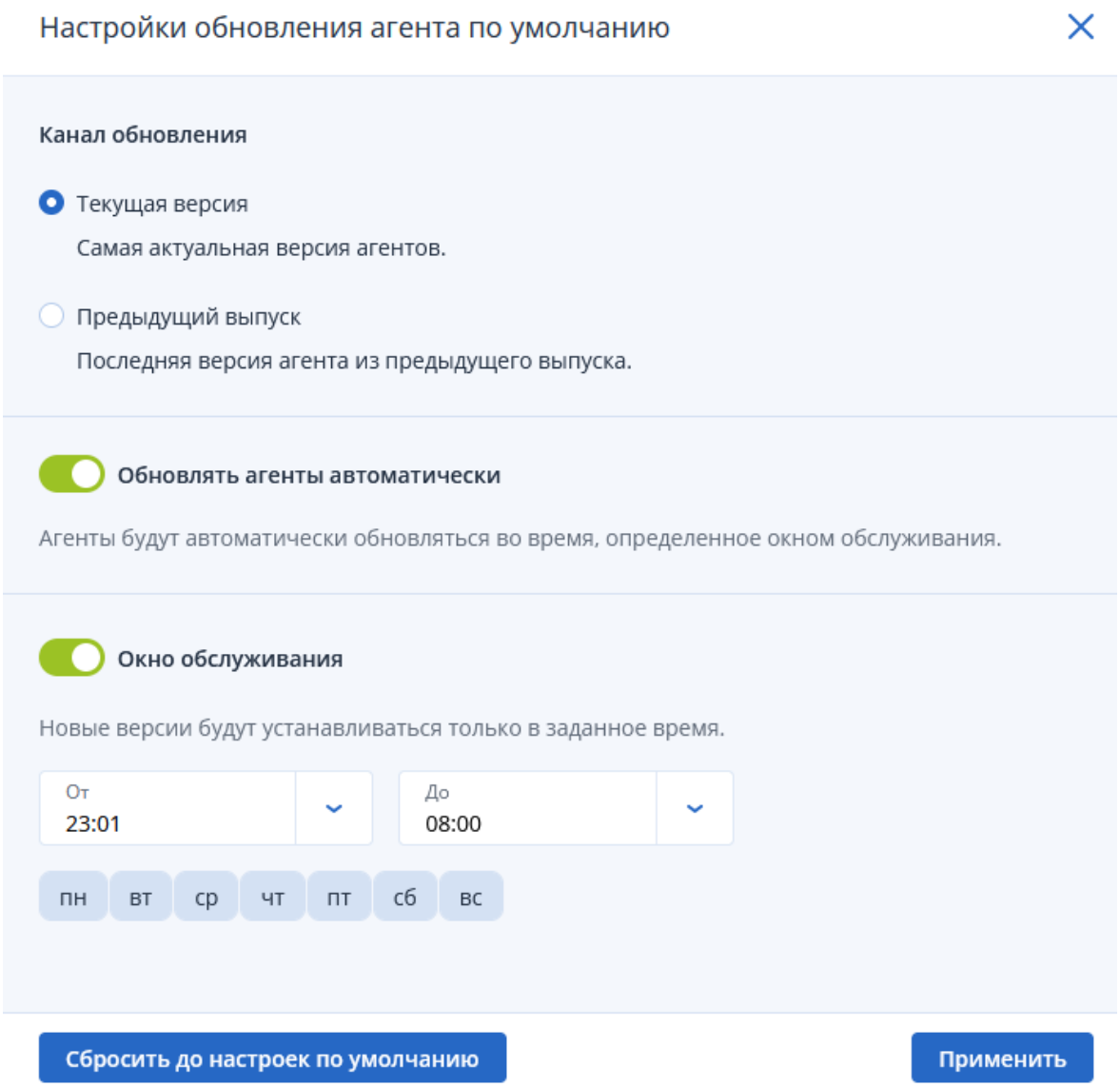
   В программе будет выведен список машин. Машины с агентами устаревших версий будут помечены оранжевым восклицательным знаком.
2. Выберите машины, на которых нужно обновить агенты. Машины должны быть включены.
3. Щелкните **Обновить агент**.

Примечание
При выполнении обновления все выполняющиеся резервные копии завершатся сбоем.

7.18.3 Порядок изменения настроек обновления агента по умолчанию

Настройки обновления агента по умолчанию наследуются от родительского тенанта партнера. Чтобы изменить их, выполните следующие действия:

1. Перейдите в раздел **Настройки** > **Агенты** и нажмите **Изменить настройки обновления агента по умолчанию**.



2. В разделе **Канал обновления** укажите версию, до которой следует обновлять агенты.
3. Для автоматического обновления установите флажок **Обновлять агенты автоматически**.
4. Чтобы задать дни и время для автоматического обновления, установите флажок **Окно обслуживания** и укажите необходимые значения.
5. Нажмите **Применить**.

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

1. Щелкните **Настройки** > **Агенты**, выберите агент, который необходимо обновить, затем щелкните **Сведения** и изучите данные раздела **Назначенные виртуальные машины**. После обновления необходимо заново ввести эти настройки.

a. Запомните положение переключателя **Автоматическое назначение**.

b. Чтобы узнать, какие виртуальные машины вручную назначены этому агенту, щелкните ссылку **Назначено:**. В программе будет выведен список назначенных виртуальных машин. Запишите виртуальные машины, которые имеют букву (M) после имени агента в столбце **Агент**.

2. Удалите агент для VMware (виртуальное устройство), как описано в разделе "Удаление агентов". В шаге 5 удалите агент из раздела **Настройки** > **Агенты**, даже если вы планируете установить агент снова.
3. Разверните агент для VMware (виртуальное устройство), как описано в разделе "Развертывание шаблона OVF".
4. Настройте агент для VMware (виртуальное устройство), как описано в разделе "Настройка виртуального устройства".

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

   a. Добавьте на виртуальное устройство диск с локальным хранилищем данных.

   b. Последовательно выберите пункты **Обновить** > **Создать хранилище** > **Подключить**.

   c. В программе отображается оригинальная **буква** и **метка** диска. Не меняйте их.

   d. Нажмите кнопку **OK**.

5. Щелкните **Настройки** > **Агенты**, выберите агент, который необходимо обновить, затем щелкните **Сведения** и восстановите настройки, которые вы записали на шаге 1. Если агенту были вручную назначены виртуальные машины, назначьте их снова, как описано в разделе «Привязка виртуальной машины».

   По окончании настройки агента планы защиты, которые были применены к прежнему агенту, будут автоматически применены к новому агенту.
6. Для планов с включенным резервным копированием с поддержкой приложений необходимо заново ввести учетные данные гостевой ОС. Измените эти планы и заново введите учетные данные.
7. Для планов, которые выполняют резервное копирование конфигурации ESXi, необходимо заново ввести пароль привилегированного пользователя (root). Измените эти планы и заново введите пароль.

7.19 Удаление агентов

7.19.1 В Windows

Если нужно удалить отдельные компоненты продукта (например, один из агентов или Кибер Бэкап Монитор), запустите программу установки **Все агенты для Windows**, выберите изменение продукта и отмените выбор компонентов, которые нужно удалить. Ссылка на программу установки доступна на странице **Загрузки** (щелкните значок учетной записи в правом верхнем углу и выберите пункт > **Загрузки**).

Если нужно удалить все компоненты продукта с машины, следуйте приведенным ниже инструкциям.

1. Войдите как администратор.
2. Откройте **Панель управления** и выберите **Программы и компоненты** (**Установка и удаление программ** в Windows XP) > **Агент Киберпротект Кибер Бэкап Облачный** > **Удалить**.
3. [Для агента, защищенного паролем] Укажите пароль, необходимый для удаления агента, и щелкните **Далее**.
4. [Необязательно] Установите флажок **Удалить журналы и параметры конфигурации**.

   Если планируется установить агент снова, не устанавливайте этот флажок. Если установить флажок, в консоли резервного копирования может быть создана точная копия (дубликат) машины. При этом резервные копии старой машины могут быть не связаны с новой машиной.
5. Щелкните **Удалить**.

7.19.2 В ОС Linux

1. В качестве привилегированного пользователя выполните **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Необязательно] Установите флажок **Удалить все элементы трассировки продукта (журналы, задания, хранилища, параметры конфигурации продукта)**.

   Если планируется установить агент снова, не устанавливайте этот флажок. Если установить флажок, в консоли резервного копирования может быть создана точная копия (дубликат) машины. При этом резервные копии старой машины могут быть не связаны с новой машиной.
3. Подтвердите операцию.

7.19.3 Удаление агента для VMware (виртуальное устройство)

1. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
2. Если виртуальное устройство включено, щелкните его правой кнопкой мыши, а затем выберите пункт **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.
   a. Щелкните виртуальное устройство правой кнопкой мыши и выберите пункт **Изменить настройки**.
   b. Выберите диск с хранилищем и щелкните **Удалить**. В разделе **Параметры удаления** нажмите кнопку **Удалить из виртуальной машины**.
   c. Нажмите кнопку **OK**.

   В результате диск остается в хранилище данных. Можно подключить диск к другому виртуальному устройству.
4. Щелкните виртуальное устройство правой кнопкой мыши и выберите пункт **Удалить с диска**. Подтвердите операцию.

5. [Необязательно] Если планируется установить агент снова, пропустите этот шаг. В противном случае в консоли службы щелкните **Хранилище резервных копий** > **Хранилища** и удалите хранилище, соответствующее локально прикрепленному хранилищу.

7.19.4 Удаление машин с консоли службы

После удаления агента его регистрация в службе Кибер Бэкап Облачный будет отменена. Кроме того, из консоли службы будет автоматически удалена машина, на которой был установлен агент.

Но если при выполнении этой операции подключение к серверу будет утрачено (например, из-за проблемы в сети), агент может удалиться, но его машина при этом может продолжать отображаться в консоли службы. В этом случае необходимо удалить машину с консоли службы вручную.

Порядок удаления машины с консоли службы вручную

1. Войдите в службу Кибер Бэкап Облачный как администратор.
2. В консоли службы последовательно выберите пункты **Настройки** > **Агенты**.
3. Выберите машину, на которой установлен агент.
4. Щелкните **Удалить**.

7.20 Изменение квоты службы машин

Квота службы автоматически назначается при первом применении плана защиты к машине.

Первоначальное назначение можно изменить позже вручную. Например, чтобы применить более расширенный план защиты к той же машине, вам может понадобиться обновить квоту службы машины. Если функции, которые необходимы для этого плана защиты, не поддерживаются текущей назначенной квотой службы, план защиты завершится сбоем. Как вариант, можно изменить квоту службы при условии покупки соответствующих дополнительных квот после назначения первоначальной. Например, виртуальной машине назначена квота **Рабочие станции**. После покупки квоты **Виртуальные машины**, ее можно вручную назначить этой машине. Как вариант, можно освободить текущую назначенную квоту службы, а затем назначить ее другой машине.

Квоту службы можно изменить для отдельной машины или для группы машин.

Порядок изменения квоты для службы отдельной машины

1. В консоли службы Кибер Бэкап Облачный откройте **Устройства**.
2. Выберите желаемую машину и щелкните **Сведения**.
3. В разделе **Квота службы** щелкните **Изменить**.
4. В окне **Изменить лицензию** выберите желаемую квоту службы или пункт **Без квоты**, а затем щелкните **Изменить**.

Порядок изменения квоты службы для группы машин

1. В консоли службы Кибер Бэкап Облачный откройте **Устройства**.
2. Выберите несколько машин, а затем щелкните **Назначить квоту**.
3. В окне **Изменить лицензию** выберите желаемую квоту службы или пункт **Без квоты**, а затем щелкните **Изменить**.

7.21 Управление маркерами регистрации

Маркер регистрации – это уникальная последовательность из 12 цифро-буквенных символов, разделенных дефисами на три части (например, 7A85-70B2-445F). Его можно создать для пользователя и затем указать при развертывании агента или виртуального устройства, не указывая и не сохраняя при этом имя учетной записи и пароль соответствующего пользователя. Маркер обладает ограниченным сроком действия (от 1 минуты до 12 месяцев), который задается при его создании, и удаляется автоматически по истечении этого срока. При необходимости можно создать несколько маркеров с разным сроком действия. С помощью одного и того же маркера, срок действия которого еще не истек, можно зарегистрировать любое количество агентов и виртуальных устройств.

Для создания маркера регистрации выполните следующие действия:

1. Войдите в консоль службы с учетными данными той учетной записи, для которой необходимо создать маркер.
2. Перейдите в раздел **Все устройства** и нажмите **Добавить** вверху справа.
3. Прокрутите вниз до области **Маркер регистрации** и нажмите **Создать**.
   Если вы вошли как администратор партнера, вы можете сгенерировать маркеры от имени любого пользователя в клиентах, которыми вы можете управлять. Для этого выберите имя пользователя в раскрывающемся списке, а затем нажмите **Создать**.
4. Укажите срок действия маркера и нажмите **Сгенерировать маркер**.
5. Скопируйте маркер или запишите его. Сохраните маркер, если он понадобится в будущем.

Для просмотра маркеров регистрации можно нажать **Управление активными маркерами** в области **Маркеры регистрации**. Имейте в виду, что из соображений безопасности полные значения маркеров не отображаются. При необходимости маркер можно удалить, выбрав его в списке и нажав **Удалить**.

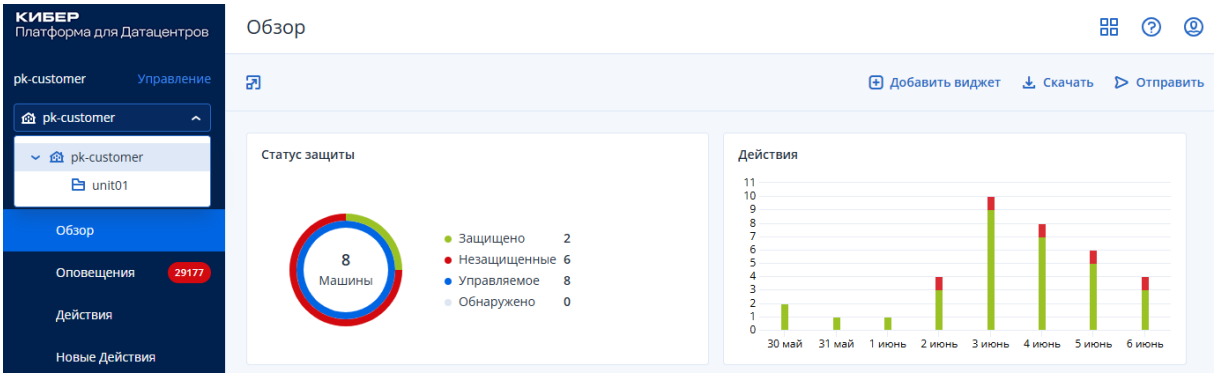
8 Консоль службы

В консоли службы можно управлять устройствами и планами защиты, изменять настройки защиты, настраивать отчет и проверять хранилище резервных копий.

На панели мониторинга вы найдете самую важную информацию о вашей защите.

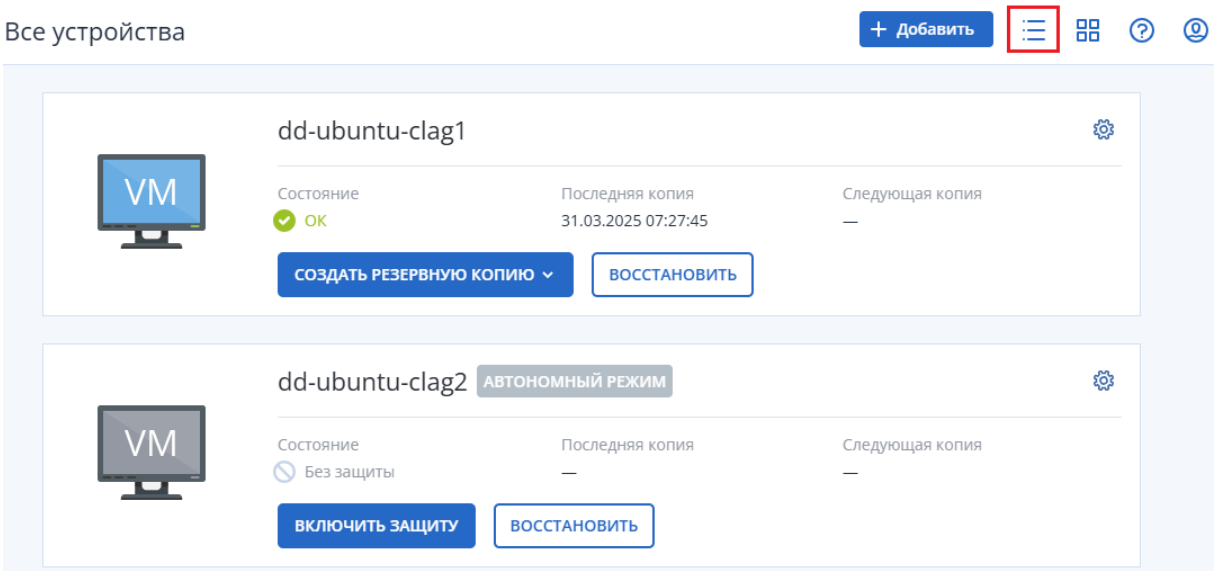
В консоли службы можно получить доступ к дополнительным службам или функциям Кибер Бэкап Облачный. Их тип и количество зависят от лицензии Кибер Бэкап Облачный.

В зависимости от разрешений доступа можно управлять защитой одного или нескольких клиентов пользователя или защитой отделов в клиенте. Для переключения уровня иерархии воспользуйтесь раскрывающимся списком в меню навигации. Показаны только те уровни, к которым у вас есть доступ. Откройте портал управления и щелкните **Управление**.

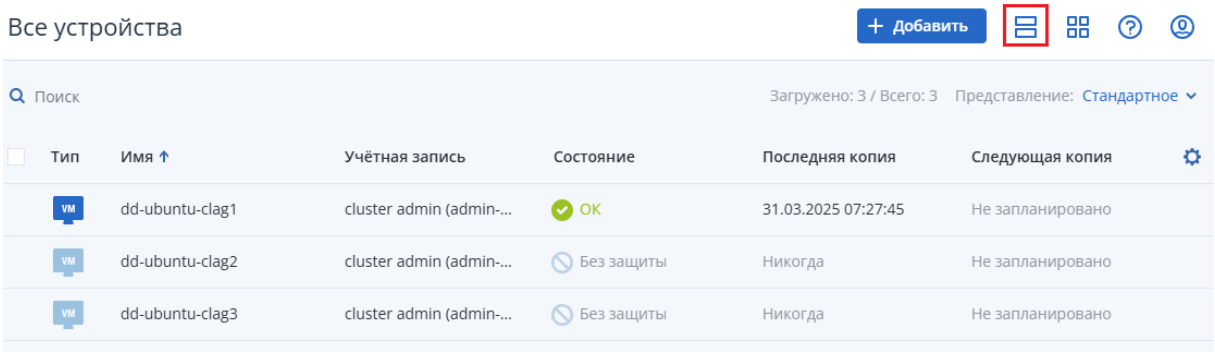


Раздел **Устройства** доступен в простом и табличном представлении. Для переключения между ними используется значок в правом верхнем углу.

В простом представлении отображаются всего несколько машин.



Табличное представление включается автоматически, когда появляются машины в большом количестве.



В обоих представлениях доступен один и тот же набор функций и операций. В этом документе описан порядок вызова различных команд из табличного представления.

Порядок удаления машины из консоли службы

1. Установите флажок рядом с желаемой машиной.
2. Щелкните **Удалить** и подтвердите свой выбор.

Внимание
После удаления машины из консоли службы агент защиты на ней не удаляется. Кроме того, не удаляются планы защиты, примененные к этой машине. Аналогично, резервные копии удаленной машины не удаляются.

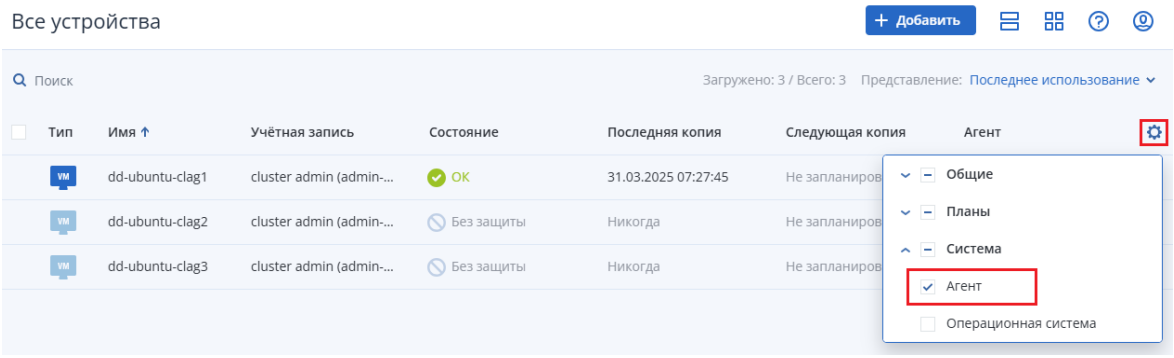
Резервные копии хостов ESXi и виртуальных машин на указанных ниже платформах виртуализации могут создаваться агентом, который не установлен на них, т. е. в режиме без агента:

- Hyper-V
- VMware
- Red Hat Virtualization/oVirt

Такие машины невозможно удалить по отдельности. Чтобы удалить их, необходимо найти и удалить машину, на которой установлен соответствующий агент (агент для Hyper-V, агент для VMware или агент для oVirt).

Порядок удаления виртуальной машины или хоста ESXi без агента

1. В разделе **Устройства** выберите **Все устройства**.
2. Щелкните значок шестерни в верхнем правом углу и активируйте столбец **Агент**.



3. В столбце **Агент** щелкните имя машины, на которой установлен соответствующий агент.
4. Удалите эту машину с консоли службы. Это также приведет к удалению всех машин, для которых резервная копия создана собственным агентом.
5. Удалите агент с удаленной машины, как описано в разделе "Удаление агентов" (стр. 110).

9 Группы устройств

Примечание
Эта функциональность доступна только в выпусках Advanced службы Кибер Бэкап Облачный.

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 **Все устройства** невозможно создать группу.

Одно устройство может входить в несколько групп.

9.1 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.

9.2 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.

9.3 Создание статической группы

1. Нажмите **Устройства** и выберите встроенную группу, которая содержит устройства, для которых вы хотите создать статическую группу.
2. Нажмите на значок шестеренки около группы, в которой вы хотите создать группу.
3. Нажмите кнопку **Новая группа**.
4. Укажите имя группы и затем нажмите кнопку **OK**.

   Новая группа появится на дереве групп.

9.4 Добавление устройств в статические группы

1. Щелкните **Устройства** и выберите устройства для добавления в группу.
2. Нажмите кнопку **Добавить в группу**.

   Программное обеспечение отобразит дерево групп, в которые можно добавить выбранное устройство.
3. Если требуется создать новую группу, выполните следующие действия. В противном случае пропустите этот шаг.
   a. Выберите группу, в которой необходимо создать группу.
   b. Нажмите кнопку **Новая группа**.

c. Укажите имя группы и затем нажмите кнопку **OK**.

4. Выберите группу, в которую необходимо добавить устройство, а затем нажмите кнопку **Выполнено**.

Другой способ добавить устройства в статическую группу – выбрать группу и щелкнуть **Добавить устройства**.

9.5 Создание динамической группы

1. Нажмите **Устройства** и выберите группу, которая содержит устройства, для которых необходимо создать динамическую группу.

   Примечание
   Невозможно создать динамические группы для группы «Все устройства».

2. Выполните поиск устройств с помощью поля поиска. Можно использовать составные условия поиска и операторы, описанные ниже.
3. Щелкните **Сохранить как** рядом с полем поиска.

   Примечание
   Определенные критерии поиска не поддерживаются для создания группы. См. таблицу в разделе "Условия поиска" ниже.

4. Укажите имя группы и затем нажмите кнопку **OK**.

9.5.1 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
comment	Комментарий для устройства. Значение по умолчанию:	comment = 'important machine' comment = '' (все машины без комментария)	Да

	• Для физических машин с ОС Windows описание компьютера считывается в свойствах компьютера в Windows. Это значение автоматически обновляется каждые 15 минут.
	• Пусто для других устройств.
	
	Чтобы просмотреть комментарий, в разделе **Устройства** выберите устройство и щелкните **Подробнее**, затем перейдите к разделу **Комментарий**.
	
	Чтобы добавить или изменить комментарий вручную, щелкните **Добавить** или **Изменить**. В этом случае автоматическое обновление перестанет работать. Чтобы снова разрешить автоматические обновления, очистите добавленный комментарий.
	
	Чтобы обновить поле комментария для устройств, перезапустите Managed Machine Service в разделе **Службы Windows** или в командной строке выполните следующую команду:
	
	`net stop mms`
	
	`net start mms`		

ip	IP-адрес (только для физических машин).	Диапазоны IP-адресов ('10.250.176.1','10.250.176.50')	Да

memorySize	Размер ОЗУ в мегабайтах (МиБ).	memorySize < 1024	Да
diskSize	Размер жесткого диска в гигабайтах или мегабайтах (только для физических машин).	diskSize < 300 ГБ diskSize >= 3000000 МБ	Нет
insideVm	Виртуальная машина с агентами в ней. Возможные значения: • true • false	insideVm = true	Да
osName	Название операционной системы.	osName LIKE '%Windows XP%'	Да
osType	Тип операционной системы. Возможные значения: • 'windows' • 'linux'	osType IN ('linux')	Да
osProductType	Тип продукта операционной системы. Возможные значения: • 'dc' Означает контроллер домена. **Примечание** После назначения роли контроллера домена на сервере Windows значение osProductType меняется с "server" на "dc". Такие машины не будут включены в результаты поиска для фильтра osProductType='server'. • 'server' • 'workstation'	osProductType = 'server'	Да
tenant	Название отдела,	tenant = 'Unit 1'	Да

	которому принадлежит устройство.		
tenantId	Идентификатор отдела, которому принадлежит устройство. Для получения идентификатора отдела напротив пункта **Устройства** выберите устройство и выберите пункт **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
protectedByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором. Для получения идентификатора плана нажмите **Планы** > **Резервное копирование**, выберите план, нажмите	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет

	на диаграмму в колонке **Статус** и затем нажмите на статус. Будет создан новый поиск с идентификатором плана.		
okByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **OK**.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
errorByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Ошибка**.	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
warningByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Предупреждение**.	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
runningByPlan	Устройства, защищенные посредством плана защиты с указанным идентификатором и со статусом **Выполняется**.	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Нет
interactionByPlan	Устройства, защищенные 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**	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	Да

	выберите устройство и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле Id.		
lastBackupTime*	Дата и время последнего успешного создания резервной копии. Формат данных следующий:'ГГГГ-ММ-ДД ЧЧ:ММ'.	lastBackupTime > '2020-03-11' lastBackupTime <= '2019-03-11 00:15' lastBackupTime is null	Нет
lastBackupTryTime*	Время последней попытки резервного копирования. Формат данных следующий:'ГГГГ-ММ-ДД ЧЧ:ММ'.	lastBackupTryTime >= '2020-03-11'	Нет
nextBackupTime*	Время следующего резервного копирования. Формат данных следующий:'ГГГГ-ММ-ДД ЧЧ:ММ'.	nextBackupTime >= '2021-03-11'	Нет
agentVersion	Версия установленного агента защиты.	agentVersion LIKE '12.0.*'	Да
hostId	Внутренний идентификатор агента защиты. Для получения идентификатора агента защиты напротив пункта **Устройства** выберите машину и щелкните **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'	resourceType = 'machine' resourceType in ('mssql_aag_database', 'mssql_database')	Да

	• 'virtual_machine.rhev' • 'virtual_machine.kvm' • 'virtual_machine.xen'		

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

9.5.2 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')
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: • * или % Астериск или знак процента могут заменять собой ни одного, один или несколько символов. • _ 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')
<	Оператор «Меньше чем».	memorySize < 1024

>	Оператор «Больше чем».	diskSize > 300 ГБ
<=	Оператор «Меньше чем или равно».	lastBackupTime <= '2019-03-11 00:15'
>=	Оператор «Больше чем или равно».	nextBackupTime >= '2021-03-11'
= или ==	Оператор «Равно».	osProductType = 'server'
!= или <>	Оператор «Не равно».	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'

9.6 Применение плана защиты к группе

1. Щелкните **Устройства**, а затем выберите встроенную группу, содержащую в себе группу, к которой необходимо применить план защиты.

   В программе будет выведен список дочерних групп.
2. Выберите группу, к которой необходимо применить план защиты.
3. Щелкните **Групповое резервное копирование**.

   В программе выводится список планов защиты, которые можно применить к группе.
4. Выполните одно из следующих действий:
   - Разверните существующий план защиты, а затем щелкните **Применить**.
   - Щелкните **Создать новый** и создайте новый план защиты, как описано в теме "План защиты".

10 Поддержка мультитенантности

Кибер Бэкап Облачный поддерживает мультитенантность. Это означает, что администратор/пользователь клиента может управлять объектами, которые связаны с его клиентом или субклиентами (отделы). Администратор/пользователь из отдела не может управлять объектами родительского клиента.

Например, администратор клиента создал план защиты и применил его к машине. Администратор клиента также может управлять планами защиты, созданными администратором отдела. Однако администратор отдела не может управлять планами защиты, созданными администратором клиента. Администратор отдела может создать собственный план защиты, который не будет конфликтовать с планом администратора клиента.

Кроме прочего, мультитенантность означает, что администратору/пользователю доступны для просмотра все объекты, которые связаны с этим клиентом или его субклиентами (отделами). Администратор/пользователь из отдела не может просматривать объекты родительского клиента.

Пример: данные, которые отображаются в оповещениях и действиях, доступны для просмотра только текущему клиенту и его субклиентам. Данные, относящиеся к родительскому клиенту, не отображаются.

11 План защиты и модули

План защиты – это план, объединяющий в себе несколько модулей защиты данных, включая указанные ниже.

- "Резервное копирование" (стр. 132): позволяет создавать резервную копию источников данных в локальном или облачном хранилище данных.
- "Active Protection (Активная защита)" (стр. 306): позволяет выполнять проверку компьютеров встроенным средством защиты от вредоносных программ.

Используйте "План защиты" (стр. 305) для защиты источников данных. Создавая гибкие планы для разных потребностей бизнеса, различные модули можно включить и отключить, задать их настройки.

11.1 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 несколькими способами (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 применен.

Порядок создания первого плана защиты в разделе «Устройства»

1. В консоли службы последовательно выберите пункты **Устройства** -> **Все устройства**.
2. Выберите машины, для которых нужно обеспечить защиту.
3. Щелкните **Защитить**, а затем щелкните **Создать план**.
   Откроются настройки плана защиты по умолчанию.
4. [Необязательно] Для изменения имени плана защиты щелкните значок карандаша рядом с именем.

   Примечание
   Для хранения имени плана может использоваться не более 128 байт. Тип используемых символов влияет на занимаемый ими объем: 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 щелкните переключатель рядом с именем модуля.
6. [Необязательно] Для настройки параметров модуля, щелкните соответствующий раздел плана

защиты.

7. После этого щелкните **Создать**.

"Резервное копирование" можно выполнить по требованию. Для этого щелкните **Запустить сейчас**.

11.2 Разрешение конфликтов плана

План защиты может иметь одно из указанных ниже состояний.

- **Активный**: план, который назначен устройствам и выполнен на них.
- **Неактивный**: план, который назначен устройствам, но отключен и не выполнен на них.

11.2.1 Применение нескольких планов к устройству

К одному устройству можно применить несколько планов защиты. В результате получится комбинация разных планов защиты, назначенных одному устройству. Планы защиты можно объединить, только если у них нет общих модулей. Если в примененных планах защиты есть одинаковые модули, необходимо разрешить конфликты между такими модулями.

11.2.2 Разрешение конфликтов плана

11.2.2.1 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.

- Создайте новый план, примените его и отключите все примененные конфликтующие планы.
- Создайте новый план и отключите его.

При редактировании нового плана на устройстве или устройствах с уже примененными планами, которые конфликтуют с внесенными изменениями, можно разрешить конфликт одним из указанных ниже способов.

- Сохраните изменения в план и отключите все уже примененные конфликтующие планы.
- Сохраните изменения, внесенные в план, и отключите его.

11.2.2.2 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.

11.2.2.3 Проблемы с лицензией

Назначенная квота на устройстве должна обеспечивать выполнение, обновление и применение плана защиты. Чтобы разрешить проблему с лицензией, выполните одно из указанных ниже действий:

- Отключите модули, которые не поддерживаются назначенной квотой, и продолжите использовать план защиты.
- Измените назначенную квоту вручную: откройте **Устройства** > **<конкретное_устройство>** > **Подробнее** > **Квота службы**, отзовите существующую квоту и назначьте новую.

11.3 Операции с планами защиты

11.3.0.1 Доступные действия с планами защиты

С планом защиты можно выполнить указанные ниже действия.

- Переименовать план.
- Включить/отключить модули и изменить настройки каждого модуля.
- Включить/отключить план.

  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 от устройства, для восстановления защиты администратору нужно только заново включить план.
- Применить план к устройству или группе устройств.
- Отозвать план с устройства.

  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 была обеспечена отозванным планом, администратор должен знать имя плана, выбрать его из списка доступных планов, а затем заново применить план к желаемому устройству.
- Импортировать/экспортировать план.

  Примечание

  Импортировать можно только те планы, которые созданы в Кибер Бэкап Облачный 9.0. Планы, созданные в предыдущих версиях продукта, несовместимы с версией 9.0.
- Удалить план.

Порядок применения существующего плана резервного копирования

1. Выберите машины, для которых нужно обеспечить защиту.
2. Щелкните **Защитить**. Если план защиты уже применен к выбранным машинам, щелкните **Добавить план**.
3. В программе отображаются ранее созданные планы защиты.
4. Выберите план защиты для применения и щелкните **Применить**.

Порядок изменения плана защиты

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. Щелкните **Защитить**.
3. Выберите план защиты, который необходимо изменить.
4. Щелкните значок многоточия рядом с именем плана резервного копирования и выберите команду **Изменить**.
5. Чтобы изменить параметры плана защиты, щелкните соответствующий раздел на его панели.
6. Щелкните **Сохранить изменения**.
7. Чтобы изменить план защиты для всех машин, к которым он применен, щелкните **Применить изменения к этому плану защиты**. Или щелкните **Создать новый план защиты только для выбранных устройств**.

Порядок отзыва плана защиты с машин

1. Выберите машины, для которых нужно отозвать план защиты.
2. Щелкните **Защитить**.
3. Если для машин применено несколько планов защиты, выберите тот из них, который необходимо отозвать.
4. Щелкните значок многоточия рядом с именем плана защиты и выберите команду **Отозвать**.

Порядок удаления плана защиты

1. Выберите любую машину, для которой применен план защиты, который необходимо удалить.
2. Щелкните **Защитить**.
3. Если для машины применено несколько планов защиты, выберите тот из них, который необходимо удалить.
4. Щелкните значок многоточия рядом с именем плана защиты и выберите команду **Удалить**.

   В результате план защиты будет отозван для всех машин и полностью удален из веб-интерфейса.

12 Резервное копирование и восстановление

С помощью модуля резервного копирования выполняется резервное копирование и восстановление физических и виртуальных машин, файлов и баз данных с использованием локального или облачного хранилища.

12.1 Резервное копирование

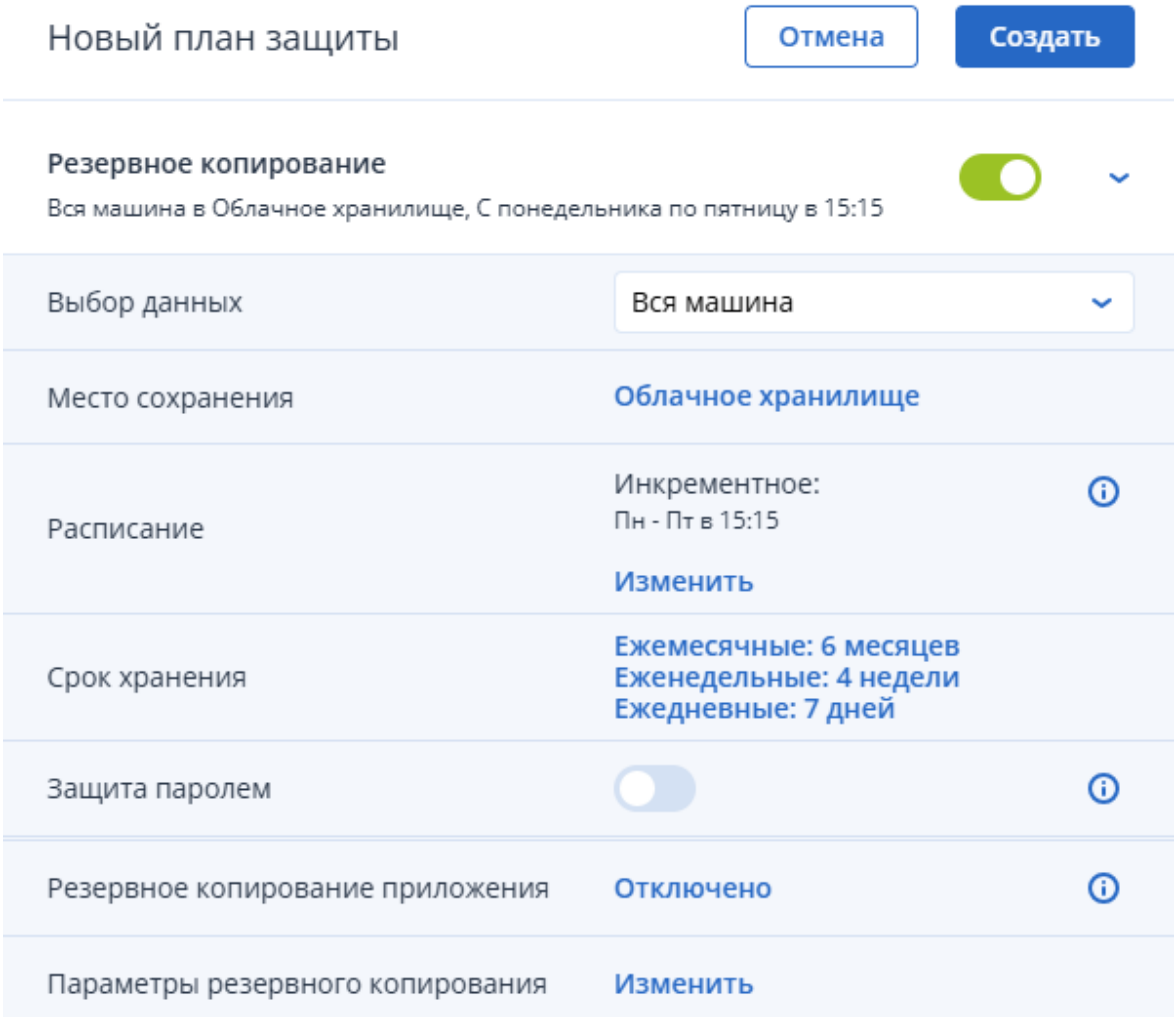
План защиты с включенным модулем "Резервное копирование" – это набор правил, определяющий способ защиты указанных данных на конкретной машине.

План защиты можно применить к нескольким машинам на этапе его создания или позже.

Порядок создания первого плана защиты с включенным модулем "Резервное копирование"

1. Выберите машины, резервные копии которых необходимо создать.
2. Щелкните **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, щелкните **Создать план**. Включите модуль **Резервное копирование** и откатите настройки.

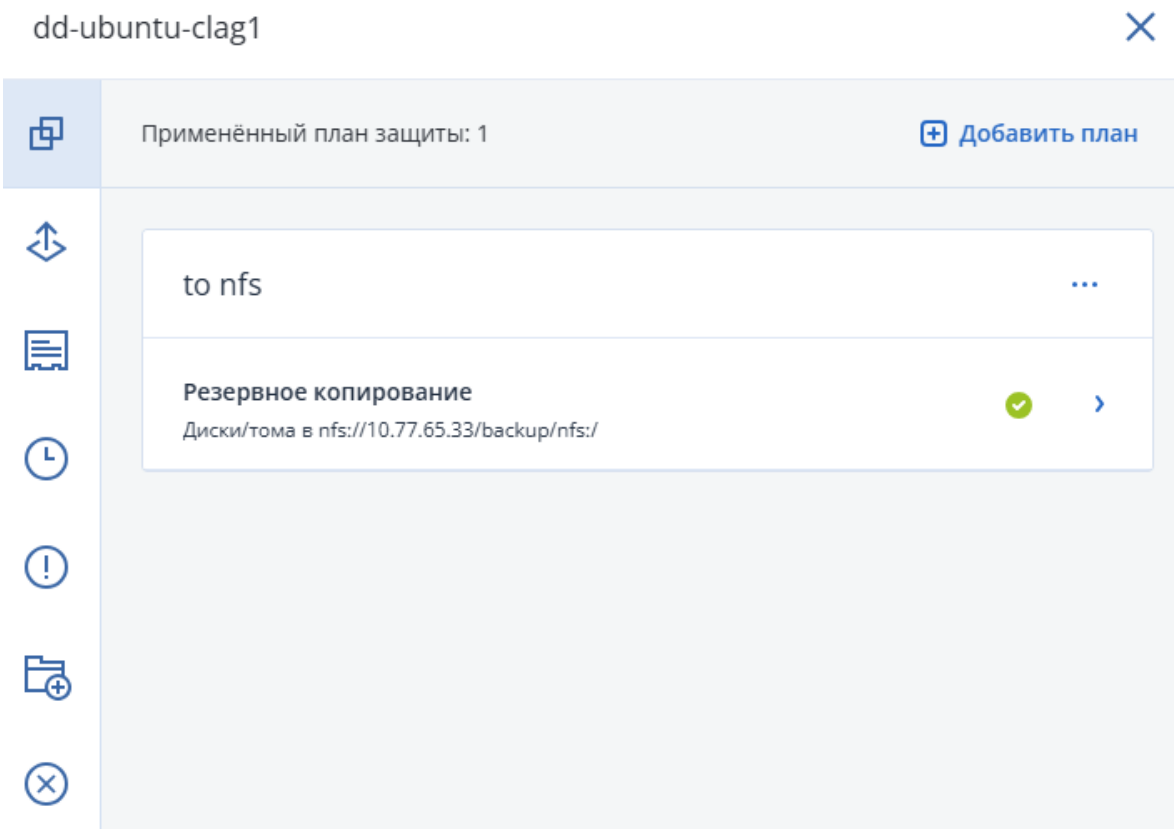


4. [Необязательно] Для изменения имени плана защиты щелкните имя по умолчанию.
5. [Необязательно] Чтобы изменить параметры модуля "Резервное копирование приложения", щелкните соответствующую настройку панели плана защиты.
6. [Необязательно] Чтобы изменить параметры резервного копирования, щелкните **Изменить** рядом с **Параметры резервного копирования**.
7. Нажмите кнопку **Создать**.

Порядок применения существующего плана резервного копирования

1. Выберите машины, резервные копии которых необходимо создать.
2. Щелкните **Защитить**. Если к выбранным машинам уже применен стандартный план защиты, щелкните **Добавить план**.

   В программе отображаются ранее созданные планы защиты.



3. Выберите план защиты для применения.
4. Нажмите кнопку **Применить**.

12.2 План защиты: памятка

В таблице ниже вкратце описаны доступные параметры плана защиты. 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) Резервное копирование выполняется с помощью агента, установленного в ОС	Непосредственный выбор Правила политики Фильтры файлов	Локальная папка Сетевая папка NFS* Зона безопасности	Всегда инкрементное (один файл) Всегда полное Еженедельно полное, ежедневно инкрементное Ежемесячно полное, еженедельно дифференциальное,	По возрасту резервной копии (одно правило на набор резервных копий) По количеству резервных копий

Диски/тома (виртуальные машины) Резервное копирование выполняется на уровне гипервизора сторонним агентом	Правила политики Фильтры файлов	Локальная папка Сетевая папка NFS*	ежедневно инкрементное (GFS) Настраиваемый вариант (П-Д-И)	По общему размеру резервных копий*** Хранить бессрочно
Файлы (только физические машины) Резервное копирование выполняется с помощью агента, установленного в ОС	Непосредственный выбор Правила политики Фильтры файлов	Облако Локальная папка Сетевая папка NFS* Зона безопасности	Всегда инкрементное (один файл)** Всегда полное Еженедельно полное, ежедневно инкрементное Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) Настраиваемый вариант (П-Д-И)	
Конфигурация ESXi	Непосредственный выбор	Локальная папка Сетевая папка NFS*		
Базы данных SQL	Непосредственный выбор	Облако Локальная папка Сетевая папка	Всегда полное Еженедельно полное, ежедневно инкрементное Настраиваемый вариант (П-И)	
Базы данных Exchange				

* Резервное копирование в общие папки NFS недоступно в Windows.

** Параметр "Всегда инкрементное (один файл)" доступен только в том случае, если основным местом назначения резервной копии является облако.

*** Правило хранения **По общему размеру резервных копий** недоступно в схеме резервного копирования **Всегда инкрементное (один файл)** или при резервном копировании в облачное хранилище данных.

12.3 Выбор данных для резервного копирования

12.3.1 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.

Для дисков, подключенных к физической машине по протоколу iSCSI, также можно создать резервную копию. В этом случае есть ограничения, если для резервного копирования дисков, подключенных по протоколу iSCSI, используется агент для VMware или агент для Hyper-V.

Есть два способа выбора дисков/томов: непосредственно на каждой машине или с помощью правил политики. Исключить файлы из резервной копии можно с помощью фильтров файлов.

12.3.1.1 Непосредственный выбор

Возможность непосредственного выбора доступна только для физических машин.

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 **Непосредственно**.
4. Для каждой из машин, которая включена в план защиты, установите флажки рядом с дисками и томами, которые требуется скопировать.
5. Нажмите кнопку **Готово**.

12.3.1.2 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.

Правила для Windows

- Буква диска (например, **C:**) обозначает том с указанной буквой.
- [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] позволяет выбрать систему и загрузочные тома. 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 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
```

12.3.1.3 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**, которое можно найти в разделе реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Это означает, что резервное копирование операционных систем, запускаемых из Windows Vista и Windows Restore Points, не производится.
  - Если параметр резервного копирования **Volume Shadow Copy Service (VSS)** включен, то файлы и папки указаны в ключе реестра **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot.**.

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.

12.3.2 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 файлов и папок на дисках, подключенных к физической машине по протоколу iSCSI, также можно создать резервную копию. В этом случае есть ограничения, если для резервного копирования данных на дисках, подключенных по протоколу iSCSI, используется агент для VMware или агент для Hyper-V.

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: непосредственно на каждой машине или с помощью правил политики. Для каждого из этих способов выбор можно уточнить с помощью фильтров файлов.

12.3.2.1 Непосредственный выбор

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.
2. Укажите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Непосредственно**.
4. Для каждой машины, включенной в план защиты, выполните указанные ниже действия.
   a. Щелкните **Выбрать файлы и папки**.
   b. Щелкните **Локальная папка** или **Сетевая папка**.
      Общая папка должна быть доступна с выбранной машины.
   c. 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.
   d. Выберите файлы и папки.
   e. Нажмите кнопку **Готово**.

12.3.2.2 Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.
2. Укажите **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 Profiles Folder] позволяет выбрать каталог **/home**. В этой папке по умолчанию размещены все профили пользователя.

12.3.3 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.
- Не удается выполнить резервное копирование конфигурации ESXi в облачное хранилище данных.

Порядок выбора конфигурации ESXi

1. Щелкните **Устройства** > **Все устройства**, после чего выберите хосты ESXi, для которых необходимо создать резервную копию.
2. Щелкните **Защитить**.
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.

12.4 Выбор места назначения

В разделе **Место сохранения** выберите один из перечисленных ниже вариантов.

- **Облачное хранилище данных**

  Резервные копии будут храниться в облачном центре обработки данных.
- **Локальные папки**

  Если выбрана одна машина, перейдите на ней в соответствующую папку или введите путь.

  Если выбрано несколько машин, 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.

  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 щелкните значок ключа рядом с именем папки.

  Резервное копирование в папку с анонимным доступом не поддерживается.
- **Папка NFS** (доступна для машин под управлением Linux)

Проверьте, что пакет nfs-utils установлен на сервере Linux с установленным агентом для 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.

Примечание
Невозможно выполнить резервное копирование в папку NFS, защищенную паролем.

- **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 "О разделе Зона безопасности" (стр. 142).

12.4.1 Расширенный выбор расположений хранения

Примечание
Эта функциональность доступна только в выпусках Advanced службы Кибер Бэкап Облачный.

Определяется сценарием (доступно для машин под управлением Windows)

Можно хранить резервную копию каждой машины в папке, определенной сценарием. Программное обеспечение поддерживает сценарии на языках JScript, VBScript или Python 3.5. При развертывании плана защиты программа выполняет сценарий на каждой машине. 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 **Хранилище 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

Пример. 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**.

12.4.2 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.

12.4.2.1 Почему нужно использовать раздел Зона безопасности?

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 назначения при использовании репликации резервных копий.

12.4.2.2 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[1]. При изменении места назначения на Зону безопасности в плане защиты, который имеет схему резервного копирования **Всегда инкрементное**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

12.4.2.3 Преобразование диска в результате создания раздела Зона безопасности

- Зона безопасности всегда создается в конце жесткого диска.

[1]Формат резервных копий, в котором первоначальная полная и последующие инкрементные резервные копии сохраняются в одном TIBX-файле. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка – сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В результате очистка выполняется очень быстро и с минимальным потреблением ресурсов. Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи.

- 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.

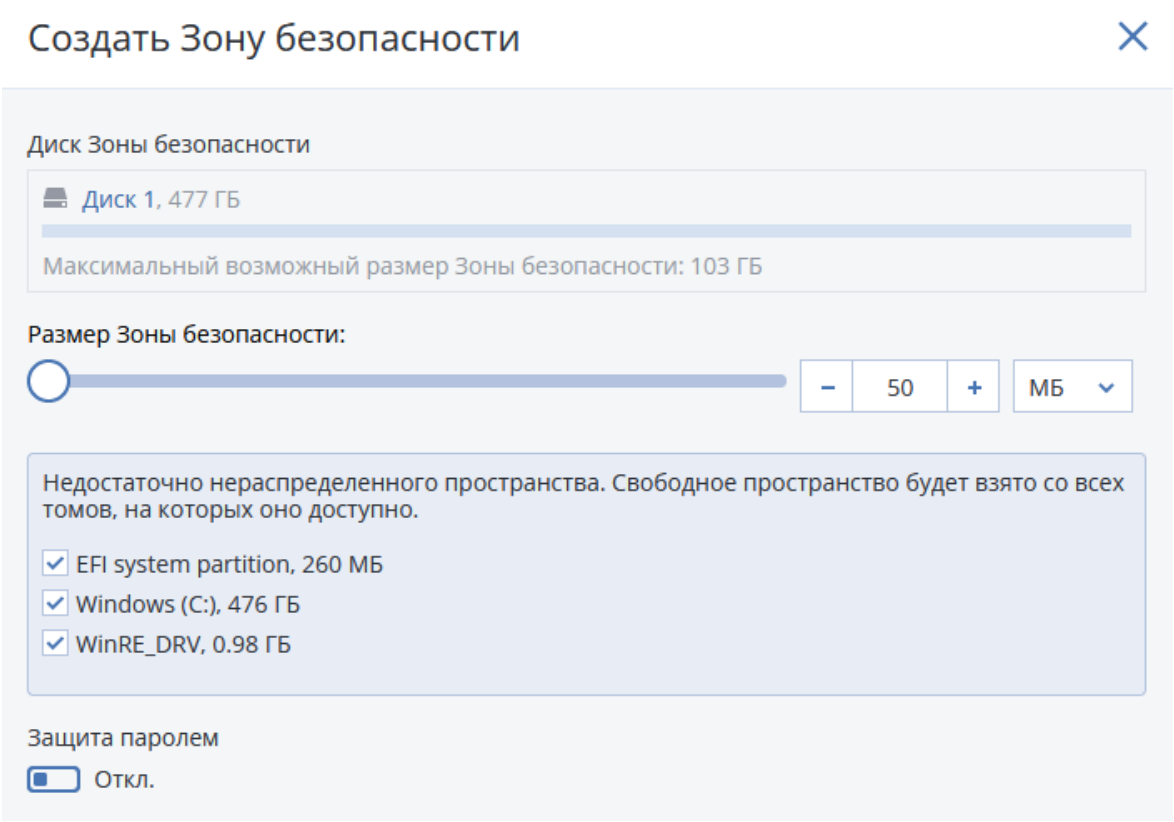
Внимание
Для перемещения или изменения размера тома, с которого загружена операционная система, потребуется перезагрузка.

12.4.2.4 Порядок создания Зоны безопасности

1. Выберите машину, на которой необходимо создать Зону безопасности.
2. Щелкните **Сведения** > **Создать Зону безопасности**.
3. В разделе **Диск Зоны безопасности** щелкните **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, щелкните **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 **OK**.
8. Подождите, пока программа создаст Зону безопасности.

После этого Зону безопасности можно выбрать в разделе **Место сохранения** при создании плана защиты.

12.4.2.5 Порядок удаления Зоны безопасности

1. Выберите машину с разделом Зона безопасности.
2. Нажмите **Сведения**.
3. Щелкните значок шестерни рядом с разделом **Зона безопасности**, затем щелкните **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. Щелкните **Удалить**.

В результате Зона безопасности будет удалена вместе со всеми содержащимися в ней резервными копиями.

12.5 Расписание

В расписании используются настройки времени (включая часовой пояс) операционной системы, в которой установлен агент. Часовой пояс агента для VMware (виртуальное устройство) можно настроить в интерфейсе агента.

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.

12.5.1 Схемы 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.

- **Всегда инкрементное (один файл)**

  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 формат резервной копии в виде одного файла[1].

  При первом резервном копировании происходит полная обработка всех данных, поэтому оно выполняется дольше последующих. Все последующие резервные копии являются инкрементными, благодаря чему процедура их выполнения занимает значительно меньше времени.

  Настоятельно рекомендуется использовать эту схему, если резервная копия расположена в облачном хранилище данных. При использовании других схем резервного копирования может создаваться несколько полных резервных копий, что приведет к существенным затратам времени и высокому объему сетевого трафика.

[1]Формат резервных копий, в котором первоначальная полная и последующие инкрементные резервные копии сохраняются в одном TIBX-файле. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка – сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В результате очистка выполняется очень быстро и с минимальным потреблением ресурсов. Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи.

Эта схема недоступна при выполнении резервного копирования 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** (щелкните значок шестеренки и выберите **Параметры резервного копирования** > **Еженедельное резервное копирование**).
- **Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS)**

  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.

  Данная схема резервного копирования отображается как схема **Пользовательская** на панели плана защиты.
- **Пользовательские**

  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».

12.5.2 Дополнительные параметры расписания

Для каждого места назначения 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.

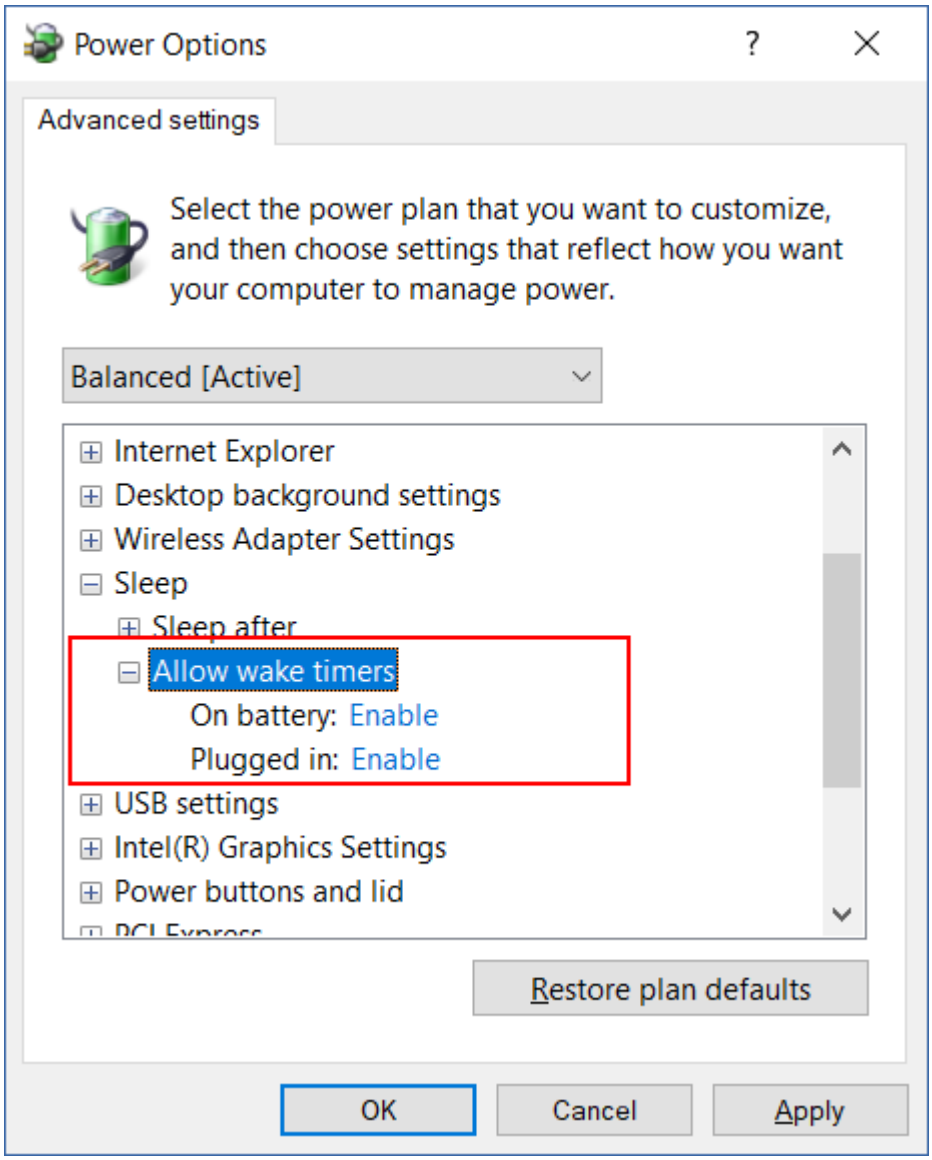
В настройках модуля "Резервное копирование" в плане защиты последовательно выберите пункты **Параметры резервного копирования** > **Планирование**. Установите флажок **Распределять время запуска резервного копирования по доступному времени**, затем укажите максимальную задержку. Продолжительность задержки 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.

Примечание
Этот параметр включен по умолчанию с максимальной задержкой 30 минут.

- Щелкните **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, для которых в настройках плана электропитания включен параметр **Разрешить таймеры пробуждения**.



Этот параметр не действует, когда машина выключена, т. е. данный параметр не использует функциональность Wake-on-LAN.

12.5.3 Планирование по событиям

При составлении расписания для модуля "Резервное копирование" в плане 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	Windows	-	-	-	-	Windows

Exchange						
Базы данных SQL	Windows	-	-	-	-	Windows

12.5.3.1 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 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 **service**, то оба источника событий (**Диспетчер служб** и **Служба времени**) приводят к вызову резервного копирования.

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**

Внимание
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**.

12.5.4 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 щелкните **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	Базы данных SQL

				Exchange	
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	-	-	-	-
Проверить IP-адрес устройства	Windows	-	-	-	-

12.5.4.1 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:

1. Если пользователь становится неактивным до 21:00, резервное копирование начинается в 21:00.

2. Если пользователь становится неактивным между 21:00 и 23:00, резервное копирование выполняется сразу после того, как пользователь стал неактивным.

3. Если пользователь все еще активен в 23:00, резервное копирование начинается в 23:00.

12.5.4.2 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, облачных хранилищ 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:

1. Если в 21:00 хост местоположения доступен, резервное копирование начнет выполняться вовремя.

2. Если в 21:00 хост с хранилищем недоступен, резервное копирование будет выполнено в следующий рабочий день, когда хост будет доступен.

3. Если хост с хранилищем вообще недоступен по рабочим дням в 21:00, задание вообще не будет выполняться.

12.5.4.3 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:

1. Если все пользователи выходят из системы к 20:00, резервное копирование начинает выполняться в 20:00.

2. Если последний пользователь выходит из системы между 20:00 и 23:00, резервное копирование начинает выполняться сразу после выхода пользователя из системы.

3. Если хотя бы один пользователь все еще активен в 23:00, резервное копирование начинается в 23:00.

12.5.4.4 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:

(1) Если пользователь выходит из системы между 16:30:00и 22:00:00, задание резервного копирования запускается сразу после выхода пользователя из системы.

(2) Если пользователь выходит из системы в любое другое время, резервное копирование пропускается.

12.5.4.5 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:

(1) Если в 21:00 устройство подключено к источнику питания, резервное копирование начнется немедленно.

(2) Если в 21:00 устройство работает от аккумуляторной батареи, резервное копирование начнется как только устройство будет подключено к источнику питания.

12.5.4.6 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 Майкрософт.

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, щелкнув 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:

(1) Если в 21:00 устройство не подключено к Интернету через лимитное подключение, резервное копирование начнется немедленно.

(2) Если в 21:00 устройство подключено к Интернету через лимитное подключение, резервное копирование начнется на следующий рабочий день.

(3) Если устройство всегда подключено к Интернету через лимитное подключение по рабочим дням 21:00, то резервное копирование вообще не запускается.

12.5.4.7 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, щелкнув 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:

(1) Если в 21:00 машина не подключена к указанной сети, резервное копирование начнется немедленно.

(2) Если в 21:00 машина подключена к указанной сети, резервное копирование начнется на следующий рабочий день.

(3) Если машина всегда подключено к указанным сетям по рабочим дням 21:00, то резервное копирование вообще не запускается.

12.5.4.8 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:

  (1) Если в 21:00 IP-адрес машины не будет находиться в указанном диапазоне, резервное копирование запустится немедленно.

  (2) Если в 21:00 IP-адрес машины будет находиться в указанном диапазоне, резервное копирование запустится, как только устройство получит IP-адрес вне диапазона IP-адресов VPN.

  (3) Если IP-адрес машины всегда находится в указанном диапазоне по рабочим дням в 21:00, резервное копирование вообще не будет выполняться.

12.6 Правила хранения

1. Нажмите **Срок хранения**.
2. В разделе **Очистка** выберите один из перечисленных ниже вариантов.
   - **По возрасту резервной копии** (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[1]. Чтобы использовать одно правило для всех резервных копий, щелкните **Перейти на использование одного правила для всех наборов резервных копий**.
   - **По количеству резервных копий**

     Укажите максимальное количество хранимых резервных копий.
   - **По общему размеру резервных копий**

     Укажите максимальный общий размер резервных копий.

     Эта настройка недоступна в схеме резервного копирования **Всегда инкрементное (один файл)** или при резервном копировании в облачное хранилище данных.
   - **Хранить резервные копии неопределенно долго**
3. Выберите время для запуска очистки.
   - **После резервного копирования** (по умолчанию)

     Правила хранения будут применены после создания новой резервной копии.

---

[1]Группа резервных копий, к которым можно применить отдельное правило хранения. Для настраиваемой схемы резервного копирования наборы резервных копий соответствуют методам резервного копирования (полный, дифференциальный и инкрементный). Во всех других случаях используются ежемесячный, ежедневный, еженедельный и почасовой наборы резервного копирования. Ежемесячная резервная копия – это первая копия, которая создается после начала месяца. Еженедельная резервная копия создается в день недели, который задан с помощью параметра Еженедельная резервная копия (щелкните значок шестеренки и последовательно выберите пункты Параметры резервного копирования > Еженедельная резервная копия). Если еженедельная копия является первой с начала месяца, она считается ежемесячной. В этом случае еженедельная резервная копия создается в назначенный день на следующей неделе. Ежедневная резервная копия – это первая копия, которая создается после начала дня, если только она не является ежемесячной или еженедельной. Почасовая резервная копия – это первая копия, которая создается после начала часа, если только она не является ежемесячной, еженедельной или ежедневной

- **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.

12.6.1 Что еще нужно знать

- 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 до резервного копирования.
- Если в соответствии со схемой резервного копирования и форматом резервного копирования каждая резервная копия хранится в отдельном файле, этот файл не может быть удален 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.
- Правила хранения – составная часть плана защиты. Они прекращают действовать для резервных копий машины, как только с нее отозван или удален план защиты или когда сама машина удалена из службы Кибер Бэкап Облачный. Если вам больше не нужны резервные копии, созданные данным планом, удалите их, как описано в разделе "Удаление резервных копий".

12.7 Защита паролем

Внимание
Если пароль утерян, восстановить защищённые резервные копии будет невозможно.

12.7.1 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 включите переключатель **Защита паролем**.
2. Укажите и подтвердите пароль.
3. Выберите один из следующих уровней защиты паролем:
   - **Низкий** – резервные копии будут защищены паролем с уровнем защиты **Низкий**.
   - **Средний** – резервные копии будут защищены паролем с уровнем защиты **Средний**.
   - **Высокий** – резервные копии будут защищены паролем с уровнем защиты **Высокий**.
4. Нажмите кнопку **OK**.

12.7.2 Защита паролем как свойство машины

Этот параметр предназначен для администраторов, которые работают с резервными копиями нескольких машин. Если необходим уникальный пароль защиты для каждой машины, или нужно защитить паролем отдельные резервные копии независимо от настроек плана защиты, сохраните настройки защиты паролем на каждой машине в отдельности. Резервные копии будут защищены с уровнем защиты **Высокий**.

Сохранение настроек защиты паролем на машине влияет на планы защиты следующим образом:

- **Планы защиты, которые уже применены к машине.** Если настройки защиты паролем в плане отличаются, резервное копирование завершится сбоем.
- **Планы защиты, которые будут применены к машине позже.** Настройки защиты паролем, сохраненные на машине, переопределят аналогичные настройки плана защиты. Паролем будут защищаться все резервные копии, даже если это отключено в плане защиты.

Это можно использовать на машине с запущенным агентом для VMware. Однако следует соблюдать осторожность, если к одному серверу vCenter Server подключено несколько агентов для VMware. Настройки защиты паролем должны быть одинаковы для всех агентов, поскольку между ними имеет место процесс распределения нагрузки.

После сохранения настроек защиты паролем их можно изменить или сбросить, как описано ниже.

Внимание
Если план защиты, который выполняется на этой машине, уже создал резервные копии, изменение настроек защиты паролем приведет к сбою этого плана. Чтобы продолжить резервное копирование, создайте новый план.

Сохранение настроек защиты паролем на машине

1. Войдите как администратор (в Windows) или пользователь root (в Linux).
2. Выполните следующий сценарий:
   - В Windows: <путь_установки>**\PyShell\bin\acropsh.exe -m manage_creds --set-password** <пароль_защиты>

     Здесь <путь_установки> – это путь к установленному агенту. По умолчанию используется путь **%ProgramFiles%\Acronis**.
   - В Linux: **/usr/sbin/acropsh -m manage_creds --set-password** <пароль_защиты>

Сброс настроек защиты паролем на машине

1. Войдите как администратор (в Windows) или пользователь root (в Linux).
2. Выполните следующий сценарий:
   - В Windows: <путь_установки>**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     Здесь <путь_установки> – это путь к установленному агенту. По умолчанию используется

путь **%ProgramFiles%\Acronis**.

- В Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Порядок изменения настроек защиты паролем с использованием программы Мониторинг Защиты Данных

1. Войдите в систему как администратор в Windows.
2. Щелкните значок **Мониторинг Защиты Данных** в области уведомлений Windows.
3. Выберите значок шестеренки.
4. Выберите пункт **Защита паролем**.
5. Выполните одно из следующих действий:
   - Установите **пароль для этой машины**. Укажите и подтвердите пароль защиты.
   - Выберите пункт **Использовать настройки защиты паролем, указанные в плане защиты**.
6. Нажмите кнопку **OK**.

12.7.3 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.

12.8 Запуск резервного копирования вручную

1. Выберите машину, для которой применен хотя бы один план защиты.
2. Щелкните **Защитить**.
3. Если применено несколько планов защиты, выберите один из них.
4. Выполните одно из следующих действий:
   - Щелкните **Запустить сейчас**. Будет создана инкрементная резервная копия.
   - Если схема резервного копирования содержит несколько методов резервного копирования, можно выбрать метод для использования. Щелкните стрелку на кнопке **Запустить сейчас**, а затем выберите **«Полная», «Инкрементная»** или **«Дифференциальная»**.

Первая резервная копия, созданная планом защиты, всегда является полной.

Прогресс выполнения резервного копирования отображается в столбце **Состояние** для выбранной машины.

12.9 Репликация

В данном разделе описана репликация резервных копий, которая включена в план защиты. Информацию о создании отдельного плана репликации для виртуальных машин VMware ESXi см. в

разделе "Репликация виртуальных машин" (стр. 271).

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.

12.9.1 Поддерживаемые расположения

Можно выполнить репликацию резервной копии из любого указанного ниже расположения:

- локальная папка,
- сетевая папка,
- папка NFS,
- Зона безопасности.

Можно выполнить репликацию резервной копии в любое указанное ниже расположение:

- облачное хранилище,
- локальная папка,
- сетевая папка,
- папка NFS,
- Зона безопасности.

Включение репликации резервных копий

1. На панели плана резервного копирования щелкните **Добавить хранилище**.
   Элемент управления **Добавить хранилище** отображается в случае, если поддерживается репликация из последнего выбранного хранилища.
2. Выберите хранилище для репликации резервных копий.
   Место сохранения отображается в плане защиты как **2-е**, **3-е**, **4-е** или **5-е хранилище**, в зависимости от количества хранилищ для репликации.
3. [Необязательно] В поле **Срок хранения** измените правила хранения для указанного хранилища, как описано в разделе "Правила хранения" (стр. 159).
4. [Необязательно] Щелкните значок шестерни и далее **Производительность и окно резервного копирования**. Задайте окно резервного копирования для выбранного расположения, как описано в разделе "Производительность и окно резервного копирования" (стр. 196). Эти настройки определят производительность репликации.
5. [Необязательно] Повторите шаги 1-4, чтобы добавить больше хранилищ для репликации резервных копий. Можно использовать до пяти хранилищ (включая основное).

12.10 Резервное копирование виртуальных машин без использования локальной сети (LAN-free backup)

В том случае, если по каким-то причинам вы не можете использовать локальную сеть для резервного копирования виртуальных машин или она становится узким местом в вашей системе, можно настроить резервное копирование без использования локальной сети.

12.10.1 Резервное копирование без использования локальной сети (LAN-free backup) для oVirt/zVirt

Резервное копирование без использования локальной сети в системах oVirt/zVirt поддерживается в следующих продуктах:

- Кибер Бэкап Облачный версии 25.07 и выше (агент резервного копирования версии 17.3 и выше);
- zVirt версии 4.4.

12.10.1.1 Схема резервного копирования без использования локальной сети

На этой схеме:

- **ВМ1**, **ВМ2** и **ВМ3** – целевые виртуальные машины для выполнения резервного копирования в системе виртуализации oVirt/zVirt;

- **Виртуальное устройство** – виртуальное устройство для взаимодействия с Кибер Бэкап Облачный и oVirt/zVirt;
- **Node1**, **Node2**, **Node3** – вычислительные узлы (хосты) системы виртуализации oVirt/zVirt;
- **------** – отображает подключение сети управления;
- **<------- >** – отображает направление трафика;
- **NFS-хранилище**, **iSCSI-хранилище**, **FC-хранилище** – устройства 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 NFS, iSCSI или из локального хранилища).

12.10.1.2 Поддерживаемые типы хранилищ для использования в качестве доменов хранения

Каждый центр данных должен иметь как минимум один домен хранения данных. Также центр данных может иметь не более одного домена хранения **Экспорт**. Домены типа **Экспорт** и **ISO** устарели, но при необходимости их можно создать.

Домен хранения может состоять из блочных устройств (iSCSI или Fibre Channel), из файловой системы (POSIX) и NFS, Gluster.

1. **NFS**. zVirt поддерживает NFS версий 3 и 4.
2. **iSCSI**. Необходим для производственных рабочих нагрузок. Рекомендуется использовать 10GBe и разделение локальной сети. Поддерживает многоканальность (multipathing) для повышения высокой доступности.

   Примечание
   zVirt поддерживает 1500 логических томов на блочный домен хранения. Разрешается использовать не более 300 LUN.

3. **Fibre Channel (FC)**. Fibre Channel является одновременно быстрым и безопасным, и его следует использовать, если он уже используется в целевом центре данных. Его преимущество заключается в низкой нагрузке на процессор по сравнению с iSCSI и NFS. Fibre Channel также может использовать многоканальность (multipathing) для повышения высокой доступности.
4. **Fibre Channel over Ethernet (FCoE)**. Чтобы использовать Fibre Channel over Ethernet, необходимо включить ключ fcoe в менеджере управления и установить пакет vdsm-hook-fcoe на хосты.
5. **Gluster Storage (GS)**. Gluster Storage – это POSIX-совместимая файловая система с открытым исходным кодом. Три или более серверов конфигурируются как кластер Gluster Storage, вместо сетевых устройств хранения данных (NAS) или массива сети хранения данных (SAN).

   Примечание
   Gluster Storage следует использовать по 10GbE и разделять с помощью виртуальных локальных сетей.

6. **POSIX**. Совместные файловые системы. Другие POSIX-совместимые файловые системы могут использоваться в качестве доменов хранения в zVirt, если они являются кластерными файловыми системами, такими как Global File System 2 (GFS2), и поддерживают разреженные файлы и прямой ввод-вывод. Файловая система Common Internet File System (CIFS), например, не поддерживает прямой ввод-вывод, что делает ее несовместимой с zVirt.

12.10.1.3 Подключение хранилищ

Вы можете подключить хранилища следующих типов: NFS, iSCSI, FC, Local (локальное).

Перед подключением ознакомьтесь с рекомендациями по проектированию хранилищ.

Схема подключения блочного хранилища (Block Storage)

Блочное хранилище может представлять собой сеть хранения SAN (Storage Area Network), которая предоставляет блочные устройства.

- **Хранилище**: iSCSI/FC/FCoE-хранилище;
- **Сервер oVirt Engine**: управляет подключением к хранилищу;
- **Хосты oVirt Node (Hypervisor)**: подключаются к блочному хранилищу через iSCSI или FC;
- **Сеть**: Для iSCSI используется отдельная сеть (желательно) для обеспечения высокой производительности и отказоустойчивости.

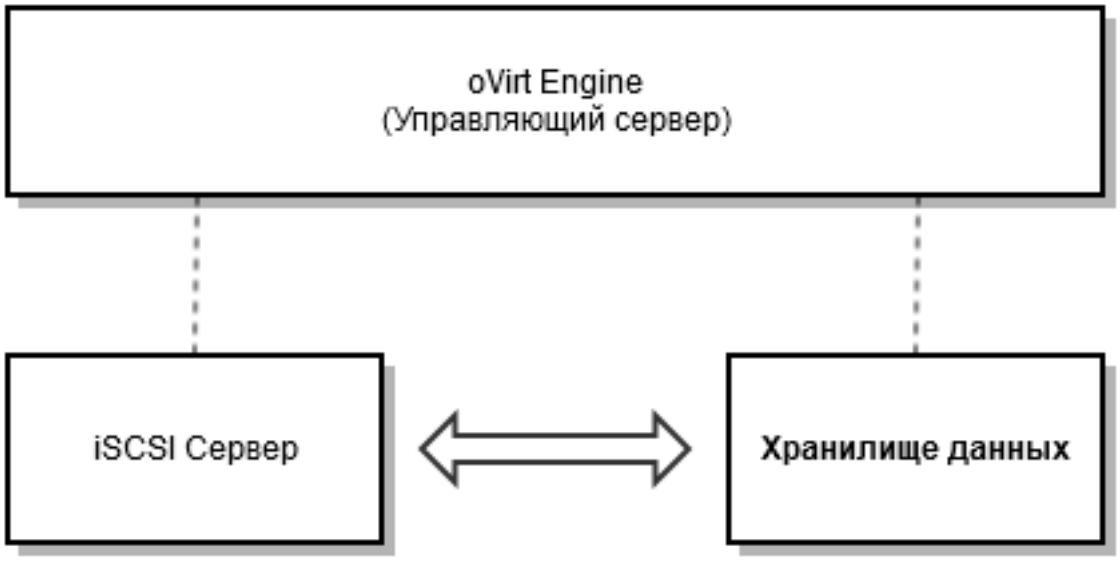
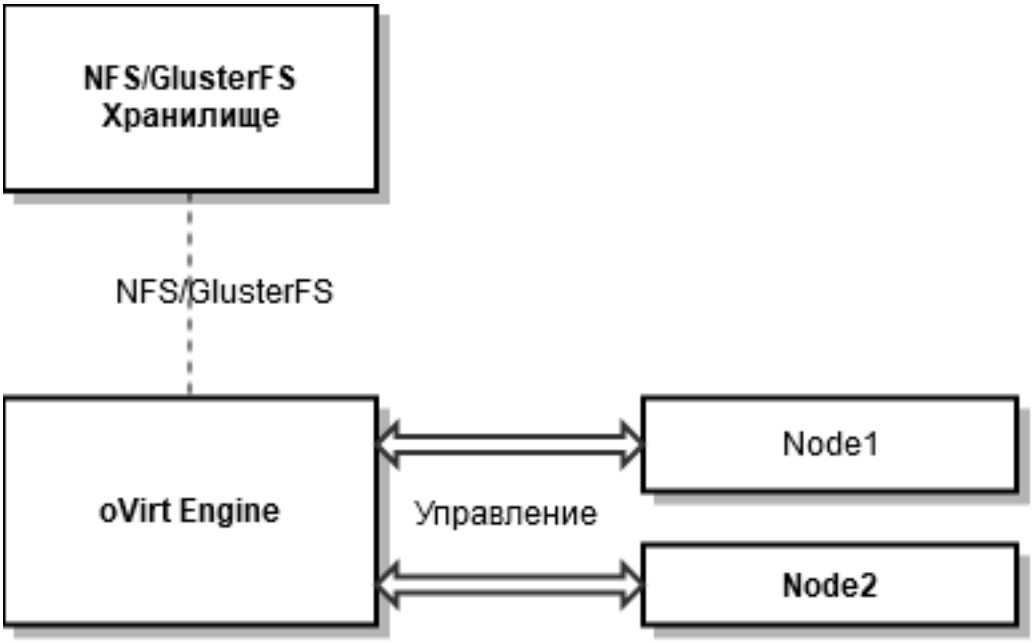


Схема подключения сетевого хранилища (Network Storage)

Сетевые хранилища предоставляют доступ к данным через сетевые протоколы, такие как NFS или GlusterFS.

- **Хранилище**: NFS-сервер или GlusterFS-кластер.
- **Сервер oVirt Engine**: управляет подключением к хранилищу.

- **Хосты oVirt Node (Hypervisor)**: подключаются к сетевому хранилищу через NFS или GlusterFS.
- **Сеть**: для NFS/GlusterFS используется отдельная сеть для обеспечения высокой производительности.



Локальное хранилище (Local Storage)

- **Хранилище**: локальные диски на хостах oVirt Node.
- **Сервер oVirt Engine**: управляет локальными хранилищами.
- **Domain**: локальный домен (локальный центр данных) и кластер, в который не могут быть добавлены другие хосты.
- **Хосты oVirt Node (Hypervisor)**: используют локальные диски для хранения данных.

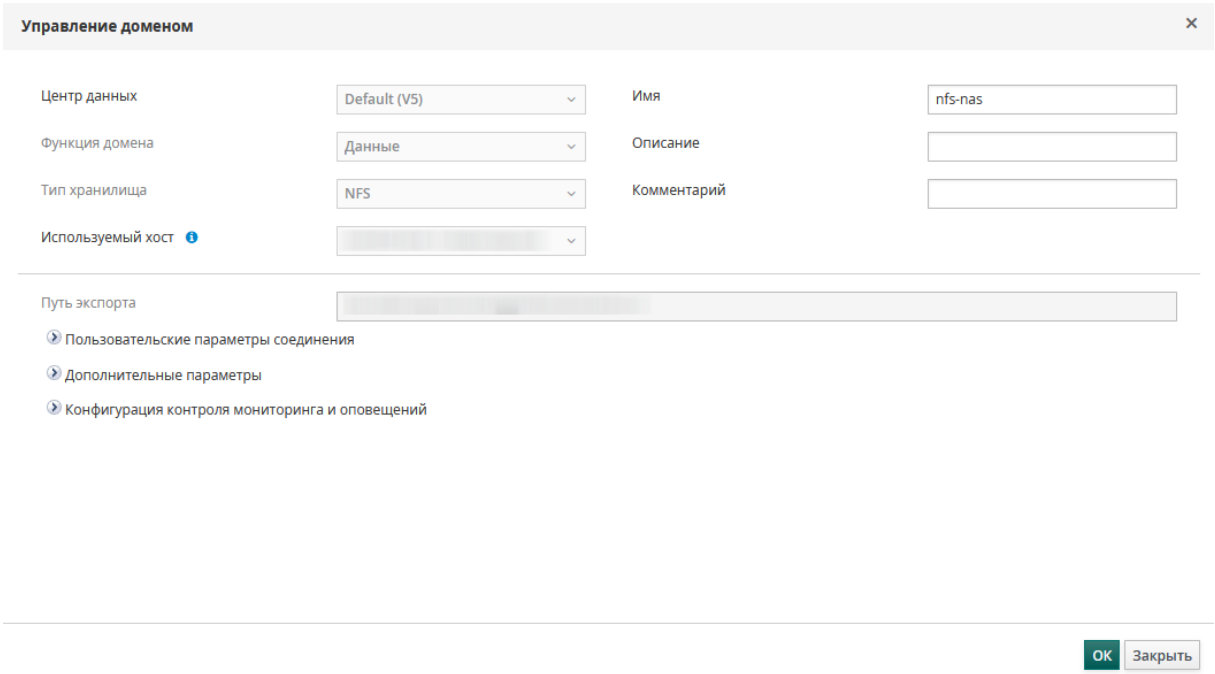
Внимание
Несмотря на то, что zVirt поддерживает локальное хранилище, не используйте его в продуктовой среде. Используйте локальное хранилище только для HostedEngine. Не используйте это хранилище для хранения образов или дисков ВМ.

Подключение NFS-хранилища

Подключение NFS-хранилища может потребоваться на этапе начальной установки zVirt в качестве основного хранилища или на этапе подключения дополнительного хранилища в уже работающий zVirt.

В первом случае на этапе установки zVirt необходимо будет указать установщику путь до NFS-хранилища: <IP_или_Доменное_Имя>:/export/data.

Во втором случае на портале администратора в разделе **Хранилище** -> **Домены** необходимо произвести подключение нового домена. В диалоговом окне потребуется указать **Тип**, **Путь** и **Имя**:



Создание NFS (на примере ОС Debian)

1. Выполните установку NFS-службы:

```
sudo apt install nfs-kernel-server
sudo systemctl enable --now nfs-blkmap
```

2. Добавьте группы **sanlock**, **kvm** и пользователей **sanlock** и **vdsm** с помощью следующих команд:

```
sudo groupadd sanlock -g 179
sudo groupadd kvm -g 36
sudo useradd sanlock -u 179 -g 179 -G kvm
sudo useradd vdsm -u 36 -g 36 -G sanlock
```

3. Создайте папку и назначьте ей необходимые права:

```
sudo mkdir /export/data
sudo chown 36:36 /export/data
sudo chmod 0775 /export/data
```

4. Настройка NFS-хранилища:

```
echo "/export/data *(rw,anonuid=36,anongid=36)" | sudo tee /etc/exports
```

   В этой записи:

   - rw – означает доступ read/write;
   - anonuid=36,anongid=36 – необходимые параметры для успешного управлениями файлами NFS-хранилища со стороны служб zVirt.

Подключение iSCSI-хранилища

zVirt поддерживает хранилища, доступные по протоколу iSCSI. Хранилища после добавления в среду виртуализации как домены хранения будут использоваться в качестве Volume Group (VG), состоящие из одного или более LUN (PV).

Volume Group (VG) и LUN (PV) не могут одновременно использоваться несколькими доменами хранения.

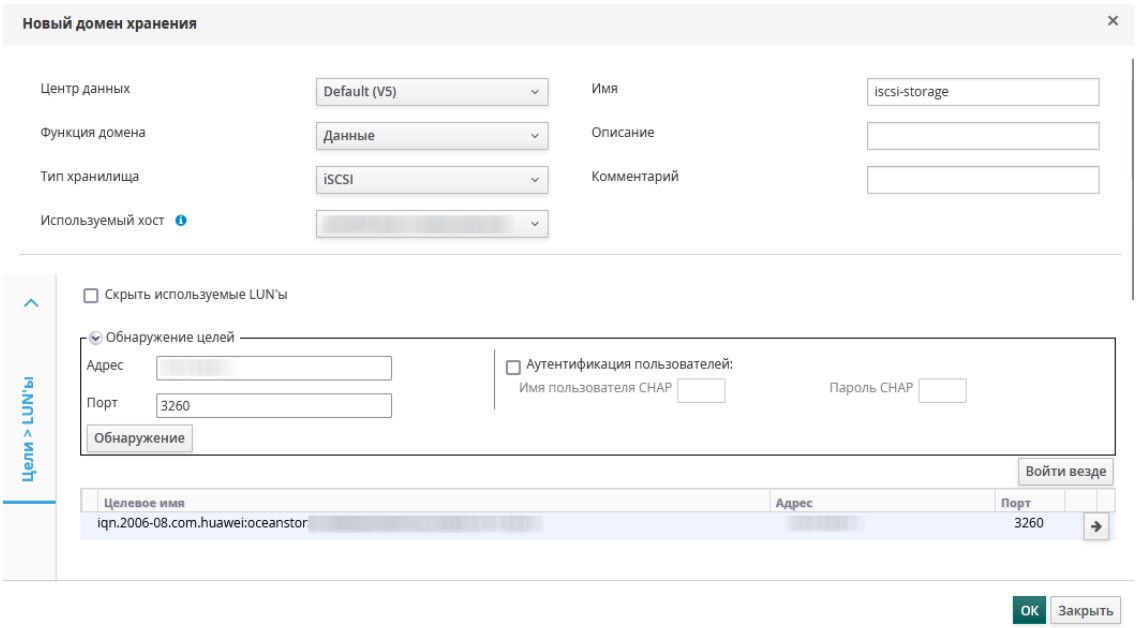
Для подключения iSCSI-хранилища выполните следующие действия:

1. Нажмите **Хранилище** (**Storage**) -> **Домены** (**Domains**).
2. Нажмите **Новый домен** (**New Domain**).
3. Задайте **Имя** (**Name**) для нового домена хранения.
4. Выберите **Центр данных** (**Data Center**) в раскрывающемся списке.
5. Выберите **Данные** (**Data**) в качестве **Функция домена** (**Domain Function**) и **iSCSI** в качестве **Типа хранилища** (**Storage Type**).
6. Выберите **Активный хост** в качестве **Используемый хост** (**Host**).

> **Внимание**
> У всех хостов должен быть доступ к устройству хранения, прежде чем домен хранения можно будет настроить.

7. Менеджер управления может сопоставлять iSCSI-таргеты с LUN или LUN с iSCSI-таргетами. Если выбран тип хранилища iSCSI, то в окне **Новый домен хранения (New Domain**) будут автоматически отображаться известные таргеты с неиспользуемыми LUN. Если таргет, который вы используете для добавления хранилища, не отображается, то для его поиска можно использовать операцию обнаружения таргетов; в противном случае перейдите к следующему шагу.
   a. Нажмите **Обнаружение целей** (**Discover Targets**), чтобы задать параметры обнаружения таргетов. После того как таргеты обнаружены и вход в них выполнен, в окне **Новый домен хранения** (**New Domain**) будут автоматически отображаться таргеты с LUN, которые не используются средой. Параметры **Обнаружение целей** (**Discover Targets**) можно использовать для добавления LUN на несколько таргетов или нескольких путей к одному LUN.
   b. В поле **Адрес** (**Address**) укажите FQDN или IP-адрес iSCSI-хоста.
   c. В поле **Порт** (**Port**) укажите порт для соединения с хостом в процессе поиска таргетов. Значение по умолчанию: 3260.
   d. Если для защиты хранилища используется CHAP, установите флажок **Аутентификация пользователей** (**User Authentication**). Введите **Имя пользователя CHAP** (**CHAP user name**) и **Пароль CHAP** (**CHAP password**).

e. Нажмите **Обнаружение** (**Discover**).

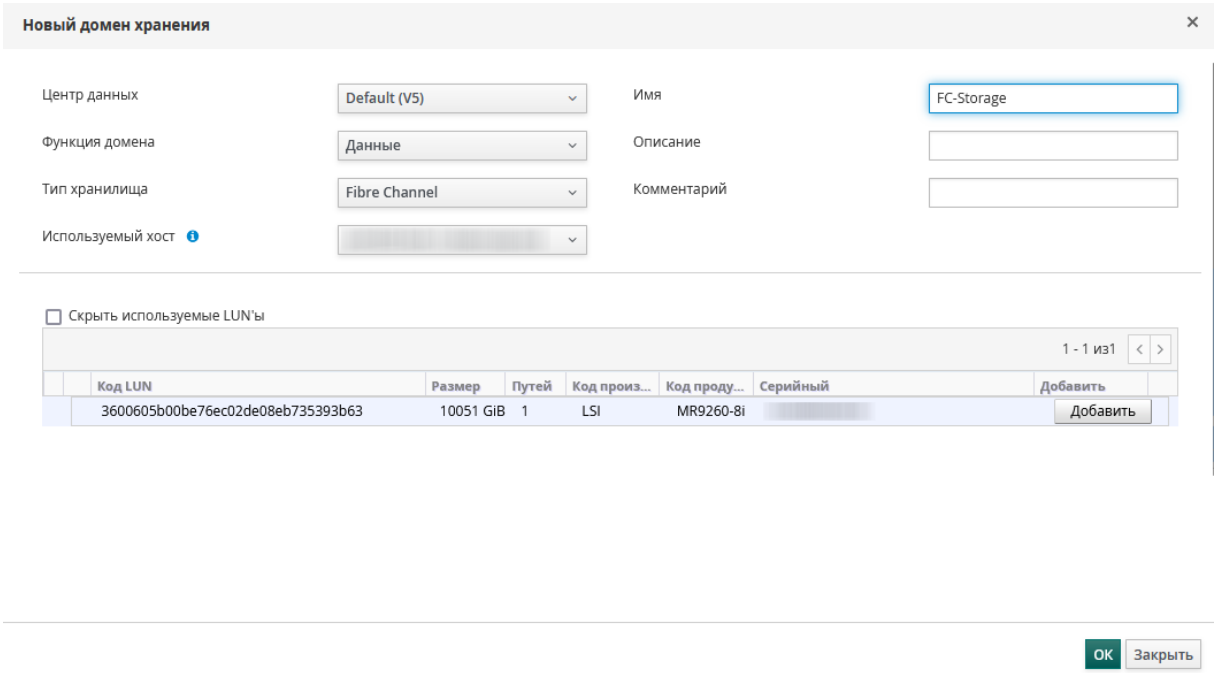


Подключение FC-хранилища

Для подключения FC-хранилища выполните следующие действия:

1. Нажмите **Хранилище** (**Storage**) -> **Домены** (**Domains**).
2. Нажмите **Новый домен** (**New Domain**).
3. Задайте **Имя** (**Name**) для домена хранения.
4. Выберите из раскрывающегося списка **Центр данных** (**Data Center**) FCP.

   Если подходящего центра данных FCP пока нет, выберите **нет** (**none**).
5. Из выпадающих списков выберите **Функцию домена** (**Domain Function**) и **Тип хранилища** (**Storage Type**). Типы доменов хранения, несовместимые с выбранным центром данных, недоступны.
6. Выберите **активный хост** в поле **Используемый хост** (**Host**). Если это не первый домен данных в центре данных, нужно выбрать хост SPM в центре данных.
7. Если выбран тип хранилища **Fibre Channel**, то в окне **Новый домен хранения** (**New Domain**) будут автоматически отображаться известные таргеты с неиспользуемыми LUN. Поставьте флажок Код LUN (LUN ID), чтобы выбрать все доступные LUN.



Подключение локального хранилища

Для подключения локального хранилища выполните следующие действия:

1. Создайте каталог локального хранилища:

   ```
   mkdir /data
   lvcreate -n <lv_name> -L <size> <vg_name>
   mkfs.ext4 /dev/mapper/<vg_name>-<lv_name>
   echo "/dev/mapper/<vg_name>-<lv_name> /data ext4 defaults,discard 1 2" >> /etc/fstab
   mount /data
   ```

   В этой записи:

   <vg_name> – имя нужной группы томов;

   <lv_name> – имя создаваемого логического тома;

   <size> – размер создаваемого тома.

2. Смонтируйте новое локальное хранилище:

   ```
   mount -a
   ```

3. Убедитесь, что каталог имеет разрешение на чтение/запись для пользователя **vdsm** (UID 36) и группы **kvm** (GID 36):

   ```
   chown 36:36 /data
   chmod 0775 /data
   ```

4. Нажмите **Ресурсы** (**Compute**) -> **Хосты** (**Hosts**) и выберите хост.

5. Нажмите **Управление** (**Management**) -> **Обслуживание** (**Maintenance**) и **OK**. Статус хоста меняется на **Обслуживание** (**Maintenance**) host maintenance.

6. Нажмите **Управление** (**Management**) -> **Настроить локальное хранилище** (**Configure Local Storage**).
7. Нажмите кнопки **Изменить** (**Edit**) рядом с полями **Центр данных** (**Data Center**) -> **Кластер** (**Cluster**) и **Хранилище** (**Storage**), чтобы настроить локальный домен хранения и дать ему имя.
8. Введите путь к локальному хранилищу в текстовое поле.
9. Если применимо, откройте вкладку **Оптимизация** (**Optimization**), чтобы настроить политику оптимизации памяти для нового кластера локального хранилища.
10. Нажмите **OK**.

При добавлении к хосту локального домена хранения и при задании пути к локальному каталогу хранения хост автоматически создается и помещается в локальный центр данных, локальный кластер и локальный домен хранения.

Для проверки выполните следующие действия:

1. Нажмите **Хранилище** (**Storage**) -> **Домены** (**Domains**).
2. Найдите локальный домен хранения, который только что добавили.

Домен должен иметь статус **Активный** (**Active**), а значение в столбце **Тип хранилища** (**Storage Type**) должно быть **Локальное на хосте** (**Local on Host**). Теперь можно выгрузить образ диска в новый локальный домен хранения.

Подробнее о подключении хранилищ см. в руководстве по установке zVirt и в руководстве администратора zVirt.

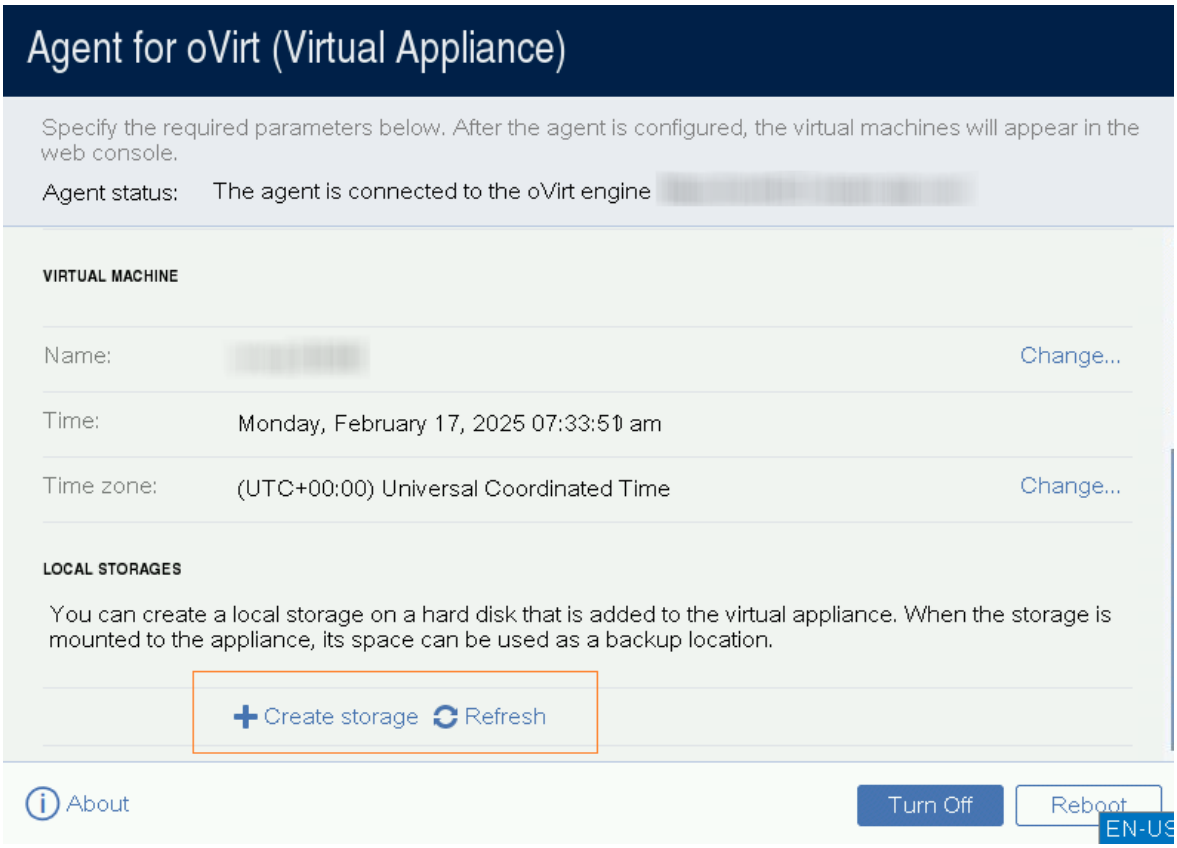
12.10.1.4 Включение прямого доступа к хранилищу для виртуального устройства

Настройка и подключение диска к виртуальному устройству

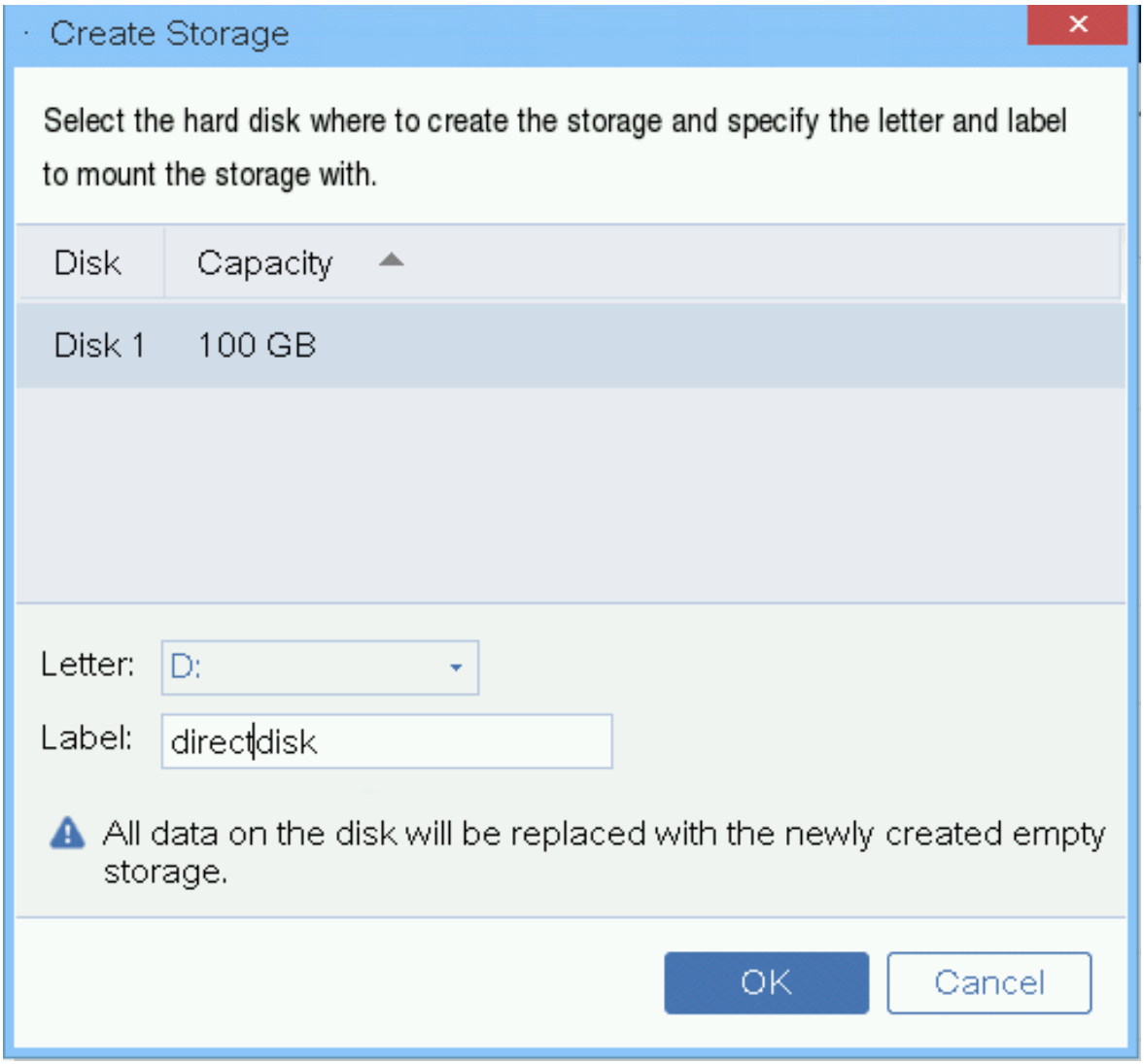
1. Установите виртуальное устройство (virtual appliance) для системы виртуализации oVirt/zVirt.
2. Убедитесь, что виртуальное устройство успешно подключено к системе виртуализации.
3. Добавьте новый диск к виртуальному устройству с помощью графического интерфейса oVirt/zVirt. Этот диск может быть представлен как диск iSCSI, FC или локальное устройство. Размер диска должен составлять не менее 10 ГБ.

   Внимание
   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.

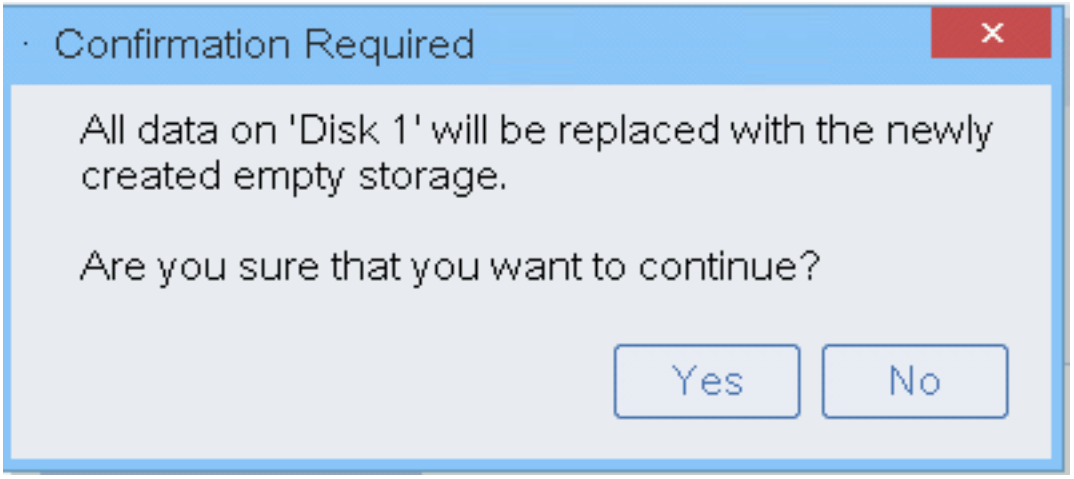
4. Перейдите в консоль виртуального устройства.
5. В веб-интерфейсе виртуального устройства в меню **Local Storages** нажмите на ссылку **Refresh**.



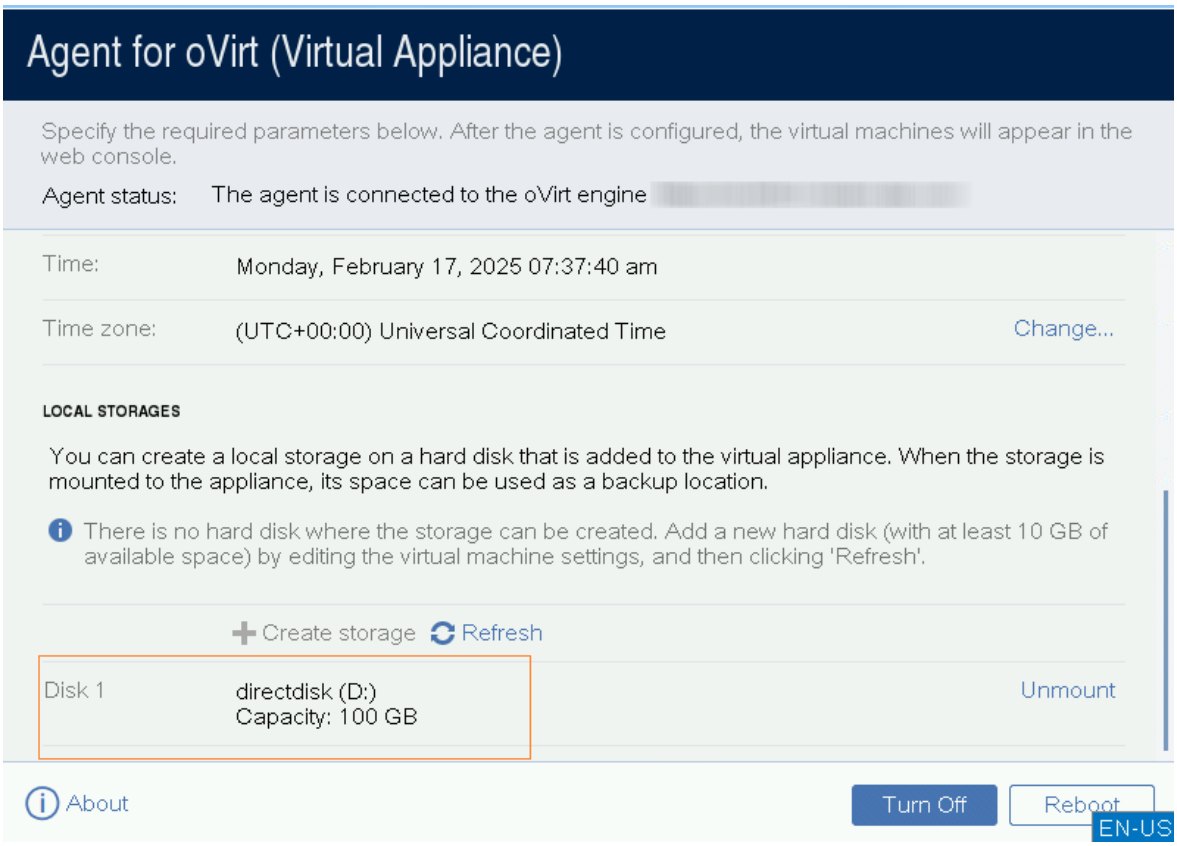
6. Ссылка **Create Storage** станет активной, нажмите на эту ссылку. Выберите диск и укажите для него метку. Длина метки ограничена 16 символами в связи с ограничениями файловой системы.



7. Подтвердите добавление диска.



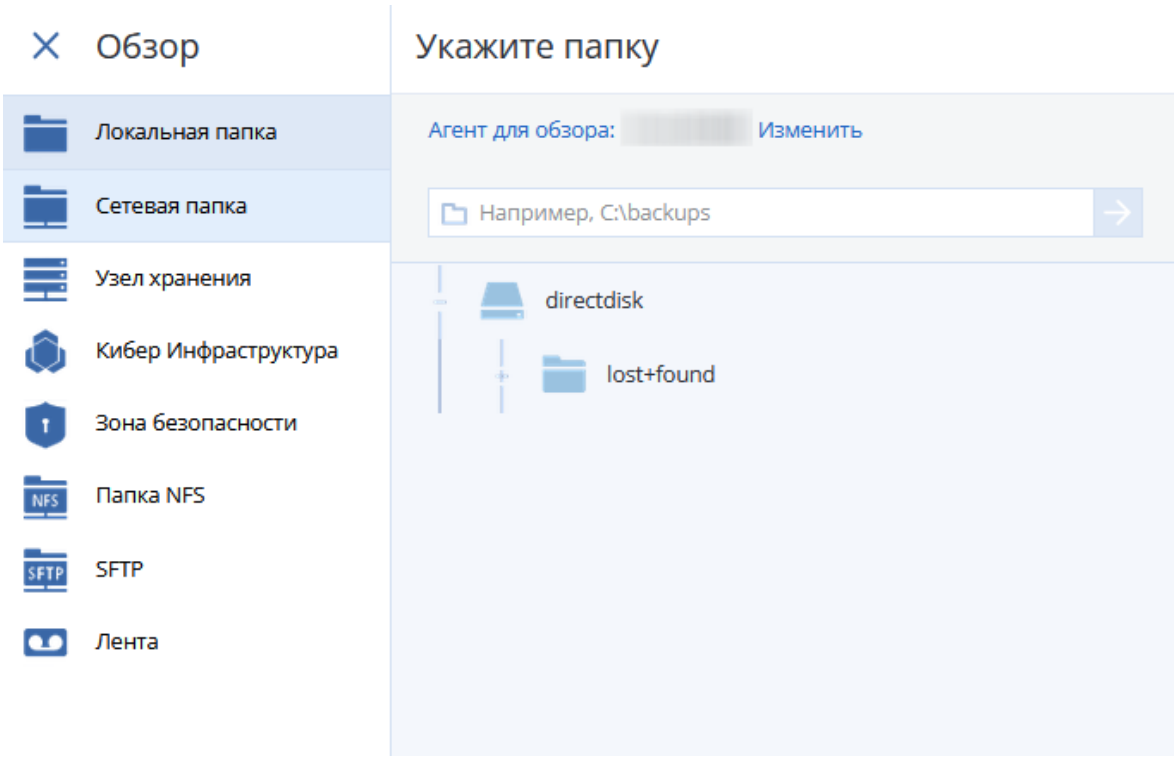
8. В интерфейсе виртуального устройства убедитесь, что диск был успешно добавлен к виртуальному устройству.



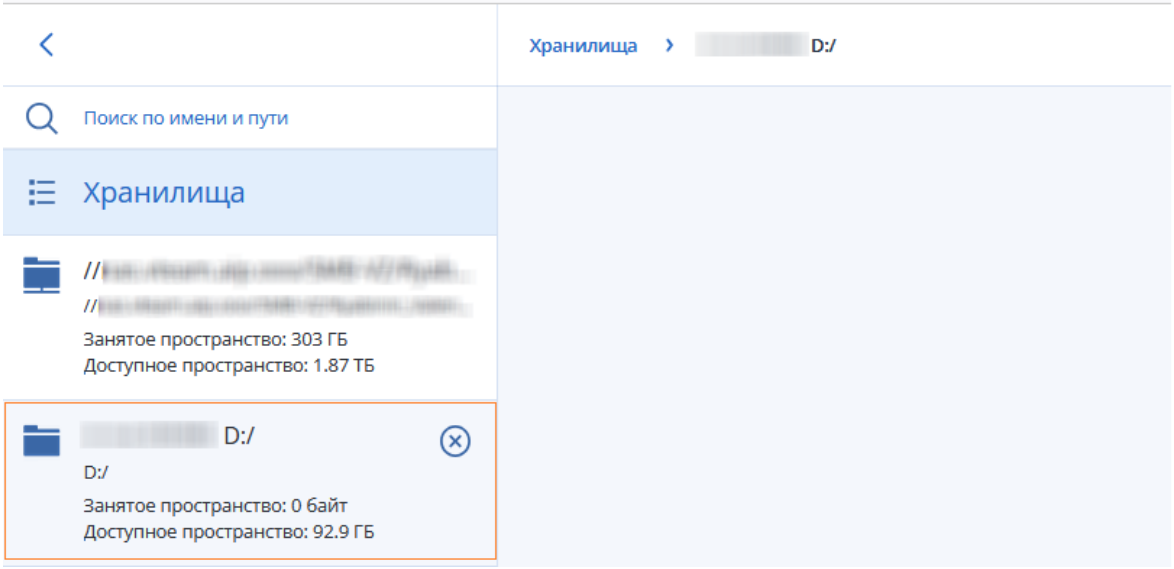
Подключение локального диска виртуального устройства в Кибер Бэкап Облачный

Для подключения выполните следующие действия:

1. Убедитесь, что виртуальное устройство (virtual appliance) установлено и подключено к oVirt/Zvirt.
2. В веб-консоли перейдите в меню **Хранилища резервных копий** и на вкладке **Действия** выберите ссылку **Добавить хранилище**.
3. На вкладке **Обзор** рядом с **Агент для обзора** щелкните **Изменить**, выберите нужное виртуальное устройство и нажмите **OK**. Далее выберите **Локальная папка** (**Local**) и после отображения дерева подключенных дисков выберите необходимый диск на виртуальном устройстве.



4. После успешного добавления в **Хранилище резервных копий** отобразится новое хранилище для резервных копий.



12.11 Параметры резервного копирования по умолчанию

Значения по умолчанию параметров резервного копирования существуют только на уровнях компании, отдела и пользователя. При создании отдела или учетной записи пользователя в компании или отделе создаваемая сущность наследует значения по умолчанию, заданные для компании или отдела.

Администраторы компаний, администраторы отделов и любые пользователи без прав администратора могут заменить значение параметра по умолчанию на другое предварительно заданное значение. Новое значение будет использоваться по умолчанию для всех планов защиты, которые будут созданы на соответствующем уровне, после внесения изменения.

При создании плана защиты пользователь может переопределить значение по умолчанию своим значением, которое будет действовать только для данного плана.

Для изменения используемых по умолчанию параметров

1. Выполните одно из следующих действий:
   - Чтобы изменить значение по умолчанию для компании, войдите в консоль службы с учетными данными администратора компании.
   - Чтобы изменить значение по умолчанию для отдела, войдите в консоль службы с учетными данными администратора отдела.
   - Чтобы изменить значение по умолчанию для своей учетной записи, войдите в консоль службы с учетными данными без прав администратора.
2. Нажмите **Настройки** > **Настройки системы**.
3. Увеличьте область раздела **Параметры резервного копирования по умолчанию**.
4. Выберите параметр и внесите необходимые изменения.
5. Нажмите кнопку **Сохранить**.

12.12 Параметры резервного копирования

Чтобы изменить параметры резервного копирования, в модуле "Резервное копирование" плана защиты щелкните **Изменить** рядом с **Параметры резервного копирования**.

12.12.1 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 (облачное хранилище данных, локальная или сетевая папка).

В следующей таблице представлены обобщенные сведения по доступности параметров резервного копирования.

	Резервное копирование на уровне дисков		Резервное копирование на уровне файлов		Виртуальные машины		SQL и Exchange
	Windows	Linux	Windows	Linux	ESXi	Hyper-	Windows

						V	
Оповещения	+	+	+	+	+	+	+
Имя файла резервной копии	+	+	+	+	+	+	+
Формат резервной копии	+	+	+	+	+	+	+
Проверка резервных копий	+	+	+	+	+	+	+
Функция Changed Block Tracking (CBT)	+	-	-	-	+	+	-
Способ резервного копирования кластера	-	-	-	-	-	-	+
Уровень сжатия	+	+	+	+	+	+	+
Обработка ошибок							
В случае ошибки повторить попытку	+	+	+	+	+	+	+
Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений)	+	+	+	+	+	+	+
Пропуск поврежденных секторов	+	+	+	+	+	+	-
Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины	-	-	-	-	+	+	-
Быстрое инкрементное/дифференциальное резервное копирование	+	+	-	-	-	-	-
Моментальные снимки резервных копий на уровне файлов	-	-	+	+	-	-	-
Фильтры файлов	+	+	+	+	+	+	-
Сокращение журнала	-	-	-	-	+	+	Только SQL
Создание моментальных снимков LVM	-	+	-	-	-	-	-
Точки подключения	-	-	+	-	-	-	-

Многотомные моментальные снимки	+	+	+	+	-	-	-
Производительность и окно резервного копирования	+	+	+	+	+	+	+
Физическая доставка данных	+	+	+	+	+	+	-
Команды до и после процедуры	+	+	+	+	+	+	+
Команды до и после захвата данных	+	+	+	+	-	-	+
Планирование							
Распределять время запуска по доступному времени	+	+	+	+	+	+	+
Ограничить число одновременно выполняющихся операций резервного копирования	-	-	-	-	+	+	-
Посекторное резервное копирование	+	+	-	-	+	+	-
Разбиение*	+	+	+	+	+	+	+
Действия при сбое задания	+	+	+	+	+	+	+
Условия запуска задания	+	+	+	+	+	+	+
Служба теневого копирования томов (VSS)	+	-	+	-	-	+	+
Служба теневого копирования томов (VSS) для виртуальных машин	-	-	-	-	+	+	-
Еженедельное резервное копирование	+	+	+	+	+	+	+
Журнал событий Windows	+	-	+	-	+	+	+

* Разбиение невозможно при резервном копировании в облачное хранилище данных.

12.12.2 Оповещения

12.12.2.1 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.

12.12.3 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.

12.12.3.1 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 резервных копий. В следующей таблице перечислены файлы, которые могут быть созданы на каждой машине или почтовом ящике.

	Всегда инкрементное (один файл)	**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
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). Если размер файла, сохраненного в локальной или сетевой (SMB) папке превышает 200 ГБ, он по умолчанию разбивается на файлы по 200 ГБ.	

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 только в формате резервного копирования "Версия 11".

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, облачного хранилища данных). Это целесообразно в том случае, если требуется просмотр пользовательских имен на вкладке **Хранилище резервных копий**.

12.12.3.2 Где можно просмотреть имена файлов резервных копий?

Выберите вкладку **Хранилище 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 **Хранилище резервных копий** в столбце **Имя**.

12.12.3.3 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**).

12.12.3.4 Имя файла резервной копии по умолчанию

По умолчанию для имени файла резервной копии всей физической или виртуальной машины, дисков/томов, файлов/папок, баз данных Microsoft SQL Server и Microsoft Exchange, а также конфигурации ESXi используется следующий формат: [ИмяМашины]-[ИД плана]-[Уникальный ИД]A.

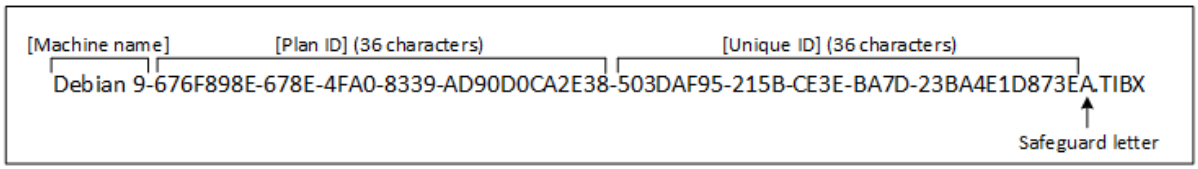
Для облачных резервных копий приложения, созданных облачными агентами, по умолчанию задается имя [Имя ресурса]_[Тип ресурса]_[Идентификатор ресурса]_[Идентификатор плана]A.

Имя по умолчанию состоит из следующих переменных:

- [Имя машины] Эта переменная заменяется именем машины (такое же имя отображается в консоли службы).
- [ИД плана], [Идентификатор плана] Эти переменные заменяются уникальным идентификатором плана защиты. При переименовании плана это значение не изменяется.
- [Уникальный ИД] Эта переменная заменяется уникальным идентификатором выбранной машины. При переименовании машины это значение не изменяется.
- [ИД почтового ящика] Эта переменная заменяется именем участника-пользователя (UPN) почтового ящика.
- [Имя ресурса] Эта переменная заменяется именем облачного источника данных. Это может быть имя участника-пользователя (UPN) или имя общей папки.

- [Тип ресурса] Эта переменная заменяется типом облачного источника данных, например mailbox.
- [ИД ресурса] Эта переменная заменяется уникальным идентификатором облачного источника данных. Это значение не меняется при переименовании облачного источника данных.
- Защитная буква «A» добавляется для того, чтобы имя файла не заканчивалось цифрой.

На приведенной ниже диаграмме показано имя по умолчанию файла резервной копии.



12.12.3.5 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 (один файл)**:

```
MyBackup.tibx
```

Для формата "Версии 12" с другими схемами резервного копирования:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

12.12.3.6 Использование переменных

Кроме переменных, используемых по умолчанию, можно использовать следующие переменные:

- Переменная [Имя плана], которая заменяется именем плана защиты.
- Переменная [Тип сервера виртуализации], вместо которой используется «vmwesx» (если резервная копия виртуальных машин создана агентом для VMware) или «mshyperv» (если резервная копия виртуальных машин создана агентом для Hyper-V).

Если выбрано резервное копирование нескольких машин или почтовых ящиков, имя файла резервной копии должно содержать переменную [Имя машины], [Уникальный ИД], [ИД почтового ящика], [Имя ресурса] или [Идентификатор ресурса].

12.12.3.7 Примеры использования

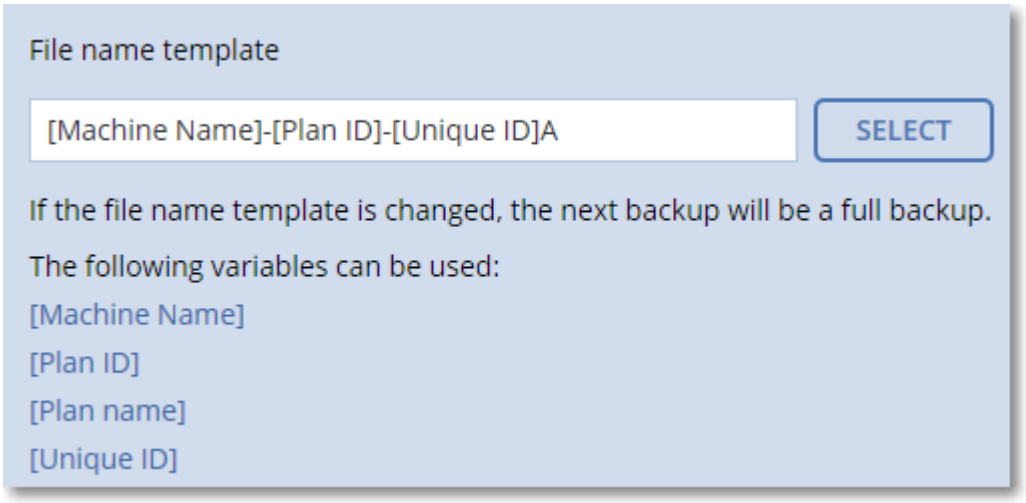
- **Просмотр дружественных к пользователю имен файлов**

  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 консоли службы 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, щелкните **Выбрать** и выберите требуемую резервную копию.

  Кнопка **Выбрать** выводит резервные копии в хранилище, выбранном в разделе **Место сохранения резервной копии** на панели плана защиты. Обзор невозможно выполнить за пределами этого хранилища.



Примечание

Кнопка **Выбрать** доступна только для планов защиты, которые созданы и применены для одного устройства.

12.12.4 Формат резервной копии

Параметр **Формат резервной копии** определяет формат резервных копий, созданных планом защиты. Этот параметр доступен только для тех планов защиты, для которых уже используется формат "Версия 11". В этом случае формат резервного копирования можно изменить на "Версия 12". После перехода к использованию формата резервной копии "Версия 12" этот параметр станет недоступным.

- **Версия 11**

  Устаревший формат, который используется для обеспечения обратной совместимости.

Примечание
Невозможно создать резервную копию групп обеспечения доступности баз данных (DAG), используя формат архива "Версия 11". Резервное копирование группы обеспечения доступности баз данных поддерживается только в формате "Версия 12".

- **Версия 12**
  Формат резервной копии, который впервые начал использоваться в Кибер Бэкап 12 для быстрого резервного копирования и восстановления. Каждая цепочка резервных копий (полного или дифференциального копирования, и всех зависящих от них инкрементных резервных копий) сохраняется в один файл TIBX.

12.12.4.1 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. В следующей таблице перечислены файлы, которые могут быть созданы на каждой машине или почтовом ящике.

	Всегда инкрементное (один файл)	**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
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). Если размер файла, сохраненного в локальной или сетевой (SMB) папке превышает 200 ГБ, он по умолчанию разбивается на файлы по 200 ГБ.	

12.12.4.2 Изменение формата резервной копии на "Версия 12" (TIBX)

При изменении формата резервной копии с версии 11 (формат .tib) на версию 12 (формат .tibx) имеет место 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 **Хранилище резервных копий**. Их можно удалить вручную.
- Старые облачные резервные копии не будут занимать пространство в пределах квоты **Облачное хранилище данных**.

- Старые локальные резервные копии будут занимать пространство в пределах квоты **Локальная резервная копия** до тех пор, пока вы не удалите их вручную.

12.12.4.3 Дедупликация в архиве

Формат резервной копии версии 12 (TIBX) 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 TIBX. Не нужно включать ее в параметрах резервного копирования. Отключить ее также невозможно.

12.12.5 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. Единственное исключение – проверка резервных копий на уровне файлов, которые расположены в облачном хранилище данных. Эти резервные копии проверяются путем проверки согласованности метаданных, сохраненных 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.

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.

Примечание
В зависимости от настроек, выбранных поставщиком услуги, проверка может быть недоступна при резервном копировании в облачное хранилище данных.

12.12.6 Функция Changed Block Tracking (CBT)

Этот параметр применим для резервных копий на уровне дисков для виртуальных и физических машин, работающих под управлением Windows. Он также применим к резервным копиям баз данных Microsoft SQL Server и Microsoft Exchange Server.

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.

12.12.7 Способ резервного копирования кластера

Примечание
Эта функциональность доступна только в выпусках Advanced службы Кибер Бэкап Облачный.

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 и кластера баз данных PostgreSQL на базе 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.

12.12.7.1 Microsoft SQL Server

Этот параметр определяет режим резервного копирования для группы доступности SQL Server Always On (AAG). Чтобы этот параметр действовал, агент для SQL должен быть установлен на всех узлах AAG.

Значение по умолчанию: **Дополнительная реплика, если возможно.**

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.

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.

12.12.7.2 Microsoft Exchange Server

Этот параметр определяет режим резервного копирования для группы обеспечения доступности баз данных Exchange Server (DAG). Чтобы этот 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)».

Значение по умолчанию: **Пассивная копия, если возможно**

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.

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.

12.12.7.3 Настройка параметра для кластера баз данных PostgreSQL на базе Patroni

Значение по умолчанию: **Реплика, если возможно**.

Можно выбрать один из следующих вариантов:

- **Реплика, если возможно**
  Создается резервная копия баз данных с подчиненных узлов. Если все подчиненные узлы выключены, создается резервная копия с главного узла. Резервное копирование главного узла может замедлить работу PostgreSQL, но в резервной копии будут самые актуальные данные.
- **Реплика**
  Создается резервная копия баз данных только с подчиненных узлов.
- **Лидер**
  Создается резервная копия баз данных только с главного узла. Резервное копирование главного узла может замедлить работу PostgreSQL, но в резервной копии будут самые актуальные данные.

12.12.8 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.

12.12.9 Обработка ошибок

Эти параметры позволяют указать, как должны обрабатываться ошибки, возникшие во время резервного копирования.

12.12.9.1 В случае ошибки повторить попытку

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).

Например, если место назначения резервной копии в сети станет недоступным при выполнении резервного копирования, 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.

Однако если место назначения резервной копии недоступно при запуске резервного копирования, будет предпринято только 10 попыток.

Облачное хранилище данных

Если облачное хранилище данных выбрано в качестве назначения резервной копии, для параметра автоматически устанавливается значение **Включено**. **Количество попыток: 300**. **Интервал между попытками: 30 секунд.**

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.

12.12.9.2 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.

12.12.9.3 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.

12.12.9.4 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).

12.12.10 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.

12.12.11 Фильтры файлов

Фильтры файлов указывают, какие файлы и папки нужно пропускать во время резервного копирования.

Фильтры файлов доступны как для резервных копий на уровне дисков, резервных копий всей машины и резервных копий на уровне файлов, если не указано иначе.

Включение фильтров файлов

1. Выберите данные для резервного копирования.
2. Щелкните **Изменить** рядом с разделом **Параметры резервного копирования**.
3. Выберите **Фильтры файлов**.
4. Воспользуйтесь любыми из перечисленных ниже вариантов.

12.12.11.1 Исключить файлы, соответствующие 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.

  Примечание
  Этот фильтр не работает для резервной копии на уровне файлов, если в поле Формат резервной копии выбрано **Версия 11**, и при этом местом назначения резервной копии не является облачное хранилище данных.

- **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**).
- **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**

12.12.11.2 Исключить скрытые файлы и папки

Установите этот флажок, чтобы пропускать файлы и папки, которые имеют атрибут **Скрытый** (для файловых систем, которые поддерживаются в Windows) или начинаются с точки (.) (для файловых систем Linux, таких как Ext2 и Ext3). Если папка скрыта, то все ее содержимое, включая нескрытые файлы, будет исключено.

12.12.11.3 Исключить системные файлы и папки

Этот параметр действует только в файловых системах, совместимых с Windows. Установите этот флажок, чтобы пропустить все файлы и папки с атрибутом **Системный**. Если папка имеет атрибут **Системный**, все ее содержимое (включая файлы, не имеющие атрибута **Системный**) будет исключено.

Примечание
Просматривать атрибуты файла или папки можно в свойствах файла или папки или с помощью команды attrib. Дополнительные сведения можно получить в центре справки и поддержки Windows.

12.12.12 Моментальные снимки резервных копий на уровне файлов

Этот параметр действует только 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.**

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.

12.12.13 Сокращение журнала

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 тот момент времени, когда этим программным обеспечением была создана резервная копия. Журналы транзакций резервного копирования создаются встроенным модулем архивации Microsoft SQL Server. Можно будет применить журналы транзакций после восстановления и таким образом восстановить базу данных в состояние на любой момент времени.

12.12.14 Создание моментальных снимков LVM

Этот параметр действует только для физических машин.

Этот параметр действует только для резервного копирования на уровне дисков томов, управляемых диспетчера 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.

12.12.15 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.

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.

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**.

12.12.16 Многотомные моментальные снимки

Этот параметр применим для резервных копий физических машин, работающих под управлением Windows или Linux.

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**.
- 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.

12.12.17 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 недоступен для процессов резервного копирования, выполняемых облачными агентами, например, для резервного копирования сайтов или серверов, расположенных на сайте облачного восстановления.

Этот параметр можно настроить отдельно для каждого хранилища, указанного в плане защиты. Чтобы настроить этот параметр для хранилища репликации, щелкните значок шестерни рядом с именем хранилища и щелкните **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 (например, проверка), 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** (в Windows, соответствует **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.

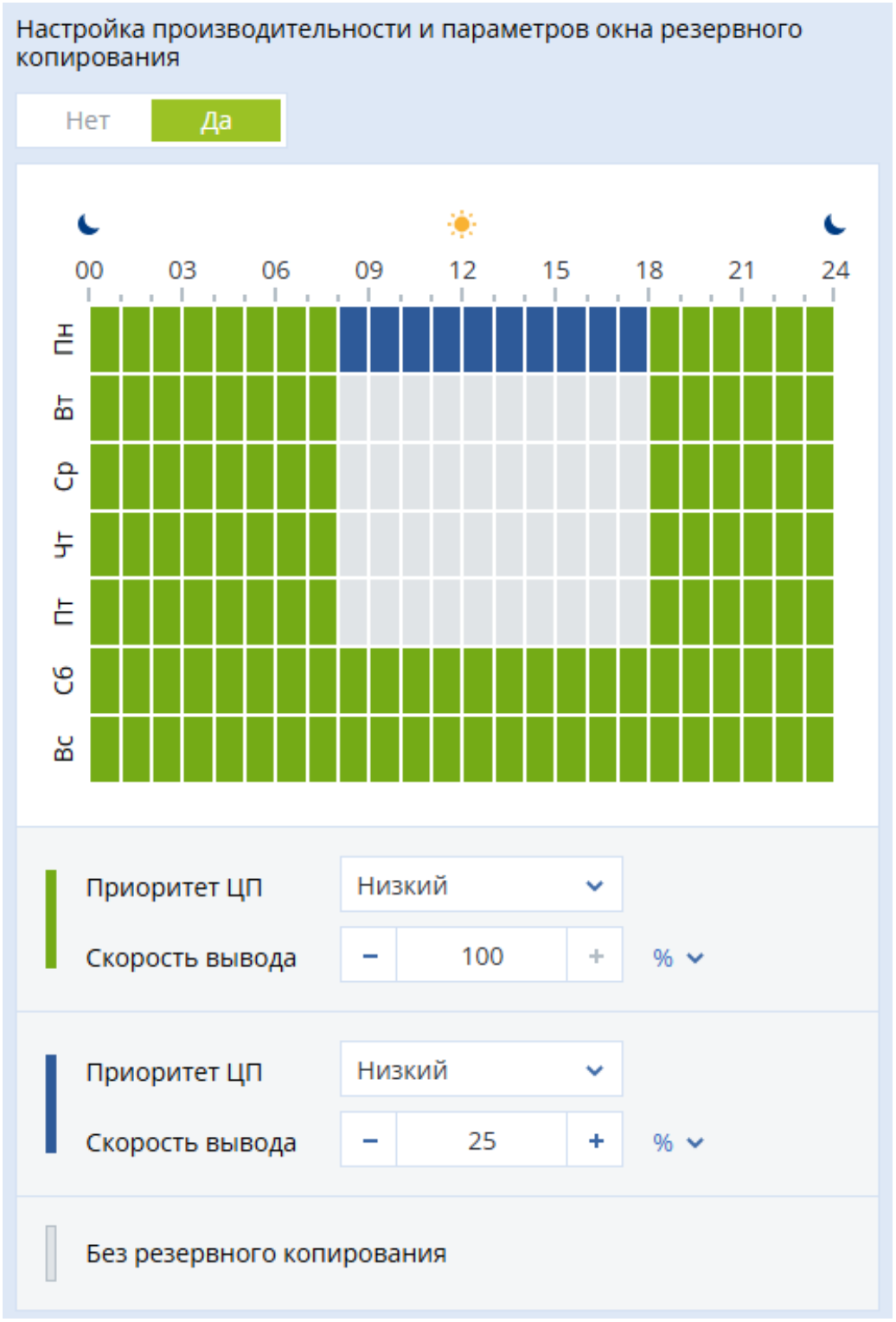
Даже если запланированные резервные копии заблокированы, резервное копирование можно запустить вручную. Для него будут использоваться параметры производительности последнего часа, когда процессы резервного копирования были разрешены.

12.12.17.1 Окно резервного копирования

Каждый прямоугольник представляет один час в пределах рабочего 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, щелкните один из них и расширьте выделение путем перетаскивания.



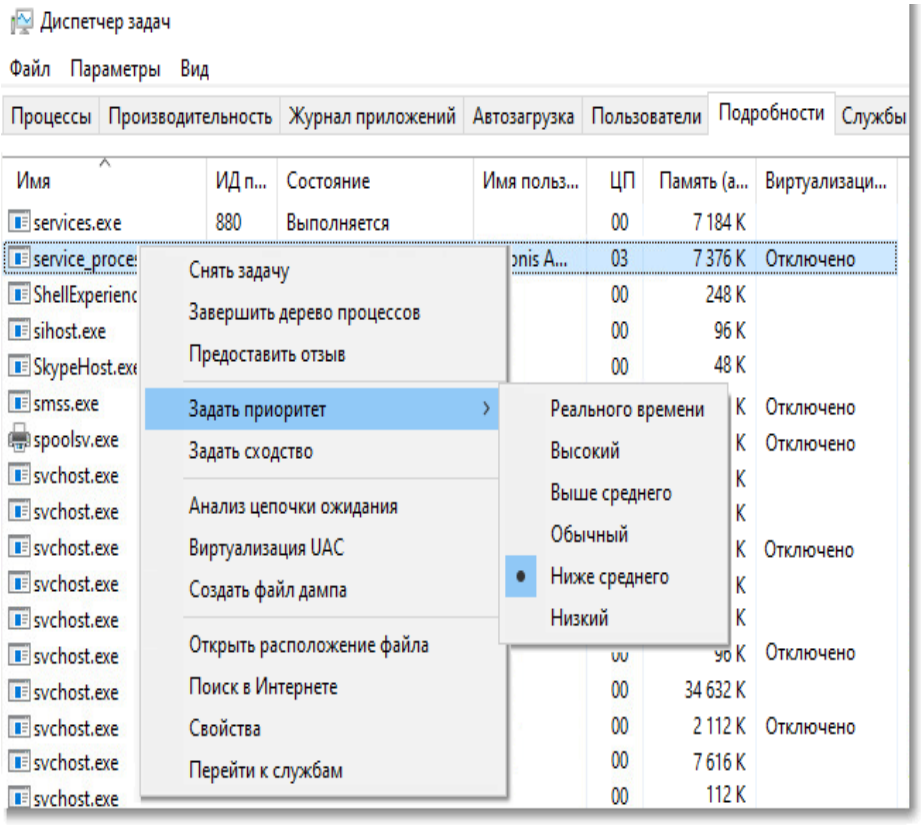
12.12.17.2 Приоритет ЦП

Этот параметр определяет приоритет процесса резервного копирования в операционной системе.

Доступные значения: **Низкий**, **Обычный**, **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.

Этот параметр задает приоритет процесса резервного копирования (**service_process.exe)** в Windows и его точность (**service_process)** в Linux и OS X.



12.12.17.3 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 или облачное хранилище данных).

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 или облачного хранилища данных).

  Эта настройка работает только в том случае, если агент выполняется в Windows.
- В КБ/секунду (для всех мест назначения).

12.12.18 Команды до и после процедуры

Этот параметр позволяет определить команды, которые должны выполняться автоматически перед выполнением процедуры резервного копирования или после нее.

Следующая схема иллюстрирует порядок выполнения команд до и после процедуры.

Команда до резервного копирования	Резервное копирование	Команда после резервного копирования

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.

Программа не поддерживает интерактивные команды, то есть команды, которые требуют пользовательского ввода (например, pause).

12.12.18.1 Команда до резервного копирования

Как 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 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 Облачный. 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 Облачный) 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*	Установить	Снять	Установить	Снять
Не продолжать создание резервной копии до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка 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).	Н/Д	Выполнить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

Примечание

Если сценарий завершается сбоем из-за конфликта, связанного с требуемой версией библиотеки Linux, исключите переменные среды LD_LIBRARY_PATH и LD_PRELOAD. Для этого добавьте в сценарий следующие строки:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

12.12.18.2 Команда после резервного копирования

Как указать команду или исполняемый файл, которые будут выполнены после завершения резервного копирования

1. Включить переключатель **Выполнение команды после резервного копирования**.
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 резервное копирование 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 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**.

12.12.19 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.

<---------- Резервная копия ---------->				
Команда до резервного копирования	Команда до захвата данных	Захват данных	Команда после захвата данных	Команда после резервного копирования

Если включен параметр «Служба теневого копирования томов (VSS)», то последовательность выполнения команд и операций Microsoft VSS будет следующей:

Команды «до захвата данных» -> приостановка VSS -> захват данных -> возобновление VSS -> команды «после захвата 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.

12.12.19.1 Команда до захвата данных

Как 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 Облачный. 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 Облачный) 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*	Установить	Снять	Установить	Снять
Не выполнять захват данных до полного выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка 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).	Н/Д	Выполнить захват данных одновременно с выполнением команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

Примечание
Если сценарий завершается сбоем из-за конфликта, связанного с требуемой версией библиотеки Linux, исключите переменные среды LD_LIBRARY_PATH и LD_PRELOAD. Для этого добавьте в сценарий следующие строки:

```
#!/bin/sh
unset LD_LIBRARY_PATH
unset LD_PRELOAD
```

12.12.19.2 Команда после захвата данных

Как 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**.

Флажок	**Выбор**			
Прерывать резервное копирование при сбое команды*	Установить	Снять	Установить	Снять
Не продолжать создание резервной копии до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Продолжить резервное	Продолжить резервное копирование после команды независимо	Н/Д	Продолжить резервное копирование

	копирование только после успешного выполнения команды.	от результатов ее выполнения (успешно или ошибка).		одновременно с выполнением команды и независимо от результатов выполнения команды.

* Команда считается сбойной, если код завершения не равен нулю.

12.12.20 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.

Значение по умолчанию: **Распределять время запуска резервного копирования по доступному времени. Максимальная задержка: 30 минут.**

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.

Резервное копирование физических машин запустится точно в соответствии с расписанием.

12.12.21 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.

12.12.22 Разбиение

Примечание
Параметр недоступен при резервном копировании в облачное хранилище данных.

Этот параметр позволяет выбрать метод разбиения резервных копий на меньшие по размеру фрагменты.

Значение по умолчанию:

- Если резервная копия расположена в локальной или сетевой папке (SMB) и имеет формат Version 12: **Постоянный размер 200 ГБ**

  Эта настройка позволяет программе резервного копирования работать с большими объемами данных в файловой системе NTFS без негативных последствий, вызванных фрагментацией файлов.
- В противном случае: **Автоматически**

Доступны следующие настройки:

- **Автоматически**

  Резервная копия будет разбита на части, если ее размер превышает максимальный размер файла, который поддерживается в файловой системе.

- **Заданный размер**

  Введите или выберите из раскрывающегося списка нужный размер файла.

12.12.23 Действия при сбое задания

Этот параметр определяет поведение программы при сбое запланированного плана защиты. Этот параметр не действует, 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**.

12.12.24 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.**

12.12.24.1 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.

12.12.24.2 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.

12.12.25 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**.

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 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.

12.12.25.1 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.

12.12.26 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, Hyper-V Integration Services или Red Hat Virtualization Guest Tools соответственно.

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.

12.12.27 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**.

12.12.28 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, которые будут заноситься в журнал, можно фильтровать.

Значение по умолчанию: **Отключено**.

12.13 Восстановление

12.13.1 Восстановление: памятка

В таблице ниже кратко описаны доступные методы восстановления. С ее помощью вы сможете выбрать способ, который лучше всего отвечает вашим потребностям.

Примечание
Восстановление через веб-интерфейс недоступно для клиентов в режиме «Улучшенная безопасность».

Объект восстановления	Метод восстановления
Физическая машина (Windows или Linux)	Использование веб-интерфейса Использование загрузочного носителя
Виртуальная машина (VMware, Hyper-V, Red Hat Virtualization (oVirt))	Использование веб-интерфейса Использование загрузочного носителя
Конфигурация ESXi	Использование загрузочного носителя
Файлы и папки	Использование веб-интерфейса Загрузка файлов из облачного хранилища данных Использование загрузочного носителя Извлечение файлов из локальных резервных копий
Базы данных SQL	Использование веб-интерфейса
Базы данных Exchange	Использование веб-интерфейса
Почтовые ящики Exchange	Использование веб-интерфейса

12.13.2 Восстановление машины

12.13.2.1 Физическая машина

В этом разделе описано восстановление физических машин через веб-интерфейс.

Используйте вместо веб-интерфейса загрузочный носитель, если вам необходимо восстановить:

- Машину с клиентом в режиме «Улучшенная безопасность».
- 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.

Примечание
Не поддерживается восстановление разделов больше 2 ТБ на дисках с таблицами разделов GPT с защитным MBR (Protective MBR). Подробнее см. в базе знаний.

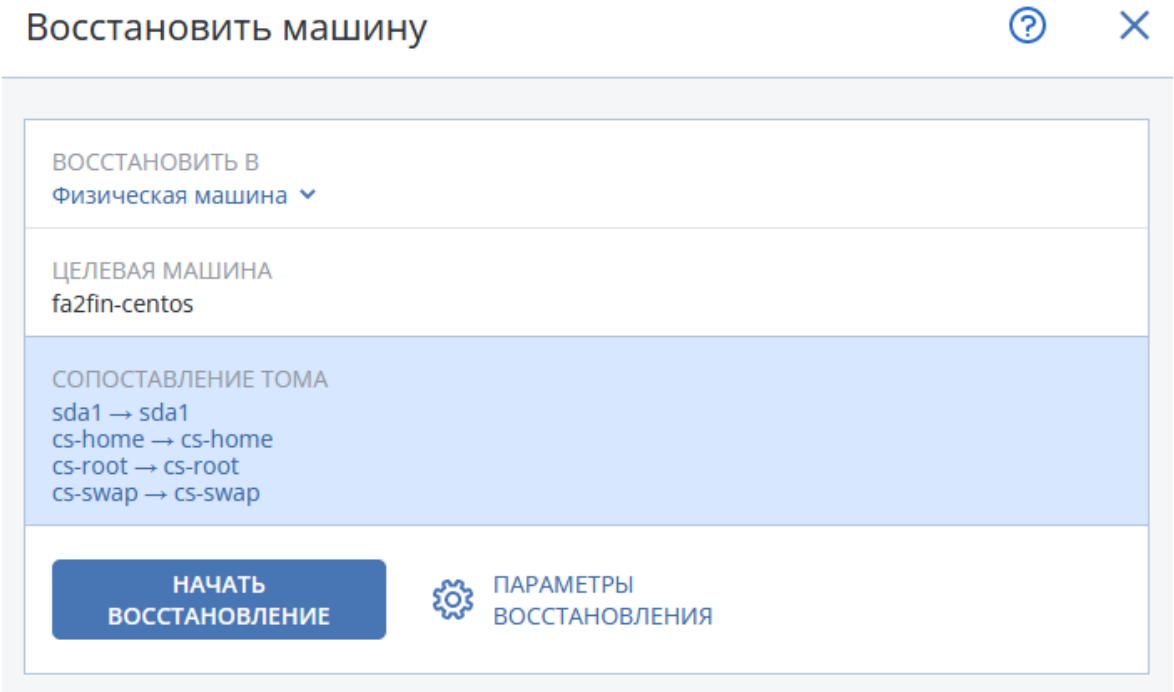
Восстановление физической машины

1. Выберите машину, для которой есть резервная копия.
2. Щелкните **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 облачном или общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилище резервных копий.
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя».
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.

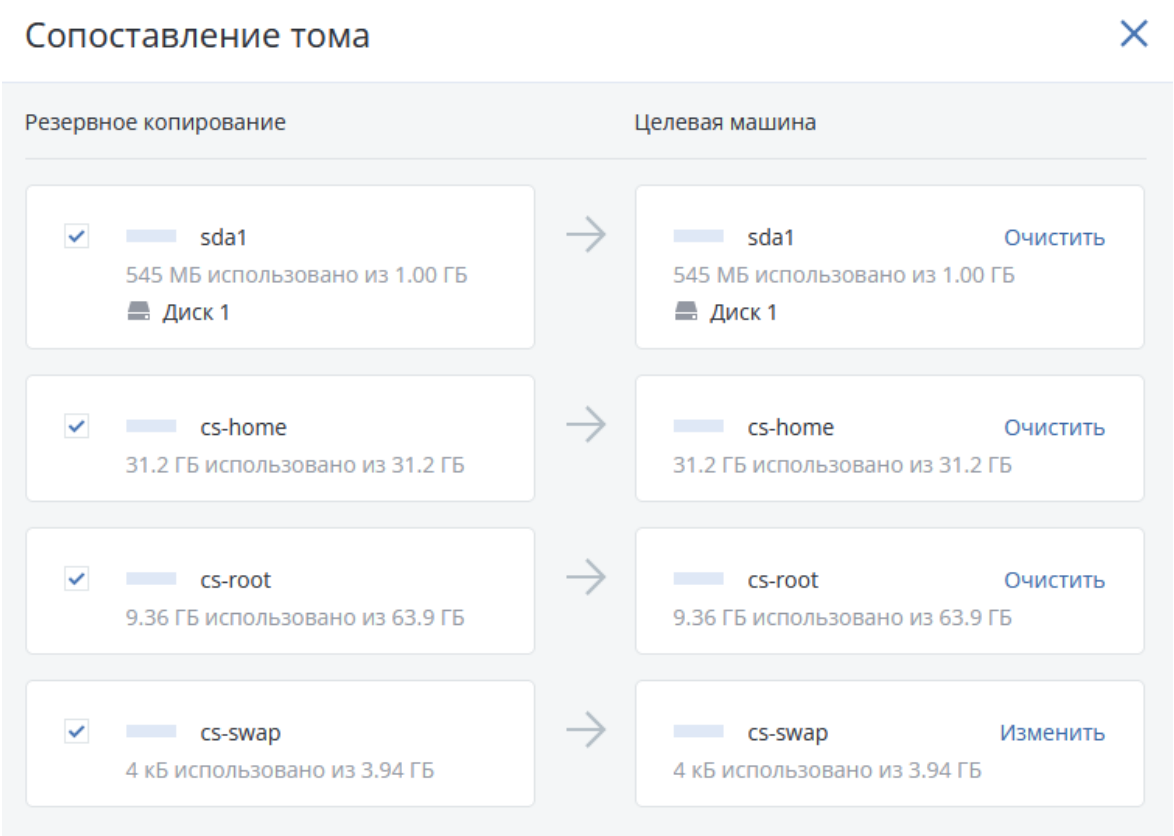
   Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

   Чтобы выполнить восстановление в другую виртуальную машину, щелкните **Целевая машина** и выберите включенную целевую машину.



5. Если результат сопоставления вас не удовлетворяет, или выполнить сопоставление не удалось, щелкните **Сопоставление тома**, чтобы сопоставить диски заново вручную.

   Раздел сопоставления также позволяет вам выбирать отдельные диски или тома для восстановления. Вы можете переключаться между восстановлением дисков и томов посредством ссылки **Переключиться на...** в верхнем правом углу.



6. Щелкните **Запуск восстановления**.
7. Подтвердите перезапись дисков версиями из резервной копии. Укажите, следует ли автоматически перезапустить машину.

Ход выполнения восстановления показан на вкладке **Действия**.

12.13.2.2 Восстановление физической машины в виртуальную

Физическую машину можно восстановить в виртуальную на одном из поддерживаемых гипервизоров. Такая же процедура используется для переноса физической машины в виртуальную. Дополнительную информацию о поддерживаемых способах миграции P2V см. в разделе Миграция машины.

В этом разделе описано восстановление физической машины в качестве виртуальной с использованием веб-интерфейса. Эту операцию можно выполнить, если в Киберпротект Management Server установлен и зарегистрирован хотя бы один агент для соответствующего гипервизора. Например, для восстановления на VMware ESXi требуется хотя бы один агент для VMware, для восстановления на Hyper-V – хотя бы один агент для Hyper-V, установленный и зарегистрированный в среде.

Восстановление через веб-интерфейс недоступно для клиентов в режиме «Улучшенная безопасность».

Восстановление физической машины как виртуальной

1. Выберите машину, для которой есть резервная копия.
2. Щелкните **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 облачном или общем хранилище данных (т .е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилище резервных копий.
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя».
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щелкните **Целевая машина**.

a. Выберите гипервизор.

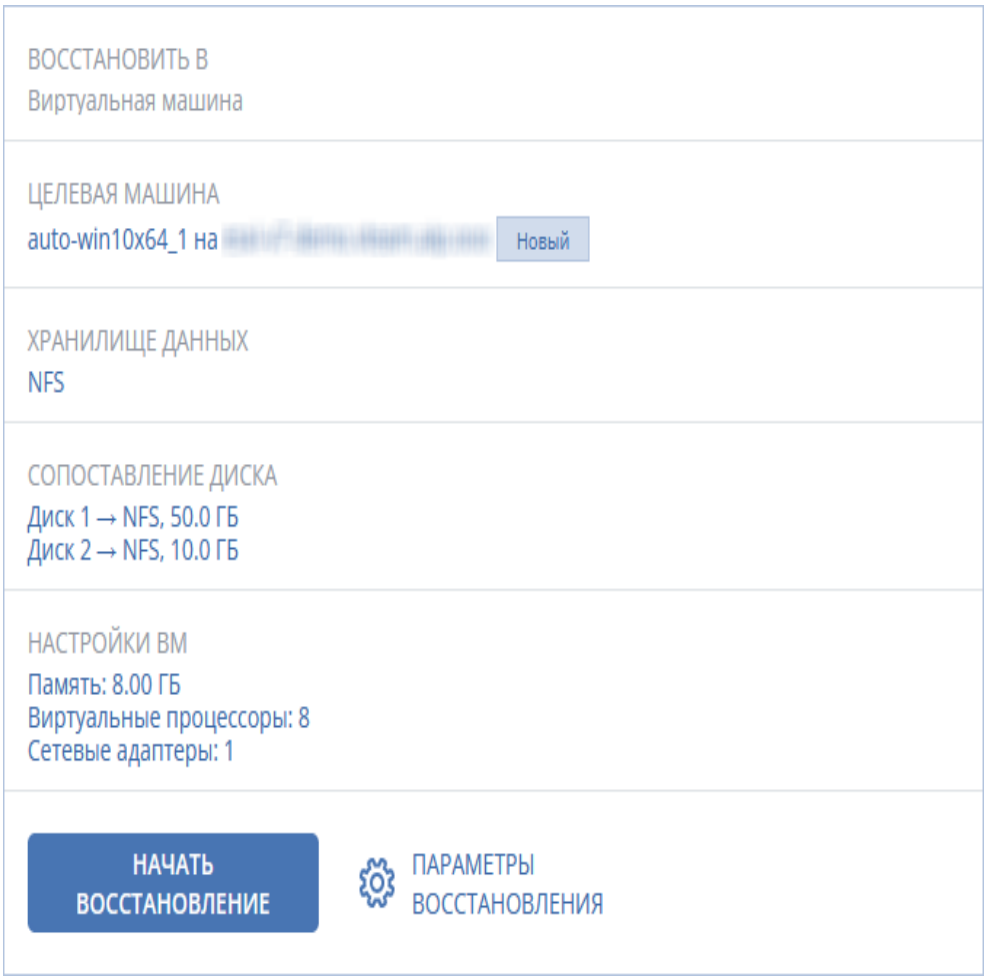
Примечание
Для этого гипервизора в Киберпротект Management Server должен быть установлен и зарегистрирован хотя бы один агент.

b. 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.

c. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.

d. Нажмите кнопку **OK**.

7. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
   - Щелкните **Сопоставление дисков**, чтобы выбрать хранилище данных, интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.
   - [Необязательно для VMware ESXi, Hyper-V и Red Hat Virtualization/oVirt] Щелкните **Настройки ВМ**, чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины.



8. Щелкните **Запуск восстановления**.
9. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход выполнения восстановления показан на вкладке **Действия**.

12.13.2.3 Виртуальная машина

Виртуальные машины можно восстановить с их резервных копий.

Примечание
Восстановление через веб-интерфейс недоступно для клиентов в режиме «Улучшенная безопасность».

Примечание
Не поддерживается восстановление разделов больше 2 ТБ на дисках с таблицами разделов GPT с защитным MBR (Protective MBR). Подробнее см. в базе знаний.

Предварительные требования

- В ходе восстановления данных на виртуальную машину она должна быть остановлена. По умолчанию программа останавливает машину без предупреждения. После завершения

восстановления машину потребуется запустить вручную. Поведение по умолчанию можно изменить, используя параметр восстановления "Управление питанием ВМ" (щелкните **Параметры восстановления** > **Управление питанием ВМ**).

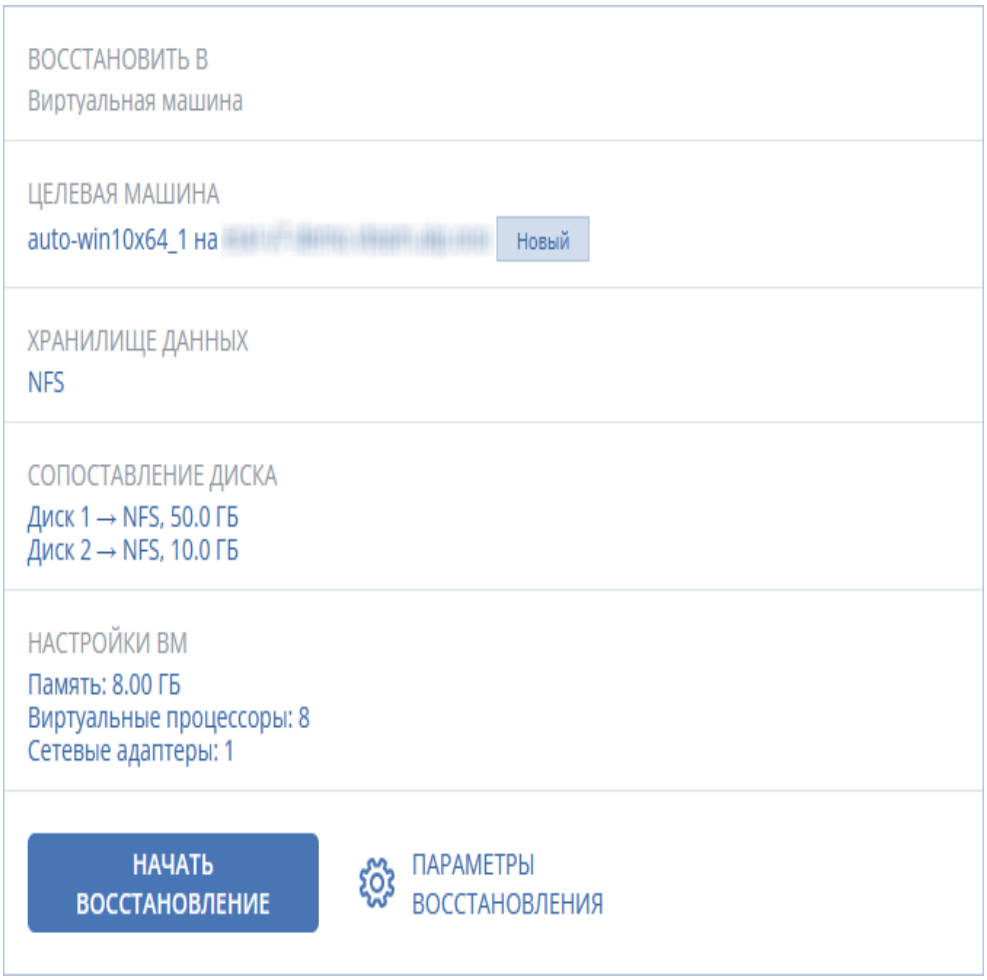
Процедура

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилище 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.

   Если это имеет место, продолжите с шага 4 в разделе «Физическая машина». В противном случае рекомендуется выполнить миграцию V2P, используя загрузочный носитель.
4. [Необязательно] По умолчанию данное программное обеспечение автоматически выбирает исходную машину в качестве целевой. Чтобы выполнить восстановление на = другую виртуальную машину, выберите **Целевая машина** и выполните следующие действия:
   a. Выберите гипервизор (**VMware ESXi**, **Hyper-V** или **oVirt**).
   b. Выберите машину, в которую будет выполняться восстановление: новая или существующая.
   c. Выберите хост и укажите имя новой машины или выберите существующую целевую машину.
   d. Нажмите кнопку **OK**.
5. Настройте дополнительные параметры восстановления по собственному усмотрению.
   - Чтобы выбрать хранилище данных для виртуальной машины, щелкните **Хранилище данных** для ESXi, **Путь** – для Hyper-V или **Домен хранилища** для Red Hat Virtualization (oVirt), а затем выберите хранилище данных (хранилище) для виртуальной машины.
   - [Необязательно] Чтобы просмотреть хранилище данных (хранилище), интерфейс и режим распределения для каждого виртуального диска, щелкните **Сопоставление диска**. Эти настройки можно изменить.

     Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.
   - [Необязательно для VMware ESXi, Hyper-V] Щелкните **Настройки ВМ**, чтобы изменить размер памяти и количество процессоров или сетевые подключения виртуальной машины.



6. Щелкните **Запуск восстановления**.
7. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход выполнения восстановления показан на вкладке **Действия**.

12.13.2.4 Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе "Создание физического загрузочного носителя" (стр. 392).

Порядок восстановления дисков с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, последовательно выберите пункты **Инструменты** > **Прокси-сервер** и укажите имя хоста или IP-адрес, порт и учетные данные прокси-сервера. В противном случае пропустите этот шаг.
4. [Необязательно] При восстановлении Windows или Linux последовательно выберите пункты **Инструменты** > **Зарегистрировать носитель в службе Кибер Бэкап Облачный** и введите маркер регистрации, полученный при загрузке носителя. Если вы сделаете это, для доступа к

облачному хранилищу данных (процедура описана в шаге 8) не нужно будет вводить учетные данные или код регистрации.

5. На экране приветствия нажмите кнопку **Восстановить**.
6. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
7. Укажите хранилище резервных копий.
   - Чтобы восстановить данные из облачного хранилища данных, выберите **Облачное хранилище данных**. Введите данные учетной записи резервного копирования, связанной с машиной, резервная копия которой вам нужна.

     При восстановлении Windows или Linux есть возможность запросить код регистрации и использовать его вместо учетных данных. Последовательно выберите пункты **Использовать код регистрации** > **Запросить код**. В программе будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. Код регистрации действует только один час.
   - Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **OK**, чтобы подтвердить выбор.
8. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
9. В разделе **Содержимое резервной копии** выберите диски, которые нужно восстановить. Нажмите кнопку **OK**, чтобы подтвердить выбор.
10. 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.

11. [При восстановлении ОС Linux] Если на машине, резервная копия которой создавалась, имелись логические тома (LVM), а вам необходимо воспроизвести исходную структуру LVM, выполните перечисленные ниже действия:
    a. Убедитесь, что количество дисков на целевой машине и емкость каждого диска равны аналогичным значениям исходной машины, а затем щелкните **Применить RAID/LVM**.
    b. Просмотрите структуру томов, а затем нажмите кнопку **Применить RAID/LVM**, чтобы создать ее.
12. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
13. Нажмите кнопку **OK**, чтобы начать восстановление.

12.13.2.5 Использование Universal Restore

Новейшие версии операционных систем сохраняют загружаемость при восстановлении на отличающееся оборудование или платформы VMware и Hyper-V. Если восстановленная операционная система не загружается, используйте средство Universal Restore, чтобы обновить драйверы и модули, необходимые для загрузки системы.

Universal Restore можно применить к операционным системам Windows и Linux.

Порядок использования Universal Restore

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Применение Universal Restore**.
3. Если на машине несколько операционных систем, выберите, к какой из них следует применить Universal Restore.
4. [Только для Windows] Настройка дополнительных настроек.
5. Нажмите кнопку **OK**.

Universal Restore в Windows

Подготовка

12.13.3 Подготовьте драйверы

Прежде чем применять 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 компонент Universal Restore.

12.13.4 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 Universal Restore

12.13.5 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, Universal Restore 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.

Universal Restore 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. Universal Restore выполняет также поиск драйвера сетевого адаптера. После его обнаружения Universal Restore передает путь к найденному драйверу операционной системе. Если на машине установлено несколько сетевых интерфейсных плат, Universal Restore попытается настроить драйверы всех плат.

12.13.6 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.

Процесс Universal Restore

Указав требуемые настройки, нажмите кнопку **OK**.

Если Universal Restore 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 Universal Restore. 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.

Universal Restore в Linux

Если Universal Restore применяется к операционной системе Linux, обновляется временная файловая система, известная как начальный электронный диск (initrd). Это обеспечивает загрузку операционной системы на новом оборудовании.

Universal Restore добавляет к начальному электронному диску модули для нового оборудования (включая драйверы устройств). Обычно все необходимые модули обнаруживаются в папке **/lib/modules**. Если Universal Restore не может найти нужный модуль, имя файла модуля записывается в журнал.

Universal Restore может изменить конфигурацию загрузчика GRUB. Возможно, для этого потребуется обеспечить загружаемость системы, если структура томов новой машины отличается от исходной машины.

Universal Restore 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 Universal Restore сохраняет его копию в той же папке. Имя копии – это имя файла с прибавлением суффикса **_cyberprotect_backup.img**. При запуске Universal Restore 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_cyberprotect_backup.img initrd-2.6.16.60-0.21-default
  ```

- Укажите копию в строке **initrd** конфигурации загрузчика GRUB.

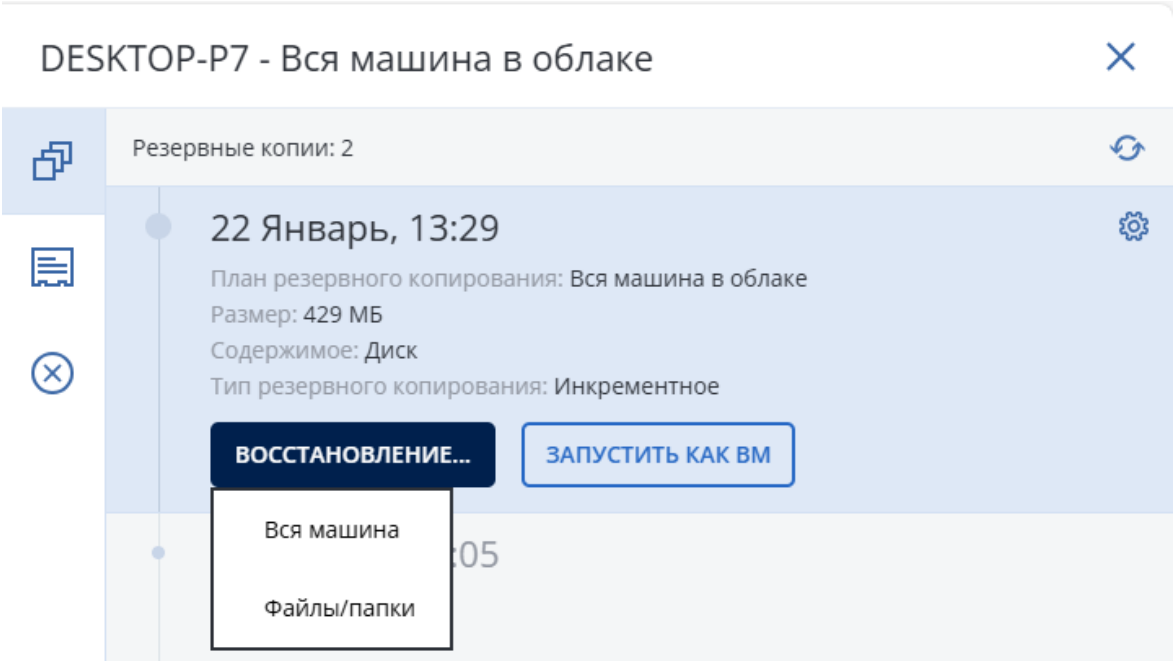
12.13.7 Восстановление файлов

12.13.7.1 Восстановление файлов с помощью веб-интерфейса

Примечание
Восстановление через веб-интерфейс недоступно для клиентов в режиме «Улучшенная безопасность».

1. Выберите машину, на которой ранее располагались данные, которые необходимо восстановить.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   Если выбрана физическая машина или машина в автономном режиме, то точки восстановления не отображаются. Выполните любое из следующих действий:
   - [Рекомендуется] Если резервная копия расположена в облачном или общем хранилище данных (т. е. другие агенты могут получить к ней доступ), щелкните **Выбрать машину**, выберите целевую машину, которая подключена, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилище резервных копий.
   - Загрузка файлов из облачного хранилища данных.
   - Использовать загрузочный носитель.
4. Последовательно выберите пункты **Восстановление** > **Файлы/папки**.



5. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов и папок.

Можно использовать один или несколько подстановочных символов (* и ?). Подробную информацию об использовании подстановочных символов см. в разделе «Фильтры файлов»..

Примечание
Поиск недоступен для резервных копий на уровне дисков, которые хранятся в облачном хранилище данных.

6. Выберите файлы, которые необходимо восстановить.
7. Чтобы сохранить файлы как ZIP-файл, нажмите кнопку **Загрузить**, выберите расположение для сохранения данных и нажмите кнопку **Сохранить**. В противном случае пропустите этот шаг.
   Загрузка недоступна, если среди выбранных элементов есть папки или общий размер выбранных файлов превышает 100 МБ.
8. Нажмите кнопку **Восстановить**.
   В поле **Восстановить в** будет отображаться один из следующих вариантов:
   - Машина, на которой изначально были файлы, которые необходимо восстановить (если на этой машине установлен агент).
   - Машина, на которой установлен агент для VMware, агент для Hyper-V или агент для oVirt (если файлы изначально находятся на виртуальной машине ESXi, Hyper-V или Red Hat Virtualization/oVirt).

   Это целевая машина для восстановления. При необходимости можно выбрать другую машину.
9. В поле **Путь** выберите целевое место восстановления. Можно выбрать один из следующих вариантов:
   - Исходное расположение (при восстановлении на исходную машину)
   - Локальная папка на целевой машине

     Примечание
     Символьные ссылки не поддерживаются.

   - Сетевая папка, которая доступна с целевой машины.
10. Нажмите кнопку **Запуск восстановления**.
11. Выберите один из вариантов перезаписи файла:
    - **Перезаписывать существующие файлы**
    - **Перезаписывать существующий файл, если он старше**
    - **Не перезаписывать существующие файлы**

Ход выполнения восстановления показан на вкладке **Действия**.

12.13.7.2 Загрузка файлов из облачного хранилища данных

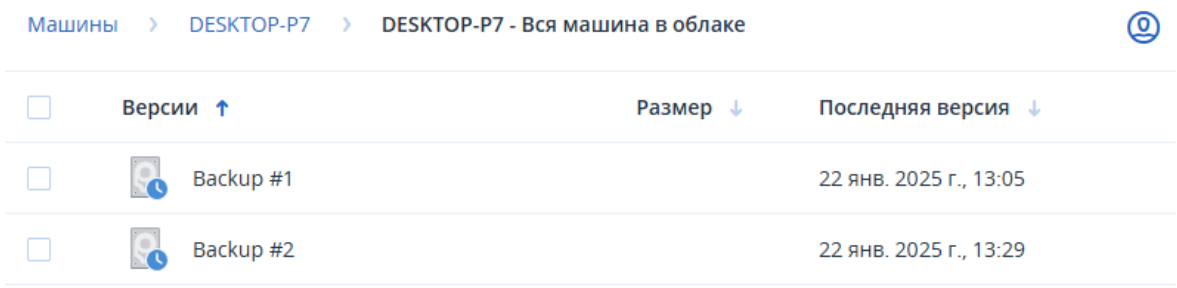
Вы можете просматривать содержимое облачного хранилища данных и резервных копий, а также загружать необходимые файлы.

Ограничения

- Резервные копии баз данных SQL и Exchange недоступны для просмотра.

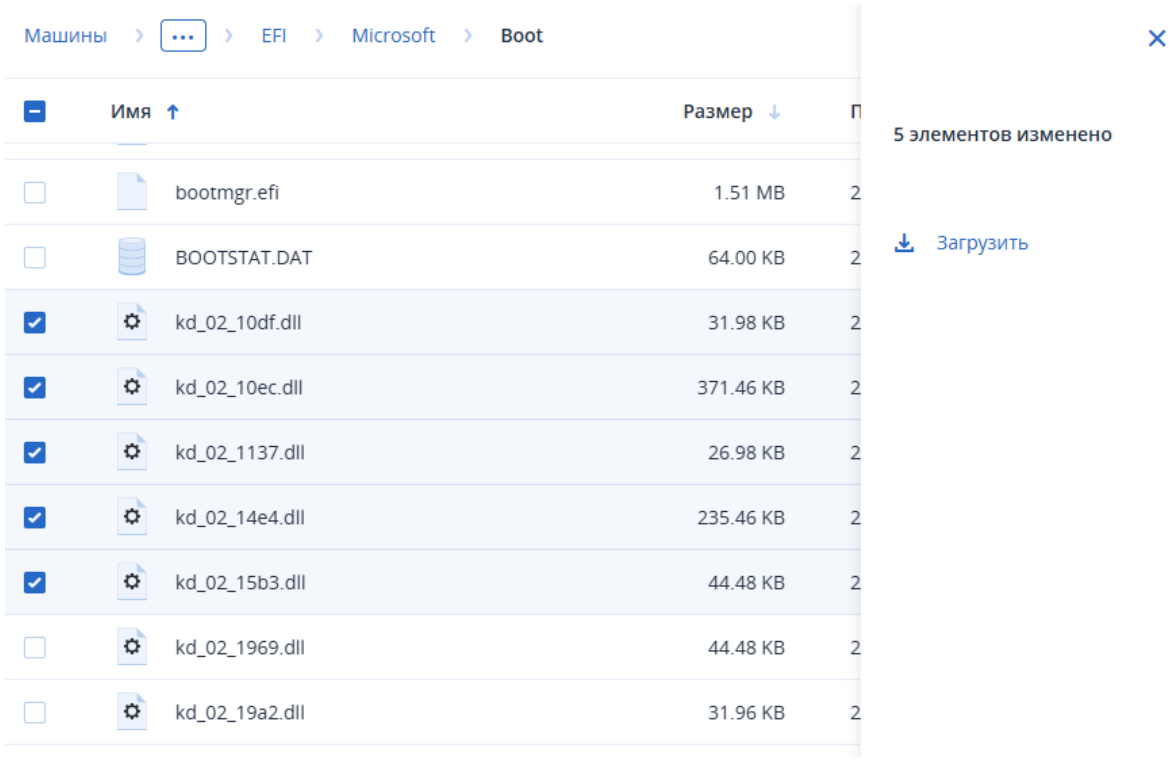
Загрузка файлов из облачного хранилища данных

1. Выберите машину, для которой была создана резервная копия.
2. Последовательно выберите пункты **Восстановление** > **Загрузить файлы**.
3. Введите данные учетной записи резервного копирования, связанной с машиной, резервная копия которой вам нужна.
4. [При просмотре резервных копий на уровне дисков] В разделе **Версии** выберите резервную копию, из которой необходимо восстановить файлы.



5. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов.
6. Установите флажки рядом с элементами для скачивания.

Примечание
Если выбрать несколько элементов, они будут скачаны как ZIP-файл.



7. Нажмите **Загрузить**.

12.13.7.3 Восстановление файлов с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя».

Восстановление файлов с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
3. Если в вашей сети включен прокси-сервер, последовательно выберите пункты **Инструменты** > **Прокси-сервер** и укажите имя хоста или IP-адрес, порт и учетные данные прокси-сервера. В противном случае пропустите этот шаг.
4. [Необязательно] При восстановлении Windows или Linux последовательно выберите пункты **Инструменты** > **Зарегистрировать носитель в службе Кибер Бэкап Облачный** и введите маркер регистрации, полученный при загрузке носителя. Если вы сделаете это, для доступа к облачному хранилищу данных (процедура описана в шаге 7) не нужно будет вводить учетные данные или код регистрации.
5. На экране приветствия нажмите кнопку **Восстановить**.
6. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.

7. Укажите хранилище резервных копий.
   - Чтобы восстановить данные из облачного хранилища данных, выберите **Облачное хранилище данных**. Введите данные учетной записи резервного копирования, связанной с машиной, резервная копия которой вам нужна.

     При восстановлении Windows или Linux есть возможность запросить код регистрации и использовать его вместо учетных данных. Последовательно выберите пункты **Использовать код регистрации** > **Запросить код**. В программе будет показана ссылка на регистрацию и код регистрации. Можно скопировать их и пройти все необходимые этапы регистрации на другой машине. Код регистрации действует только один час.
   - Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **OK**, чтобы подтвердить выбор.
8. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
9. В области **Содержимое резервной копии** выберите **Файлы/папки**.
10. Выберите данные, которые необходимо восстановить. Нажмите кнопку **OK**, чтобы подтвердить выбор.
11. В разделе **Место восстановления** укажите нужную папку. При желании можно запретить перезапись более новых версий файлов или исключить некоторые файлы из списка восстанавливаемых.
12. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
13. Нажмите кнопку **OK**, чтобы начать восстановление.

12.13.7.4 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 храниться 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 щелкните файл резервной копии. Файлы имеют имена на основе следующего шаблона:

   <имя машины> - <GUID плана защиты>

3. Если резервная копия зашифрована, введите пароль шифрования. В противном случае пропустите этот шаг.

   В проводнике отображаются точки восстановления.
4. Дважды щелкните 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.

12.13.8 Восстановление конфигурации ESXi

Чтобы восстановить конфигурацию ESXi, необходим загрузочный носитель на основе Linux. Информацию о том, как создать загрузочный носитель, см. в разделе "Создание физического загрузочного носителя" (стр. 392).

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. Щелкните **Локальное управление этой машиной**.
3. На экране приветствия нажмите кнопку **Восстановить**.
4. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
5. Укажите хранилище резервных копий.
   - Укажите папку в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **OK**, 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 **OK**.
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] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
13. Нажмите кнопку **OK**, чтобы начать восстановление.

12.13.9 Параметры восстановления

Чтобы изменить параметры восстановления, щелкните **Параметры восстановления** при настройке восстановления.

12.13.9.1 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.

	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	+	+	-	+	+	-	+	+
Команды до и после процедуры	+	+	-	+	+	-	+	+
Изменение идентификатора безопасности	+	-	-	-	-	-	-	-
Управление питанием ВМ	-	-	-	-	-	-	+	-
Журнал событий Windows	+	-	-	+	-	-	Только Hyper-V	+

12.13.9.2 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. Единственное исключение – проверка резервных копий на уровне файлов, которые расположены в облачном хранилище данных. Эти резервные копии проверяются путем проверки согласованности метаданных, сохраненных 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.

Примечание
В зависимости от настроек, выбранных поставщиком услуги, проверка может быть недоступна при резервном копировании в облачное хранилище данных.

12.13.9.3 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 с 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, начиная с Windows Vista SP1.
  - 64-разрядных операционных систем Windows Server, начиная с Windows Server 2008 SP1.
- Перенос между UEFI и BIOS не поддерживается, если резервная копия 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.

12.13.9.4 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: **Включено**.

12.13.9.5 Обработка ошибок

Они позволяют указать, как должны обрабатываться ошибки, возникшие при восстановлении.

В случае ошибки повторить попытку

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.

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 технической поддержки определить проблему.

12.13.9.6 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.

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.

12.13.9.7 Безопасность на уровне файлов

Этот параметр действует только при восстановлении файлов томов NTFS с диска и резервных копий на уровне файлов.

Этот параметр определяет, должны ли восстанавливаться разрешения NTFS вместе с файлами.

Значение по умолчанию: **Включено**.

Можно выбрать восстановление разрешений или наследование файлами их разрешений NTFS из папки, в которую они восстанавливаются.

12.13.9.8 Flashback

Этот параметр действует при восстановлении дисков и томов на физических и виртуальных машинах.

Этот параметр работает, только если структура восстанавливаемого тома диска в точности соответствует структуре тома целевого диска.

Если этот параметр включен, восстанавливаются только различия между данными в резервной копии и данными на целевом диске. Это ускоряет восстановление физических и виртуальных машин. Данные сравниваются на уровне блоков.

При восстановлении физической машины предварительно задана настройка **Отключено**.

При восстановлении виртуальной машины предварительно задана настройка **Включено**.

12.13.9.9 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**.

12.13.9.10 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.

12.13.9.11 Производительность

Этот параметр определяет приоритет процесса восстановления в операционной системе.

Доступные значения: **Низкий**, **Обычный**, **Высокий**.

Значение по умолчанию: **Обычное**.

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.

12.13.9.12 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

Как 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*	Установить	Снять	Установить	Снять
Не начинать восстановление до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				

	Предустановка 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).	Н/Д	Выполнить восстановление параллельно с выполнением команды независимо от результата ее выполнения.

* Команда считается сбойной, если код завершения не равен нулю.

Команда после восстановления

Как 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**.
6. Нажмите кнопку **Готово**.

Примечание
Команда после восстановления не будет выполнена, если восстановление заканчивается перезагрузкой.

12.13.9.13 Изменение идентификатора безопасности

Этот параметр действует при восстановлении ОС Windows 8.1 и Windows Server 2012 R2 или более ранних версий.

Этот параметр не работает, если восстановление на виртуальную машину выполняется агентом для VMware, агентом для Hyper-V или агентом для oVirt.

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.

12.13.9.14 Управление питанием ВМ

Эти параметры применяются, если восстановление на виртуальную машину выполняется агентом для VMware, агентом для Hyper-V или агентом для oVirt.

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.

12.13.9.15 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, которые будут заноситься в журнал, можно фильтровать.

Значение по умолчанию: **Отключено**.

12.14 Операции с резервными копиями

12.14.1 Вкладка «Хранилище резервных копий»

На вкладке **Хранилище резервных копий** предоставлен доступ ко всем резервным копиям, включая копии автономных машин и машин, которые больше не зарегистрированы в службе Кибер Бэкап Облачный.

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.

В облачном хранилище данных у пользователей есть доступ только к собственным резервным копиям.

Администратор может просматривать резервные копии в облаке от имени любой учетной записи, которая принадлежит данному отделу или компании и ее дочерним группам. Для этого он выбирает облачное хранилище данных для конкретной учетной записи. Чтобы выбрать устройство, которое нужно использовать для получения данных из облака, щелкните **Изменить** в строке **Машина для обзора**. На вкладке **Хранилище резервных копий** показаны резервные копии всех машин, когда-либо зарегистрированных для выбранной учетной записи.

Хранилища резервных копий, которые используются в планах защиты, автоматически добавляются на вкладку **Хранилище резервных копий**. Чтобы добавить другую папку (например, съемное USB-устройство) в список хранилищ резервных копий, щелкните **Обзор** и укажите путь к папке.

Если некоторые резервные копии добавлены или удалены в диспетчере файлов, щелкните значок шестерни рядом с именем хранилища, затем щелкните **Обновить**.

Предупреждение
Не пытайтесь редактировать файлы резервной копии вручную, поскольку это может привести к повреждению файла и сделать резервные копии нестабильными. Кроме того, мы рекомендуем реплицировать резервную копию, а не перемещать ее файлы вручную.

Хранилище резервных копий (за исключением облачного хранилища данных) исчезает с вкладки **Хранилище резервных копий**, если все машины, для которых когда-либо создавалась резервная копия в данном хранилище, были удалены из службы Кибер Бэкап Облачный. Это гарантирует, что вам не нужно будет платить за резервные копии, которые хранятся в этом хранилище. Как только в этом хранилище создается резервная копия, оно заново добавляется на вкладку резервных копий вместе со всеми резервными копиями в нем.

Порядок выбора точки восстановления на вкладке «Хранилище резервных копий»

1. На вкладке **Хранилище 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] Щелкните **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.

   Внимание
   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 щелкните **Восстановление**, дважды проверьте настройку **Целевая машина**, чтобы убедиться в правильности указанной машины, в которую будет выполнено восстановление. Чтобы изменить целевое место восстановления, укажите другую машину в поле **Машина для обзора**.
4. Щелкните **Показать резервные копии**.
5. Выберите точку восстановления.

12.14.2 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. Тома подключаются в режиме только для чтения.

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.

Порядок подключения тома из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щелкните файл резервной копии. Файлы имеют имена на основе следующего шаблона:

   <имя машины> - <GUID плана защиты>

3. Если резервная копия зашифрована, введите пароль шифрования. В противном случае пропустите этот шаг.

   В проводнике отображаются точки восстановления.
4. Дважды щелкните точку восстановления.

   В проводнике отображаются тома, для которых созданы резервные копии.

   Примечание
   Дважды щелкните том для обзора его содержимого. Можно скопировать файлы и папки из резервной копии в любую папку в файловой системе.
5. Щелкните подключаемый том правой кнопкой мыши и выберите пункт **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 **Компьютер** (**Этот компьютер** в Windows 8.1 и более поздней версии).
2. Правой кнопкой мыши щелкните подключенный том.
3. Нажмите **Отключить**.

   Программа отключит выбранный том.

12.14.3 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 консоли службы

1. На вкладке **Все устройства** выберите машину, резервные копии которой необходимо удалить.
2. Щелкните **Восстановление**.
3. Выберите хранилище, в котором расположены резервные копии для удаления.
4. Удалите нужные резервные копии. Можно удалить всю цепочку резервных копий или одну резервную копию в ней.
   - удалить всю цепочку резервных копий, щелкните **Удалить все**.
   - Порядок удаления одной резервной копии в выбранной цепочке
     a. Выберите резервную копию для удаления и щелкните значок шестерни.

b. Щелкните **Удалить**.

5. Подтвердите операцию.

Порядок удаление резервных копий на любой машине

1. На вкладке **Хранилище 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 в цепочки резервных копий. Для имен цепочки резервных копий используется следующий шаблон:

   - <имя машины> - <имя плана защиты>
   - Для резервных копий «облако в облако»: <имя пользователя> или <имя диска> - <облачная служба> - <имя плана защиты>
2. Выберите цепочку резервных копий.
3. Удалите нужные резервные копии. Можно удалить всю цепочку резервных копий или одну резервную копию в ней.
   - Чтобы удалить всю цепочку резервных копий, щелкните **Удалить**.
   - Порядок удаления одной резервной копии в выбранной цепочке
     a. Щелкните **Показать резервные копии**.
     b. Выберите резервную копию для удаления и щелкните значок шестерни.
     c. Щелкните **Удалить**.
4. Подтвердите операцию.

Порядок удаления резервных копий непосредственно из облачного хранилища данных

1. Войдите в облачное хранилище данных, как описано в разделе "Загрузка файлов из облачного хранилища данных".
2. Щелкните имя машины, для которой необходимо удалить резервные копии.

   В программе будет показано несколько групп резервных копий.
3. Щелкните значок шестерни рядом с группой резервных копий, которую необходимо удалить.
4. Нажмите кнопку **Удалить**.
5. Подтвердите операцию.

Если вы удалили локальные резервные копии в диспетчере файлов

Мы рекомендуем удалять резервные копии в консоли службы, когда это возможно. Если вы удалили локальные резервные копии в диспетчере файлов, выполните следующие действия:

1. На вкладке **Хранилище резервных копий** щелкните значок шестерни рядом с именем хранилища.
2. Нажмите кнопку **Обновить**.

Таким образом вы передадите в службу Кибер Бэкап Облачный информацию об уменьшении использования локального хранилища данных.

12.15 Защита приложений Microsoft

12.15.1 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.

Для Microsoft Exchange Server вы можете выбрать **Резервное копирование почтового ящика**. При выборе данной опции 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.

12.15.2 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.

12.15.3 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	Вся машина Базы данных в запущенный Exchange	Вся машина

	Фрагментарное восстановление в запущенный Exchange*	Базы данных как файлы Фрагментарное восстановление в запущенный Exchange*	
Доменные службы Active Directory	-	Вся машина	-

* Фрагментарное восстановление также доступно из резервной копии почтового ящика.

12.15.4 Предварительные требования

Перед настройкой резервного копирования приложений убедитесь, что перечисленные ниже требования выполнены.

Чтобы проверить состояние модуля записи VSS, используйте команду vssadmin list writers.

12.15.4.1 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 2.0 или более поздней версии.
- Установлена платформа Microsoft .NET Framework 3.5 или более поздней версии.
- Модуль записи Exchange для VSS включен.

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 и машин с установленным агентом включен параметр резервного копирования Служба теневого копирования томов (VSS).
- Для виртуальных машин включен параметр резервного копирования Служба теневого копирования томов (VSS) для виртуальных машин.

12.15.4.2 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 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 2008 или более поздней версии.
- Для Hyper-V 2008 R2: в качестве гостевой операционной системы используется Windows Server 2008/2008 R2/2012.
- 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, доступное по ссылке.

- В настройках виртуальной машины включен параметр **Управление** > **Службы интеграции** > **Резервное копирование (контрольная точка тома)**.
- Для Hyper-V 2012 и более поздних версий: виртуальная машина не имеет контрольных точек.
- Для Hyper-V 2012 и более поздних версий: виртуальная машина имеет контроллер SCSI (проверьте **Настройки** > **Оборудования**).

12.15.5 Резервное копирование базы данных

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.

12.15.5.1 Выбор баз данных SQL

Резервная копия базы данных SQL 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 SQL. Усечение журнала SQL можно отключить в параметрах плана защиты.

Порядок выбора баз данных SQL

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 щелкните элементы списка, расположенного справа от дерева.
3. Выберите данные, резервную копию которых необходимо создать. Выберите AAGs, машины, на которых запущен SQL Server, экземпляры SQL Server или отдельные базы данных.
   - При выборе AAG, для всех баз данных, включенных в выбранную AAG, будет создана резервная копия.
   - При выборе машины на которых запущен SQL Server, будет создана резервная копия всех баз данных, подключенных к экземпляру SQL Server.
   - При выборе экземпляра 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. Щелкните **Защитить**. 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.

12.15.5.2 Выбор данных Exchange Server

В таблице ниже приведены основные сведения о том, какие именно данные Microsoft Exchange Server можно выбрать для резервного копирования, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2013/2016/2019	Базы данных, Группы обеспечения доступности баз данных (DAG)	Участие в группе ролей **Управление сервером**.

При полном резервном копировании в копию включаются все выбранные данные Exchange Server.

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 Server

1. Нажмите **Устройства** > **Microsoft Exchange**.

   Программное обеспечение отобразит дерево групп обеспечения доступности баз данных (DAG) Exchange Server, машины, на которых запущен Microsoft Exchange Server, и базы данных Exchange Server. Если агент для Exchange настроен, как описано в разделе «Резервное копирование почтовых ящиков», в этом дереве также отображаются почтовые ящики.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды щелкните 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«Защита групп обеспечения доступности базы данных (DAG)».
   - При выборе машины на которых запущен сервер Microsoft Exchange, будет создана резервная копия всех баз данных, подключенных к серверу Exchange.
   - 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. Щелкните **Защитить**.

12.15.6 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 приложений** для дополнительной защиты данных этих приложений.

12.15.6.1 Почему нужно использовать резервное копирование 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 восстановления 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.

12.15.6.2 Что необходимо для использования 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 приложений. Чтобы восстановить данные приложений из резервных копий, созданных этим агентом, необходимо иметь агент для VMware

(Windows), агент для SQL или агент для Exchange на машине с доступом к хранилищу, в котором хранятся резервные копии. При настройке восстановления данных приложения выберите точку восстановления на вкладке **Хранилище резервных копий**, а затем выберите эту машину в списке **Машина для обзора**.

Другие требования перечислены в разделах «Предварительные требования» и «Необходимые права пользователя».

12.15.6.3 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:

  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 Exchange Server:

  Учетная запись должна входить в группу **Администраторы** на данной машине, а также в группу ролей **Управление организацией**.
- Для Active Directory:

  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).

12.15.7 Резервная копия почтового ящика

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. Щелкните **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, щелкните **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**.

12.15.7.1 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. Щелкните **Защитить**.

12.15.7.2 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.

Минимальные требуемые права пользователя:

- Учетная запись должна входить в группы ролей **Управление сервером** и **Управление получателями**.
- Для учетной записи должна быть включена роль управления **ApplicationImpersonation** для всех пользователей или групп пользователей, к почтовым ящикам которых будет обращаться агент.

  Информацию о настройке роли управления **ApplicationImpersonation** см. в статье базы знаний Microsoft.

12.15.8 Восстановление баз данных SQL

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. Щелкните **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 облачном хранилище или 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 Хранилище 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

   a. Щелкните имя базы данных.

   b. В поле **Восстановить в** выберите вариант **Новая база данных**.

   c. Укажите имя новой базы данных.

   d. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов.
6. [Необязательно] [Недоступно для базы данных, восстановленной в свой исходный экземпляр как новая база данных] Чтобы изменить состояние базы данных после восстановления, щелкните 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.
   - **Не работает (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.

- **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. Щелкните **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. Щелкните **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 облачном хранилище или 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 Хранилище 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. Щелкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке Действия.

12.15.8.1 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.

12.15.8.2 Подключение баз данных SQL Server

В этом разделе описывается процедура подключения базы данных в 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 Microsoft SQL Server Management Studio.
2. Подключитесь к требуемому экземпляру SQL Server и разверните его.

3. Правой кнопкой мыши щелкните пункт **Базы данных** и щелкните **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.

   Подробнее. Файлы базы данных 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 SQL Server из резервной копии.
7. Когда все файлы будут найдены, нажмите кнопку **OK**.

12.15.9 Восстановление баз данных Exchange

В этом разделе описано восстановление из резервных копий базы данных и резервных копий с поддержкой приложений.

Можно восстановить данные Exchange Server в работающий Exchange Server. Это может быть исходный Exchange Server или Exchange Server 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 Server можно выбрать для восстановления, а также о минимальных правах пользователя, которые для этого необходимы.

Версия Exchange	Элементы данных	Права пользователя
2013/2016/2019	Базы данных	Участие в группе ролей **Управление сервером**.

Базы данных (группы хранения) 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).

В нижеуказанной процедуре как базы данных, так и группы хранения описываются термином «базы данных».

Для восстановления баз данных Exchange на запущенный сервер Exchange 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 Exchange** > **Базы данных** и затем выберите базы данных, которые необходимо восстановить.
2. Щелкните **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 облачном хранилище или 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 Хранилище 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
   a. Щелкните имя базы данных.
   b. В поле **Восстановить в** выберите вариант **Новая база данных**.
   c. Укажите имя новой базы данных.
   d. Укажите путь к новой базе данных и журналу. В указанной папке не должно быть файлов исходной базы данных и ее журналов.
6. Щелкните **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. Щелкните **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 облачном хранилище или 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 Хранилище 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. Щелкните **Запуск восстановления**.

Ход выполнения восстановления показан на вкладке Действия.

12.15.9.1 Подключение баз данных 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 Server и локальную группу администраторов для данного целевого сервера.

Подробную информацию о подключении базы данных см. в документации Microsoft Exchange Server.

12.15.10 Восстановление почтовых ящиков Microsoft Exchange и элементов почтового ящика

В этом разделе описана процедура восстановления почтовых ящиков Microsoft 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 Microsoft 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.

12.15.10.1 Восстановление на целевой Microsoft Exchange Server

Фрагментарное восстановление может быть выполнено агентом для Microsoft Exchange или агентом для VMware (Windows). Целевой Microsoft Exchange Server и машина с работающим агентом должны быть в одном лесу Active Directory.

Если почтовый ящик восстанавливается в существующий почтовый ящик, то элементы с одинаковыми идентификаторами будут перезаписаны.

При восстановлении элементов почтового ящика перезапись не происходит. Вместо этого в целевой папке заново создаётся полный путь к элементу почтового ящика.

Требования к учётным записям пользователей

Почтовый ящик, восстанавливаемый из резервной копии, должен иметь связанную с ним учётную запись пользователя в Active Directory.

Пользовательские почтовые ящики и их содержимое можно восстановить, только если *включены* связанные с ними учётные записи пользователей. Общие почтовые ящики, почтовые ящики помещения и оборудования могут быть восстановлены, только если соответствующие учётные 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.

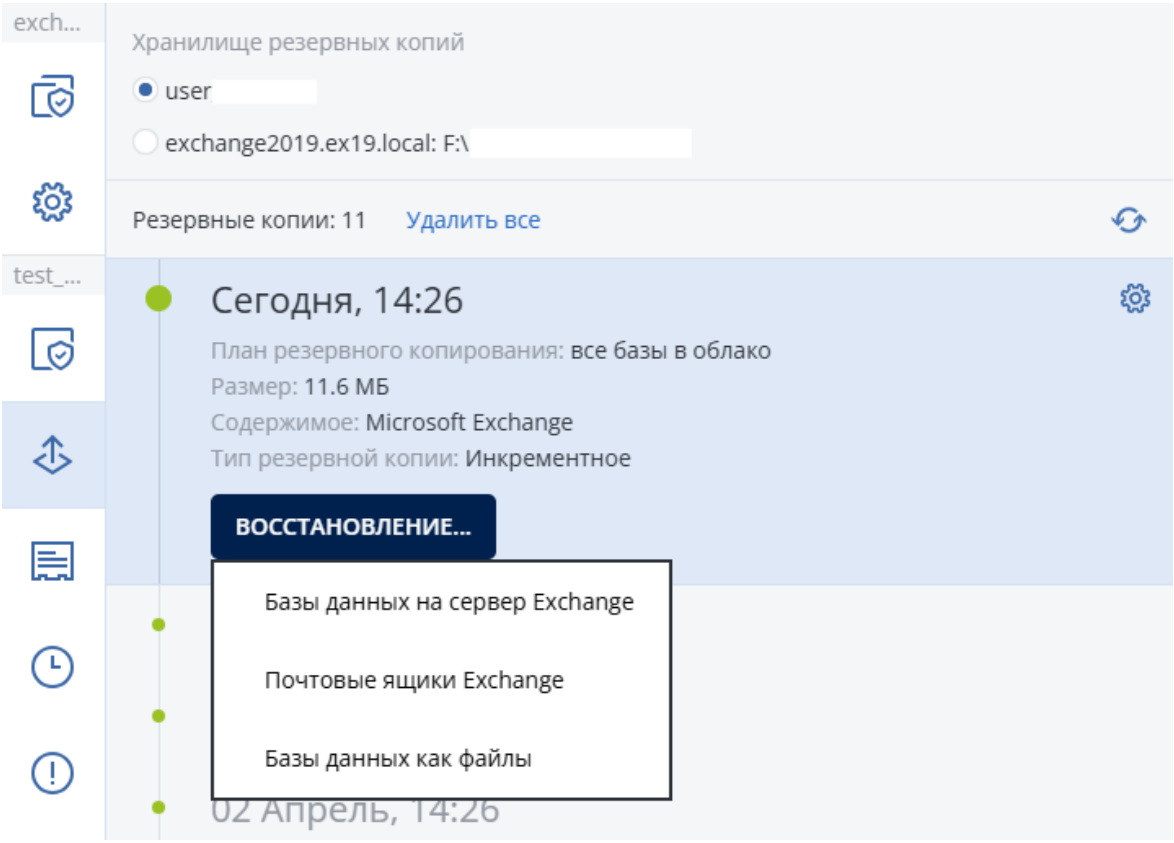
12.15.10.2 Восстановление почтовых ящиков

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.

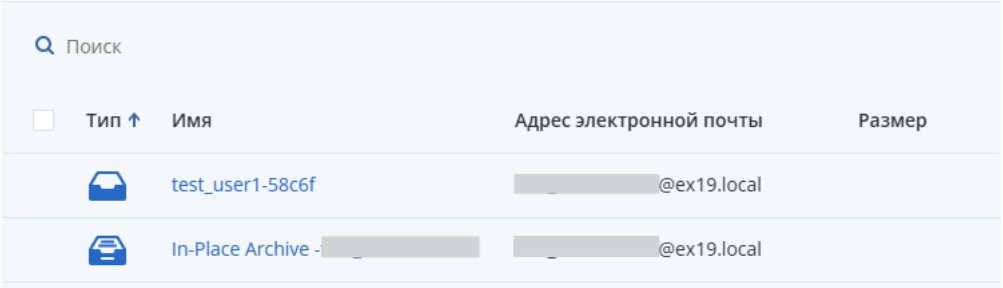
   Если машина отключена, точки восстановления не отображаются. В этом случае воспользуйтесь одним из перечисленных ниже способов.
   - [Только при восстановлении из резервной копии с поддержкой приложений] Если резервная копия расположена в облачном хранилище или общем хранилище (т. е. другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включенную машину, на которой установлен агент для Microsoft Exchange или агент для VMware, а затем выберите точку восстановления.
   - Выберите точку восстановления на вкладке Хранилище 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**.

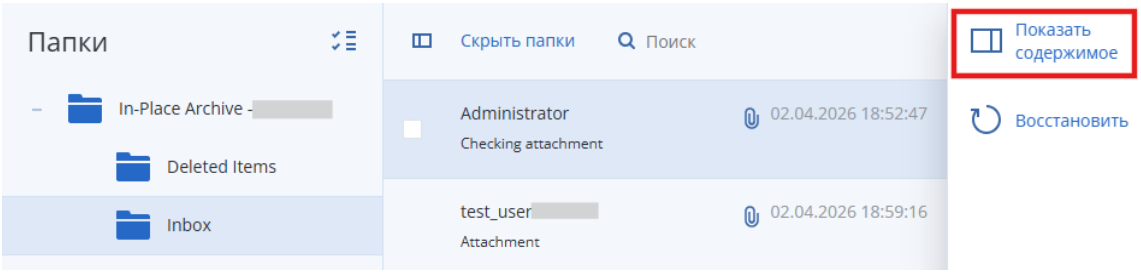


5. Выберите почтовые ящики, которые необходимо восстановить. Архивные почтовые ящики имеют специальную иконку и имя, состоящее из названия архива писем и псевдонима пользователя.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.



   Для просмотра содержимого выбранного почтового ящика внутри резервной копии нажмите **Показать содержимое**. Чтобы загрузить вложенный файл, щёлкните его имя.



6. Нажмите кнопку **Восстановить**.

Чтобы выбрать или изменить целевую машину, щёлкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Microsoft 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.

7. 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. [Необязательно] Чтобы изменить автоматически выбранную базу данных, щёлкните **База данных для воссоздания отсутствующих почтовых ящиков**.
9. Щёлкните **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 **Восстановление**.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.

   Если почтовый ящик был удалён, выберите его на вкладке Хранилище 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** > **Весь почтовый ящик**.
5. Выполните шаги 5-9 вышеописанной процедуры.

12.15.10.3 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 облачном хранилище или общем хранилище (т. е. другие агенты могут получить к ней доступ), нажмите **Выбрать машину**, выберите включённую машину, на которой установлен агент для Microsoft Exchange или агент для VMware, а затем выберите точку восстановления.
- Выберите точку восстановления на вкладке Хранилище резервных копий.

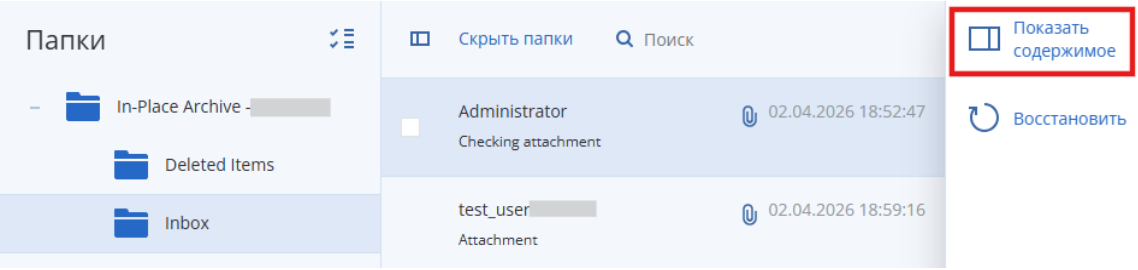
Вместо выключенной исходной машины восстановление будет выполнено с помощью машины, которая выбрана для просмотра одним из двух указанных выше действий.

4. Щёлкните **Восстановление** > **Почтовые ящики Exchange**.
5. Щёлкните почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить.
6. Выберите элементы, которые необходимо восстановить.

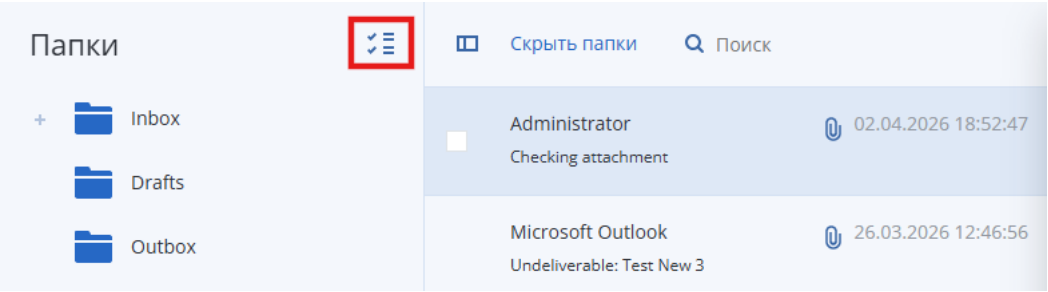
   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - 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.

   Если выбрано сообщение электронной почты, можно посмотреть его содержимое, щёлкнув **Показать содержимое**. Чтобы загрузить вложенный файл, щёлкните его имя.



   Чтобы выбрать папки, щёлкните значок восстановления папок, после чего установите флажки для выбранных элементов.



7. Нажмите кнопку **Восстановить**.

8. Чтобы выполнить восстановление на Microsoft Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.

   [Только при восстановлении на Microsoft Exchange Server] Чтобы выбрать или изменить целевую машину, щёлкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Microsoft 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.
9. 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.
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. Щёлкните **Запуск восстановления**.

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 удалён, выберите его на вкладке Хранилище 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 посмотреть его содержимое, щёлкнув **Показать содержимое**. Чтобы загрузить вложенный файл, щёлкните его имя.

Выбранное сообщение электронной почты также можно отправить по адресу электронной почты. Для этого щёлкните **Отправить как сообщение электронной почты**. Сообщение отправится с адреса электронной почты администратора учётной записи.

Чтобы выбрать папки, щёлкните значок восстановления папок  , после чего установите флажки для выбранных элементов.

6. Нажмите кнопку **Восстановить**.
7. Выполните шаги 8-12 вышеописанной процедуры.

12.15.10.4 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%\Киберпротект\ese**. Если папка не существует, создайте ее вручную.

12.15.11 Изменение учетных данных для доступа к SQL Server или Exchange Server

Можно изменить учетные данные для доступа к SQL Server или Exchange Server без переустановки агента.

Для изменения учетных данных для доступа к SQL Server или Exchange Server

1. Щелкните **Устройства**, а затем щелкните **Microsoft SQL** или **Microsoft Exchange**.

2. Выберите группу обеспечения доступности Always On, группу обеспечения доступности баз данных, экземпляр SQL Server или Exchange Server, для которых необходимо изменить учетные данные.
3. Щелкните **Укажите учетные данные**
4. Укажите новые учетные данные для доступа, а затем щелкните **OK**.

Для изменения учетных данных Exchange Server для доступа к резервной копии почтового ящика

1. Щелкните **Устройства** > **Microsoft Exchange** и разверните узел **Почтовые ящики**.
2. Выберите Microsoft Exchange для которого необходимо изменить учетные данные для доступа.
3. Щелкните **Настройки**.
4. Ниже поля **Учетная запись администратора Exchange** укажите новые учетные данные для доступа, а затем щелкните **Сохранить**.

12.16 Защита размещенных данных Exchange

12.16.1 Для каких элементов можно создавать резервные копии?

Можно создать резервную копию почтовых ящиков пользователя, общих почтовых ящиков и почтовых ящиков группы. При необходимости можно выбрать резервное копирование архивных почтовых ящиков (**архив на месте**) для выбранных почтовых ящиков.

12.16.2 Какие элементы можно восстановить?

Из резервной копии почтового ящика можно восстановить следующие элементы:

- почтовые ящики;
- папки электронной почты;
- сообщения электронной почты;
- события календаря;
- задания;
- контакты;
- записи журнала;
- заметки.

Чтобы найти эти элементы, можно воспользоваться поиском.

При восстановлении почтовых ящиков, элементов почтовых ящиков, общих папок и элементов общих папок можно выбрать, перезаписывать ли элементы в целевое расположение.

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.

12.16.3 Выбор почтовых ящиков

Выберите почтовые ящики, как указано ниже, а затем укажите другие настройки плана защиты как требуется.

1. Щелкните **Устройства > Размещенный Exchange**.
2. Если в службу Кибер Бэкап Облачный добавлено несколько размещенных организаций Exchange, выберите ту организацию, для пользователей которой необходимо создать резервные копии данных. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы создать резервную копию почтовых ящиков всех пользователей и всех общих почтовых ящиков (включая почтовые ящики, которые будут созданы в будущем), разверните узел **Пользователи**, выберите **Все пользователи** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков отдельных пользователей или общих почтовых ящиков, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователей, для почтовых ящиков которых необходимо создать резервные копии, и щелкните **Резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков всех групп (включая почтовые ящики групп, которые будут созданы в будущем), разверните узел **Группы**, выберите **Все группы** и щелкните **Групповое резервное копирование**.
   - Чтобы создать резервную копию почтовых ящиков отдельных групп, разверните узел **Группы**, выберите **Все группы**, затем выберите группы, для почтовых ящиков которых необходимо создать резервные копии, и щелкните **Резервное копирование**.

12.16.4 Восстановление почтовых ящиков и элементов почтовых ящиков

12.16.4.1 Восстановление почтовых ящиков

1. Щелкните **Устройства > Размещенный Exchange**.
2. Если в службу Кибер Бэкап Облачный добавлено несколько размещенных организаций Exchange, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы восстановить почтовый ящик пользователя, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, почтовый ящик которого необходимо восстановить, и щелкните **Восстановить**.

- Чтобы восстановить общий почтовый ящик, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите общий почтовый ящик, который необходимо восстановить, и щелкните **Восстановить**.
- Чтобы восстановить почтовый ящик группы, разверните узел **Группы**, выберите **Все группы**, затем выберите группу, почтовый ящик которой необходимо восстановить, и щелкните **Восстановить**.
- Если пользователь, группа или общий почтовый ящик удалены, выберите элемент в разделе **Резервные копии приложений в облаке** на вкладке Хранилище резервных копий и щелкните **Показать резервные копии**.

Можно выполнить поиск по имени пользователей и групп. Подстановочные символы не поддерживаются.

4. Выберите точку восстановления.
5. Последовательно выберите пункты **Восстановить** > **Весь почтовый ящик**.
6. Если в службу Кибер Бэкап Облачный добавлено несколько размещенных организаций Exchange, щелкните **Размещенная организация Exchange** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в службе Кибер Бэкап Облачный, необходимо указать целевую организацию.
7. Раздел **Восстановить в почтовый ящик** позволяет просматривать, изменять или указывать целевой почтовый ящик.

   По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана организация, которая не является исходной, необходимо указать целевой почтовый ящик.
8. Щелкните **Запуск восстановления**.
9. Выберите один из вариантов перезаписи:
   - **Перезаписывать существующие элементы**
   - **Не перезаписывать существующие элементы**
10. Щелкните **Продолжить**, чтобы подтвердить решение.

12.16.4.2 Восстановление элементов почтовых ящиков

1. Щелкните **Устройства > Размещенный Exchange**.
2. Если в службу Кибер Бэкап Облачный добавлено несколько размещенных организаций Exchange, выберите ту организацию, данные которой необходимо восстановить из резервной копии. В противном случае пропустите этот шаг.
3. Выполните одно из следующих действий:
   - Чтобы восстановить элементы с почтового ящика пользователя, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите пользователя, почтовый ящик которого изначально содержал элементы для восстановления, и щелкните **Восстановить**.

- Чтобы восстановить элементы из общего почтового ящика, разверните узел **Пользователи**, выберите **Все пользователи**, затем выберите общий почтовый ящик, который изначально содержал элементы для восстановления, и щелкните **Восстановить**.
- Чтобы восстановить элементы с почтового ящика группы, разверните узел **Группы**, выберите **Все группы**, затем выберите группу, в почтовом ящике которой изначально содержались элементы для восстановления, и щелкните **Восстановить**.
- Если пользователь, группа или общий почтовый ящик удалены, выберите элемент в разделе **Резервные копии приложений в облаке** на вкладке Хранилище резервных копий и щелкните **Показать резервные копии**.

Можно выполнить поиск по имени пользователей и групп. Подстановочные символы не поддерживаются.

4. Выберите точку восстановления.
5. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
6. Перейдите к нужной папке или используйте поиск для получения списка нужных элементов.

   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.
   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю, имени вложения 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.
7. Выберите элементы, которые необходимо восстановить. Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок 

   Кроме того, можно выполнить любое из следующих действий:
   - Чтобы просмотреть содержимое выбранного элемента, щелкните **Показать содержимое**. Чтобы скачать вложенный файл, щелкните его имя.
   - После выбора сообщения электронной почты или календаря щелкните **Отправить как сообщение электронной почты**, чтобы отправить элемент по указанному адресу электронной почты. Можно выбрать отправителя и записать текст, который будет добавлен к пересылаемому элементу.
   - Только в том случае, если вы выполнили поиск в незашифрованной резервной копии и выбрали один элемент в результатах поиска, можно щелкнуть **Показать версии**, чтобы выбрать версию элемента для восстановления. Можно выбрать любую версию в резервной копии, датированную до или после точки восстановления.
8. Нажмите кнопку **Восстановить**.
9. Если в службу Кибер Бэкап Облачный добавлено несколько размещенных организаций Exchange, щелкните **Размещенная организация Exchange** для просмотра, изменения или указания целевой организации.

   По умолчанию выбрана исходная организация. Если эта организация больше не зарегистрирована в службе Кибер Бэкап Облачный, необходимо указать целевую организацию.

10. Раздел **Восстановить в почтовый ящик** позволяет просматривать, изменять или указывать целевой почтовый ящик.

    По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует или выбрана организация, которая не является исходной, необходимо указать целевой почтовый ящик.
11. [Только при восстановлении в почтовый ящик пользователя или общий почтовый ящик] В поле **Путь** просмотрите или измените целевую папку в целевом почтовом ящике. По умолчанию выбрана папка **Восстановленные элементы**.

    Элементы почтового ящика группы всегда восстанавливаются в папку **Входящие**.
12. Щелкните **Запуск восстановления**.
13. Выберите один из вариантов перезаписи:
    - **Перезаписывать существующие элементы**
    - **Не перезаписывать существующие элементы**
14. Щелкните **Продолжить**, чтобы подтвердить решение.

12.17 Защита Oracle Database

Защита Oracle Database описана в отдельном документе, который доступен по ссылке.

Примечание
Эта функциональность доступна только в выпусках Advanced службы Кибер Бэкап Облачный.

12.18 Специальные операции с виртуальными машинами

12.18.1 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.

12.18.1.1 Примеры использования

- **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.

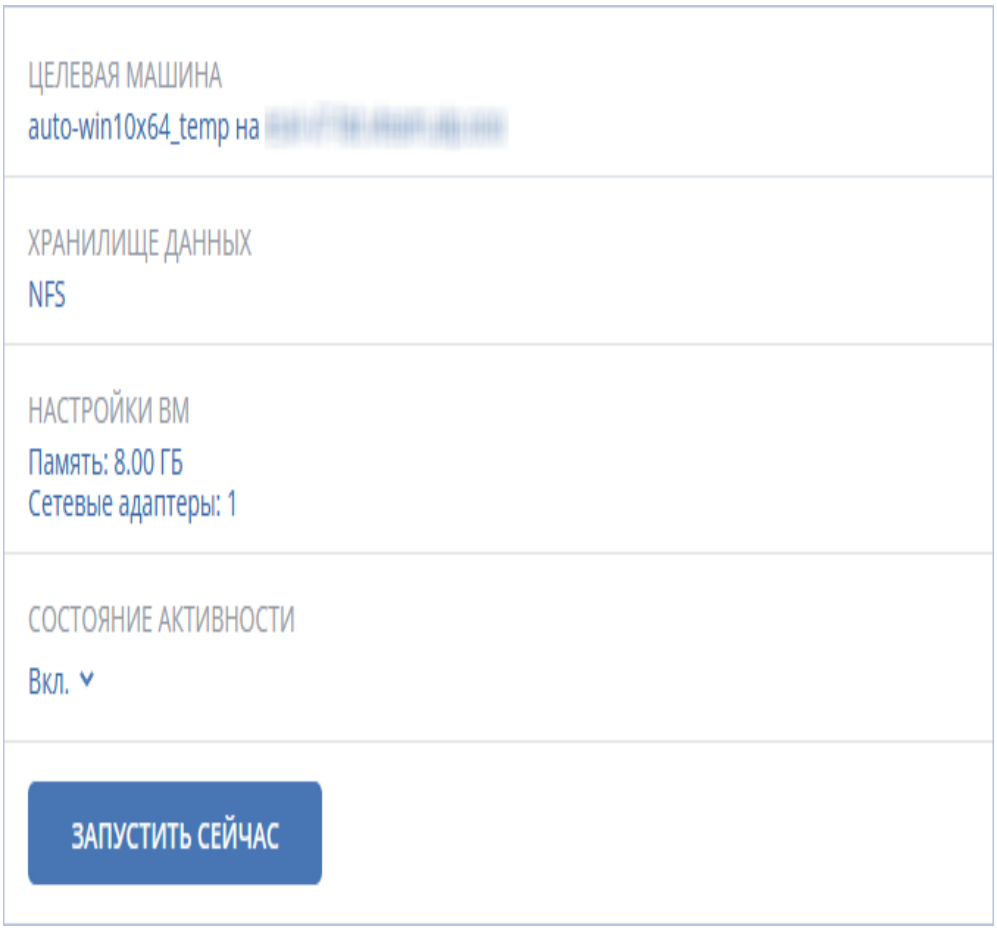
12.18.1.2 Предварительные требования

- В службе Кибер Бэкап Облачный необходимо зарегистрировать хотя бы один агент для VMware или агент для Hyper-V.
- Резервная копия может храниться в сетевой папке 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 можно также запустить из резервной копии, которая хранится в облачном хранилище данных, но в этом случае она будет работать медленнее. Причина состоит в том, что для этой операции требуется интенсивное чтение из резервной копии с произвольным доступом к данным.
- 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).

12.18.1.3 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 Хранилище резервных копий.
2. Щелкните **Запустить как ВМ**.

   Программа автоматически выберет хост и другие требуемые параметры.



3. [Необязательно] Щелкните **Целевая машина**, затем измените тип виртуальной машины (ESXi или Hyper-V), хост или имя виртуальной машины.
4. [Необязательно] Щелкните **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] Щелкните **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.
6. [Необязательно] Выберите состояние активности ВМ (**Включено**/**Выключено**).
7. Щелкните **Запустить сейчас**.

В результате этого машина появляется в веб-интерфейсе с одним из следующих значков:  или 

. Такие виртуальные машины невозможно выбрать для резервного копирования.

12.18.1.4 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 **Все устройства** выберите машину, которая запущена из резервной копии.
2. Щелкните **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.

12.18.1.5 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.

Примечание
Финализация не поддерживается для Hyper-V, который выполняется в Windows Server 2008/2008 R2 и Microsoft Hyper-V Server 2008/2008 R2, поскольку в этих версиях Hyper-V отсутствует необходимый API.

Порядок финализации машины, которая запущена из резервной копии

1. На вкладке **Все устройства** выберите машину, которая запущена из резервной копии.
2. Щелкните **Финализировать**.
3. [Необязательно] Укажите новое имя для данной машины.
4. [Необязательно] Измените режим распределения ресурсов диска. По умолчанию задана

настройка **Экономное**.

5. Щелкните **Финализировать**.

Имя машины сразу же меняется. Ход выполнения восстановления показан на вкладке **Действия**. После выполнения восстановления значок машины меняется на значок постоянной виртуальной машины.

Полезная информация о финализации

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.

Финализация машин, запушенных из резервных копий в облаке

Из-за интенсивного доступа к данным в резервных копиях скорость финализации сильно зависит от пропускной способности подключения между хранилищем резервных копий и агентом. Для резервных копий, расположенных в облаке, финализация будет выполняться медленнее, чем для локальных резервных копий. При медленном или нестабильном подключении к Интернету финализация машины, которая выполняется из резервной копии в облаке, может завершиться сбоем. Если вы планируете выполнять финализацию, рекомендуем запускать виртуальные машины с локальных резервных копий (при наличии такой возможности).

12.18.2 Работа в VMware vSphere

В этом разделе описаны операции, характерные для среды VMware vSphere.

12.18.2.1 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
  Переход к реплике – это 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:

- Отказоустойчивые машины, которые выполняются в ESXi 5.5 и более ранних версий.
- 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. Щелкните **Репликация**.
   В программе отображается новый шаблон плана репликации.
3. [Необязательно] Чтобы изменить имя плана репликации, щелкните имя по умолчанию.
4. Щелкните **Целевая машина** и выполните указанные ниже действия:
   a. Выберите, создавать ли новую или использовать уже существующую реплику исходной машины.
   b. Выберите хост ESXi и укажите имя новой реплики или выберите существующую реплику.
      Новая реплика будет иметь имя по умолчанию **[Имя первоначальной машины]_replica**.
   c. Нажмите кнопку **OK**.
5. [Только при репликации на новую машину] Щелкните **Хранилище данных** и выберите хранилище данных для виртуальной машины.
6. [Необязательно] Щелкните **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] Щелкните значок шестерни, чтобы изменить параметры репликации.
8. Нажмите кнопку **Применить**.
9. [Необязательно] Чтобы запустить план вручную, щелкните **Запустить сейчас** на панели плана.

В результате выполнения плана репликации реплика виртуальной машины появляется в списке **Все устройства** с указанным ниже значком: 

Тестирование реплики

Порядок подготовки реплики к тестированию

1. Выберите реплику для тестирования.
2. Щелкните **Тестировать реплику**.
3. Щелкните **Начать тестирование**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика не будут подключена к сети.
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. Щелкните **Тестировать реплику**.
3. Щелкните **Остановить тестирование**.
4. Подтвердите операцию.

Переход к реплике

Переход с машины к реплике

1. Выберите реплику, к которой необходимо перейти.
2. Щелкните **Действия с репликой**.
3. Щелкните **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. Щелкните **Действия с репликой**.
3. Щелкните **Остановить переход к реплике**.
4. Подтвердите операцию.

Выполнение окончательного перехода на реплику

Порядок выполнения окончательного перехода на реплику

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Окончательный переход на реплику**.
4. [Необязательно] Измените имя виртуальной машины.
5. [Необязательно] Установите флажок **Остановить исходную виртуальную машину**.
6. Нажмите кнопку **Запустить**.

Возврат из реплики

Порядок выполнения возврата из реплики

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Возврат из реплики**.

   Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.
4. [Необязательно] Щелкните **Целевая машина** и выполните следующие действия:
   a. Выберите новую или существующую машину для возврата из реплики.
   b. Выберите хост ESXi и укажите имя новой машины или выберите существующую машину.
   c. Нажмите кнопку **OK**.
5. [Необязательно] При возврате из реплики на новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных**, чтобы выбрать хранилище данных для виртуальной машины.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.

6. [Необязательно] Щелкните **Параметры восстановления**, чтобы изменить параметры возврата из реплики.
7. Щелкните **Запуск восстановления**.
8. Подтвердите операцию.

Параметры репликации

Чтобы изменить параметры репликации, щелкните значок шестерни рядом с именем плана репликации и нажмите кнопку **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**.

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, щелкните **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.

Внимание
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.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к исходному хосту vCenter\ESXi.
   c. Выберите только что созданную реплику в списке.
   d. Щелкните **Файл** > **Экспорт** > **Экспорт шаблона OVF**.
   e. В поле **Папка** укажите папку на внешнем жестком диске.
   f. Нажмите кнопку **OK**.
5. Перенесите жесткий диск в удаленное расположение.
6. Импортируйте реплику на целевой хост ESXi.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к целевому хосту vCenter\ESXi.
   c. Щелкните **Файл** > **Развернуть шаблон OVF**.
   d. В поле **Развернуть из файла или URL-адреса** укажите шаблон, экспортированный на шаге 4.
   e. Завершите процедуру импорта.

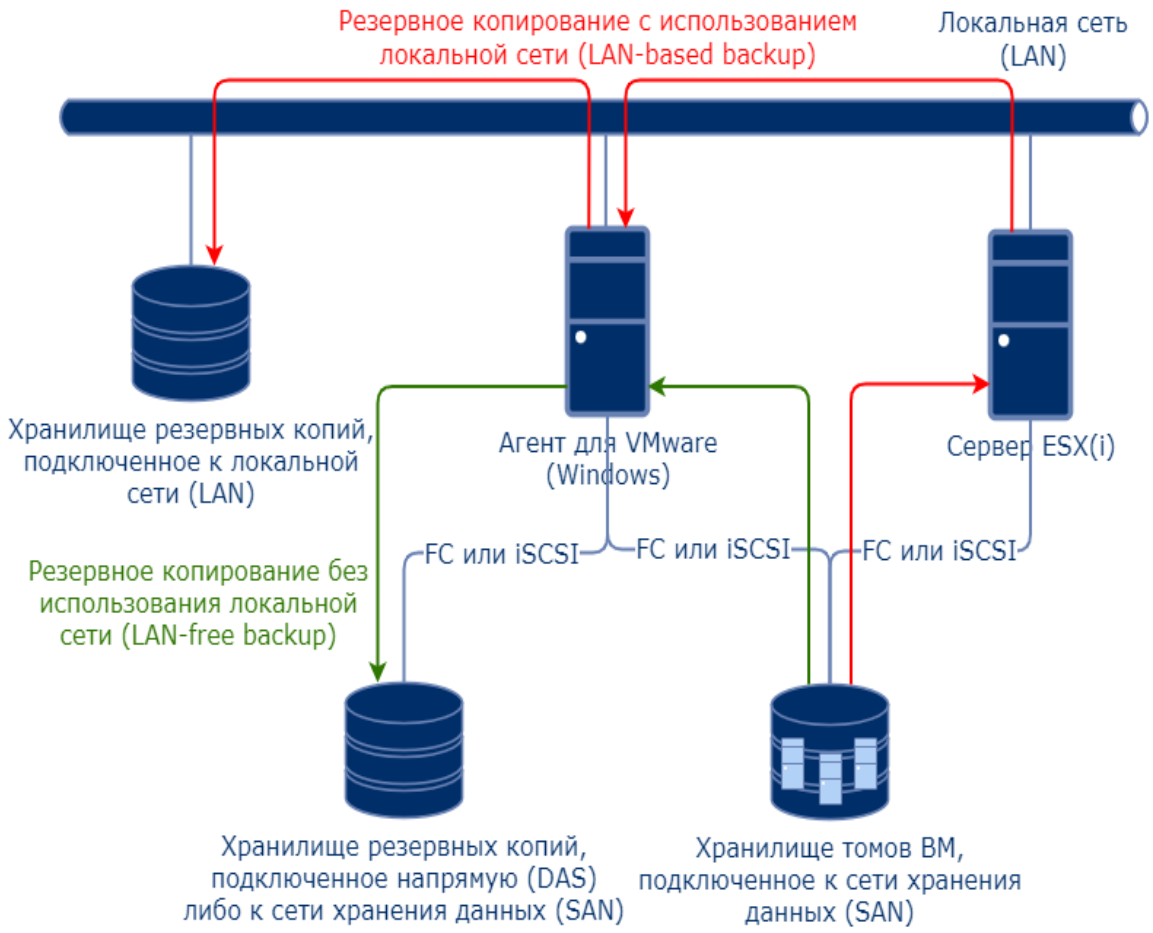
7. Измените план репликации, созданный на шаге 2. В поле **Целевая машина** выберите **Существующая реплика**, а затем выберите импортированную реплику.

В результате программа продолжит обновлять реплику. Все репликации будут инкрементными.

12.18.2.2 Агент для VMware – 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. 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 появится как «автономный» диск в разделе **Управление дисками**. Если Windows инициализирует логическое устройство, оно может быть повреждено и стать нечитаемым для VMware vSphere.

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 6.0 и более поздней версии 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: На экране отобразится Перевод в автономное состояние всех ресурсов**.
3. Если для политики SAN задано другое значение:
   a. Введите san policy=offlineall.
   b. Нажмите клавишу **Ввод**.
   c. Чтобы проверить правильность применения настройки, выполните шаг 2.
   d. Перезапустите машину.

Настройка инициатора iSCSI

1. Последовательно выберите пункты **Панель управления** > **Администрирование** > **Инициатор iSCSI**.

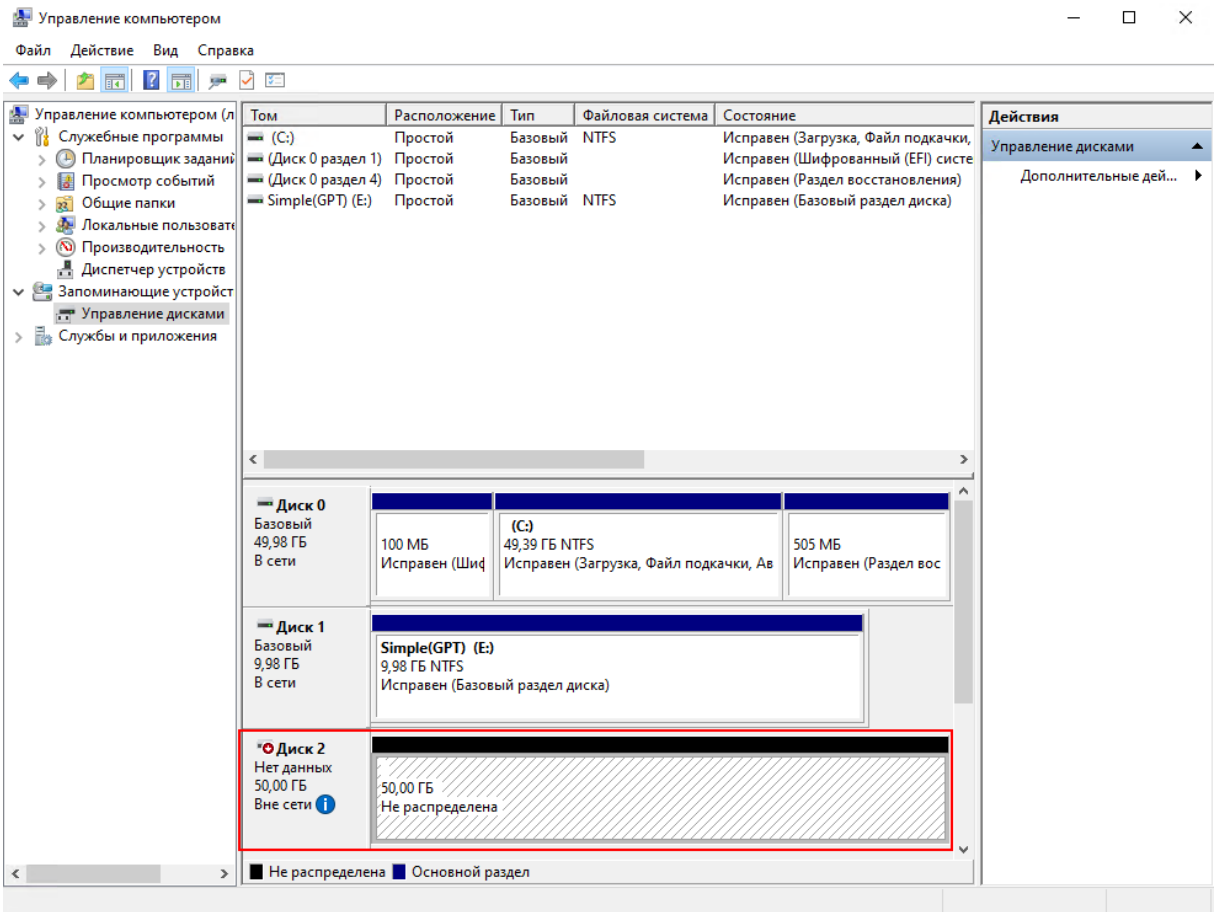
Примечание

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 щелкните **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 **OK**.

Готовое логическое устройство SAN должно появится в разделе **Управление дисками**, как показано на снимке экрана ниже.



12.18.2.3 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 щелкните 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 назначения 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:**.

12.18.2.4 Привязка виртуальной машины

В этом разделе показано, как служба Кибер Бэкап Облачный 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 служба Кибер Бэкап Облачный 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. Служба Кибер Бэкап Облачный назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится.

Если агент удаляется из службы Кибер Бэкап Облачный, 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 **Все устройства**;
- 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. Щелкните **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 волоконный канал, тогда как резервные копии других машин создаются виртуальными устройствами.
- 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.

12.18.2.5 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.

12.18.2.6 Управление средами виртуализации

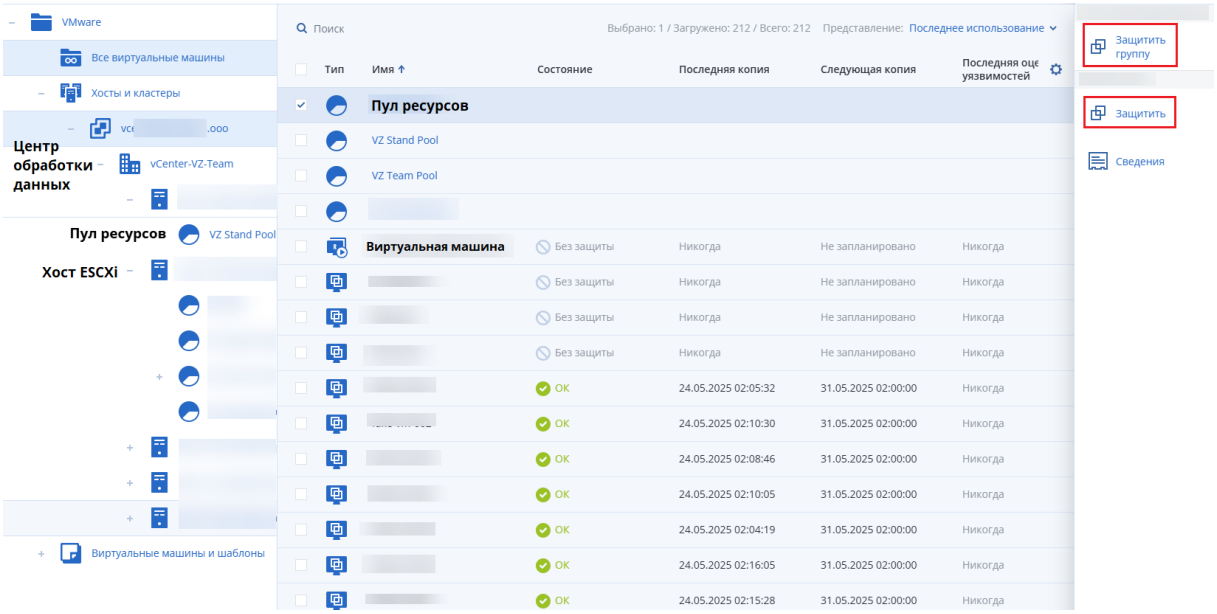
Можно просмотреть среды vSphere и Hyper-V в их собственном представлении. После установки и регистрации соответствующего агента в разделе **Устройства** появляются вкладки **VMware** или **Hyper-V**.

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, щелкнув **Защитить**, или машин родительской группы, в которую входит выбранная группа, щелкнув **Защитить группу**.

Например, вы выбрали кластер, а затем – пул ресурсов в нем. Если щелкнуть **Защитить**, будет создана резервная копия для всех виртуальных машин в выбранном пуле ресурсов. Если щелкнуть **Защитить группу**, будет создана резервная копия для всех виртуальных машин в кластере.



Вкладка **VMware** позволяет изменить учетные данные доступа для 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 щелкните **OK**.

12.18.2.7 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**

12.18.2.8 Агент для VMware: необходимые привилегии

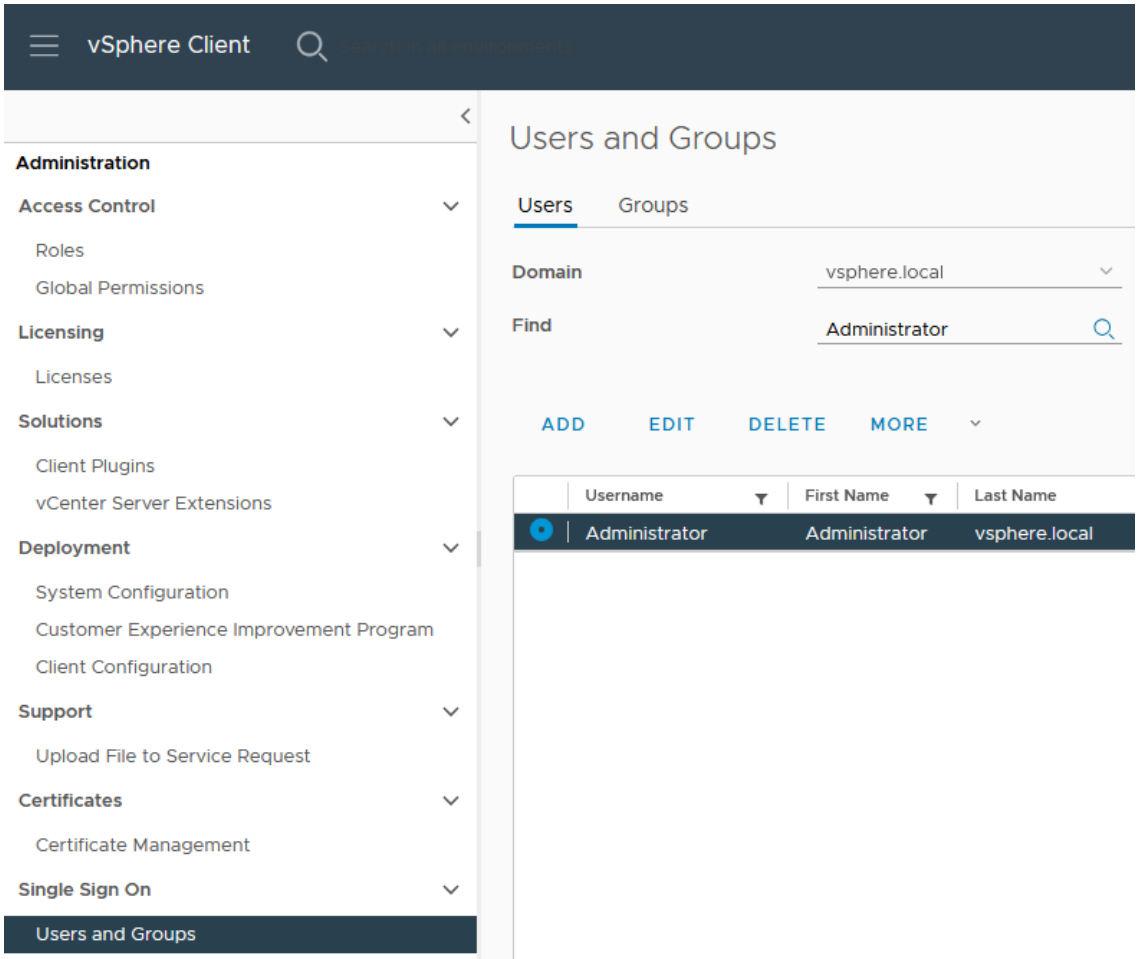
В этом разделе описаны права, необходимые для операций с виртуальными машинами ESXi, а также для развертывания виртуальных устройств.

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».

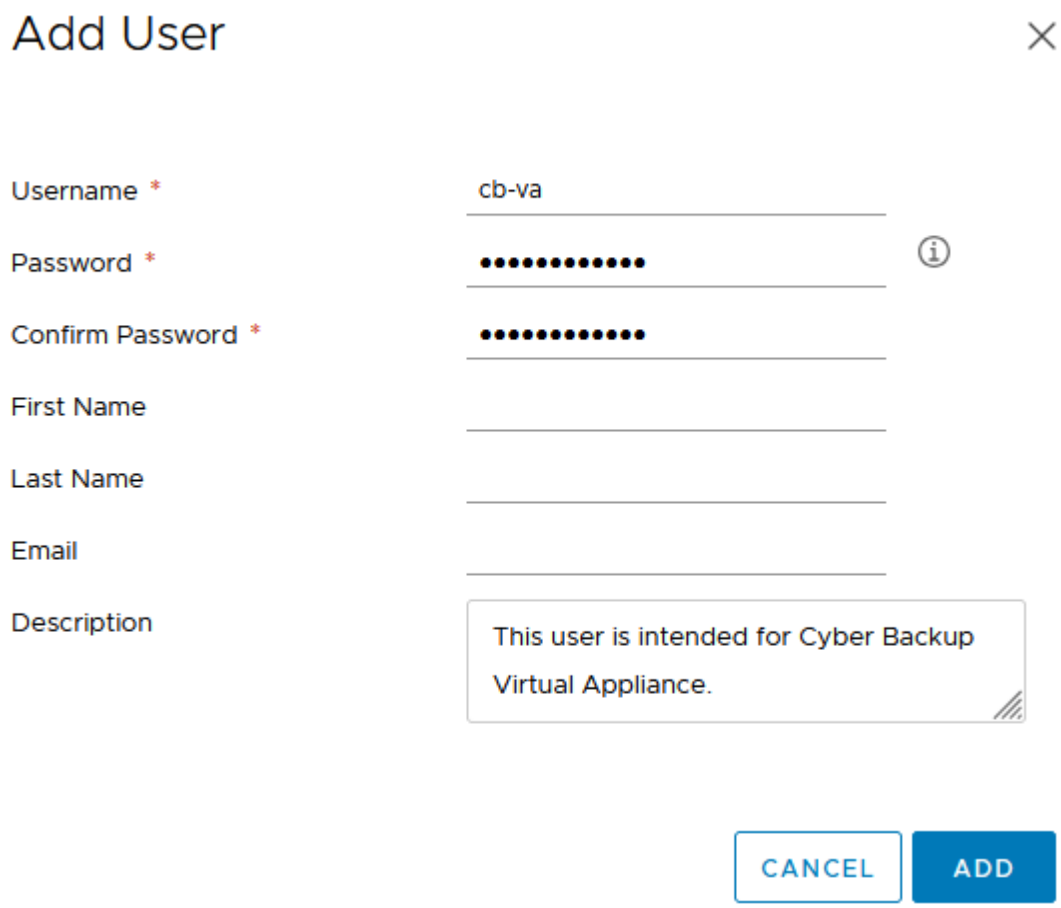
Порядок подготовки пользователя vSphere с необходимыми правами:

1. Подключитесь к vCenter с помощью веб-клиента vSphere, использовав учетные данные администратора.
2. Создайте пользователя:
   a. Перейдите в раздел **Administration** > **Single Sign On** > **Users and Groups** (Администрирование > Единый вход > Пользователи и группы), выберите вкладку **Users** (Пользователи) и нажмите **ADD** (ДОБАВИТЬ).

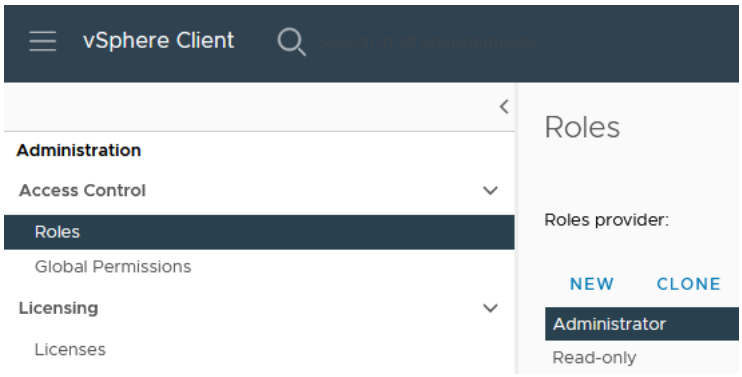


   b. В окне **Add User** (Добавление пользователя) укажите имя пользователя и пароль, затем

нажмите **ADD** (ДОБАВИТЬ).



3. Создайте роль:
   a. Перейдите в раздел **Administration** > **Access Control** > **Roles** (Администрирование > Контроль доступа > Роли) и нажмите **NEW** (НОВАЯ).



   b. 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),

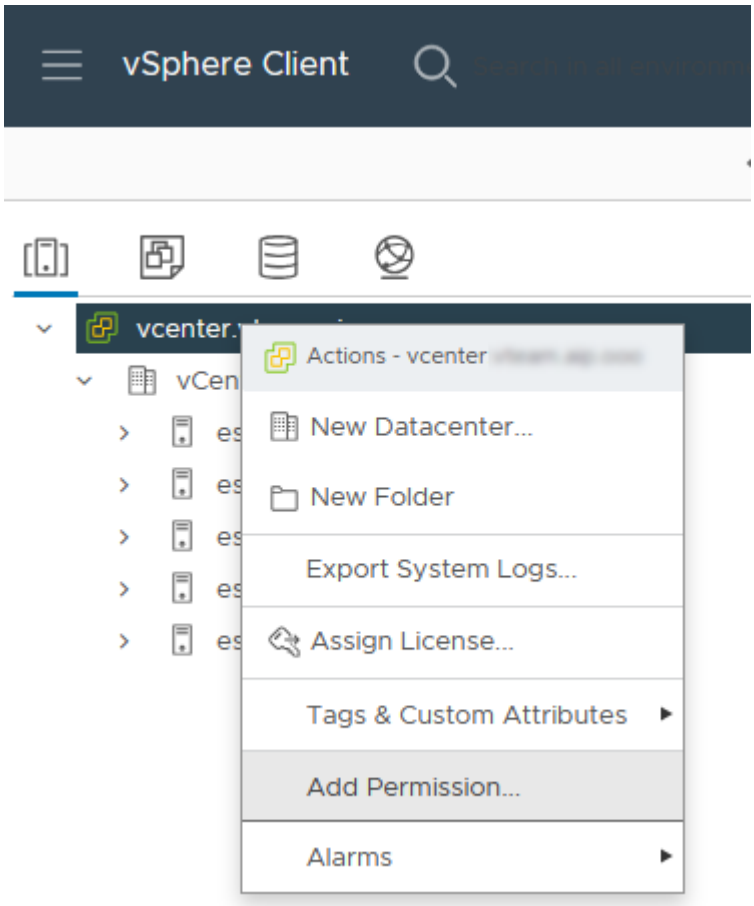
- **Datastore** > **Browse datastore** (Хранилище данных > Обзор хранилища данных),
- **Datastore** > **Configure datastore** (Хранилище данных > Настройка хранилища данных),
- **Datastore** > **Low level file operations** (Хранилище данных > Низкоуровневые файловые операции),
- **Global** > **Disable 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** > **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 (доступно начиная с vSphere 5.1)),

- **Virtual machine** > **Interaction** > **Power off** (Виртуальная машина > Взаимодействие > Отключение),
- **Virtual machine** > **Interaction** > **Power on** (Виртуальная машина > Взаимодействие > Включение),
- **Virtual machine** > **Interaction** > **Acquire guest control ticket** (Виртуальная машина > Взаимодействие > Получение контрольного билета гостя (для vSphere 4.1 и 5.0)),
- **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).

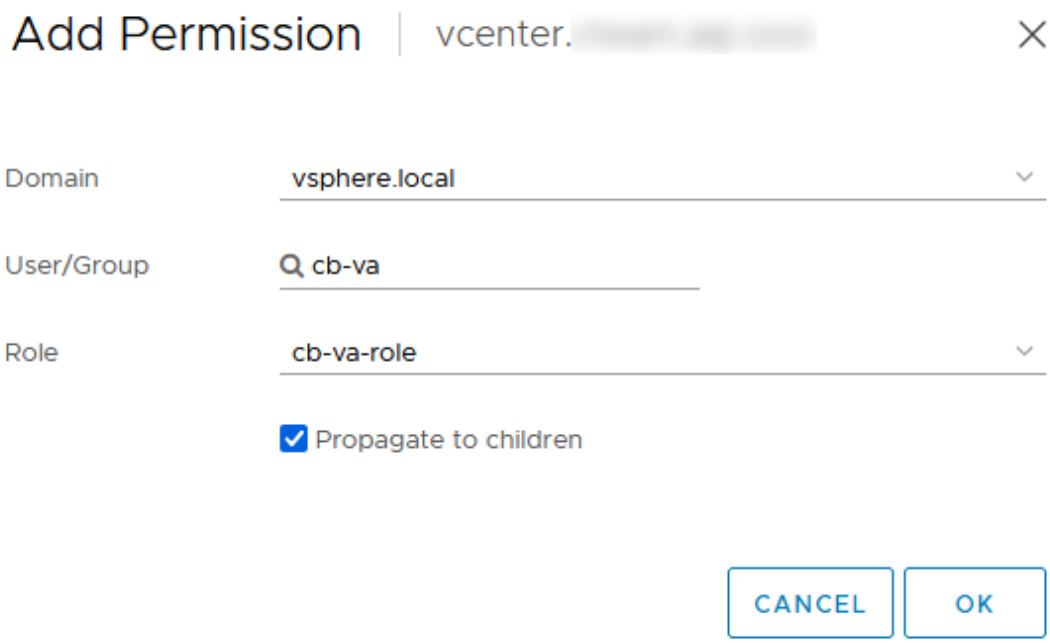
c. Нажмите **CREATE** (СОЗДАТЬ) для завершения создания роли.

4. Назначьте пользователю роль на уровне vCenter:
   a. Перейдите в раздел **Inventory** > **Hosts and Clusters** (Инвентарь > Хосты и кластеры) и щелкните правой кнопкой мыши vCenter.

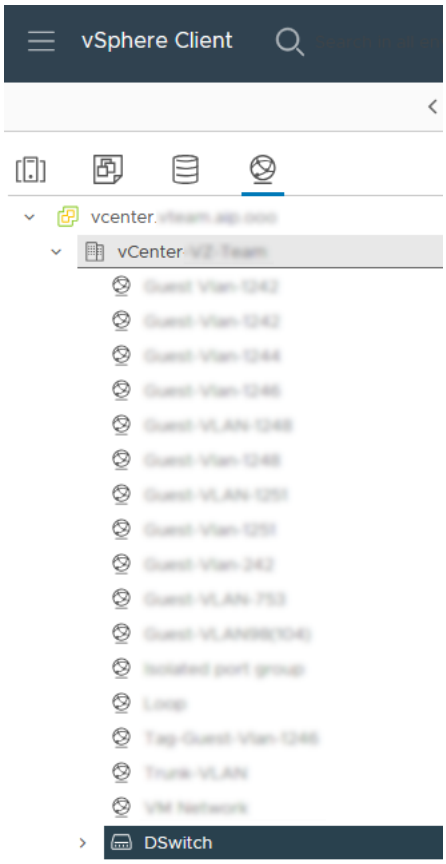


b. В меню выберите **Add Permission** (Добавить право).

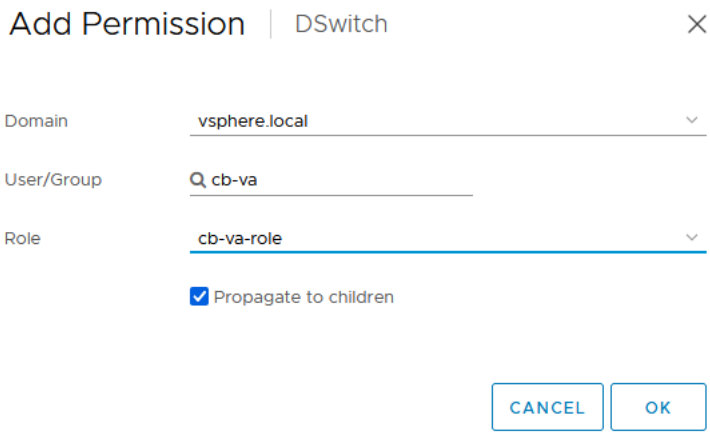
c. В окне **Add Permission** (Добавить право) выберите пользователя и роль, которые были созданы на предыдущих шагах, затем установите флажок **Propagate to children** (Распространить на дочерние элементы) и нажмите **OK**.



5. Назначьте пользователю роль на уровне распределенного виртуального коммутатора (dvSwitch):
   a. Перейдите в раздел **Inventory** > **Networking** (Инвентарь > Сеть) и щелкните правой кнопкой мыши распределенный виртуальный коммутатор, который будет использоваться при восстановлении в новую ВМ, затем щелкните **Add Permission** (Добавить право).



b. 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)	+*				
	Direct Access (Прямой доступ)	+*				
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)	+	+	+		

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
	Manage custom attributes (Управление настраиваемыми атрибутами)	+	+	+		
	Set custom attribute (Задание настраиваемых атрибутов)	+	+	+		
Host > **Configuration** (Хост > Конфигурация)	**VM autostart configuration** (Конфигурация автозапуска ВМ)					+
	Storage partition configuration (Конфигурация раздела хранения данных)				+	
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)		+	+	+	+

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
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)	+	+		+	
	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)	+		+		

Объект	Привилегия	Операция				
		Резервное копирование ВМ	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
	Change memory (Управление ОЗУ)		+			
	Remove disk (Удаление диска)	+	+	+	+	
	Rename (Переименование)		+			
	Set annotation (Настройка аннотации)				+	
	Change settings (Изменение настроек)		+	+	+	
Virtual machine > **Guest Operations** (Виртуальная машина > Гостевые операции)	**Guest Operation Program Execution** (Выполнение программы гостевой операции)	+**				+
	Guest Operation Queries (Запросы гостевой операции)	+**				+
	Guest Operation Modifications (Изменения гостевых операций)	+**				
Virtual machine >	**Acquire guest control ticket**				+	+

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
Interaction (Виртуальная машина > Взаимодействие)	(Получение контрольного билета гостя (для vSphere 4.1 и 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))				+	+
	Power off (Отключение)			+	+	+
	Power on (Включение)		+	+	+	+
Virtual machine >	**Create from existing** (Создание из		+	+	+	

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
Edit Inventory (Виртуальная машина > Редактирование инвентаря)	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**	**Create snapshot** (Создание моментального снимка)	+		+	+	+

Объект	Привилегия	Операция				
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии	Развертывание виртуального устройства
(Виртуальная машина > Управление моментальными снимками)						
	Remove snapshot (Удаление моментального снимка)	+		+	+	+
vApp	**Add virtual machine** (Добавление ВМ)				+	
	Import (Импорт)					+

* Эта привилегия требуется только для резервного копирования зашифрованных машин.

** Эта привилегия требуется только для резервных копий с поддержкой приложений.

12.18.3 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.

   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 в службе Кибер Бэкап Облачный.

12.18.3.1 Высокая доступность восстановленной машины

При восстановлении резервных копий дисков на *существующей* виртуальной машине Hyper-V свойство высокой доступности данной машины остается без изменений.

В случае восстановления резервных копий дисков на *новой* виртуальной машине Hyper-V целевая виртуальная машина не обладает свойством высокой доступности. 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**.

12.18.4 Ограничение общего количества виртуальных машин, для которых одновременно выполняется резервное копирование

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 агент для VMware или агент для Hyper-V может одновременно создавать резервные копии.

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:

```
Редактор реестра Windows версии 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLi
mits]
"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.
   a. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
   b. Нажмите кнопку **OK**.
   c. Выполните следующие команды:

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

Установка ограничения на общее количество виртуальных машин, резервные копии которых может создавать агент для VMware (виртуальное устройство)

1. Чтобы запустить командную оболочку, в пользовательском интерфейсе виртуального устройства нажмите клавиши CTRL+SHIFT+F2.
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. Чтобы перезапустить агент, выполните команду reboot.

12.18.5 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 архивированной машины	Доступные места восстановления				
	Физическая машина	Виртуальная машина ESXi	Виртуальная машина Hyper-V	Виртуальная машина RHV/oVirt	Виртуальная машина OpenStack (VK Cloud)1
Физическая машина	+	+	+	+	+
Виртуальная машина VMware ESXi	+	+	+	+	+
Виртуальная машина Hyper-V	+	+	+	+	+
Виртуальная машина Red Hat Virtualization/oVirt	+	+	+	+	+
Виртуальная машина OpenStack (VK Cloud)	-	+	-	+	+

1 Платформа OpenStack наряду с KVM использует драйверы VirtIO и VirtIO SCSI для сети и дисков. Для миграции виртуальной машины на ОС Windows или Linux на OpenStack 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. Подготовленная машина может не запускаться на платформе 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.

Инструкции о выполнении миграции см. в следующих разделах:

- Миграция систем с физической машины на виртуальную (P2V): миграция систем с физической машины на виртуальную
- Миграция систем с виртуальной машины на виртуальную (V2V): Виртуальная машина
- Миграция систем с виртуальной машины на физическую (V2P): Виртуальная машина или Восстановление дисков с помощью загрузочного носителя

Хотя можно выполнить миграцию V2P в веб-интерфейсе, в определенных случаях рекомендуется использовать загрузочный носитель. Иногда вы можете создать носитель для миграции в ESXi или Hyper-V.

Носитель позволяет выполнить следующие действия:

- Выполнить миграцию P2V, миграцию V2P или 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.

13 Вкладка «Планы»

Примечание
Эта функциональность доступна только в выпусках Advanced службы Кибер Бэкап Облачный.

Планами защиты и прочими планами можно управлять на вкладке **Планы**.

Каждый раздел вкладки **Планы** содержит планы конкретного типа. Доступны следующие разделы:

- Защита;
- Репликация ВМ.

13.1 План защиты

Порядок создания плана резервного копирования

1. В консоли службы последовательно выберите пункты **Планы** > **Защита**.
2. Нажмите **Создать план**.
3. Выберите машины, для которых нужно обеспечить защиту.
4. Щелкните **Защитить**. Отобразится план защиты с настройками по умолчанию.
5. [Необязательно] Для изменения имени плана защиты щелкните значок карандаша рядом с именем.
6. [Необязательно] Для включения или отключения модуля плана щелкните переключатель рядом с именем модуля.
7. [Необязательно] Для настройки параметров модуля, щелкните соответствующий раздел плана защиты.
8. Щелкните **Добавить устройства** для выбора машин, к которым необходимо применить план.
9. После этого щелкните **Создать**.

В результате этого выбранные устройства будут защищены планом защиты.

С планом защиты можно выполнить указанные ниже операции.

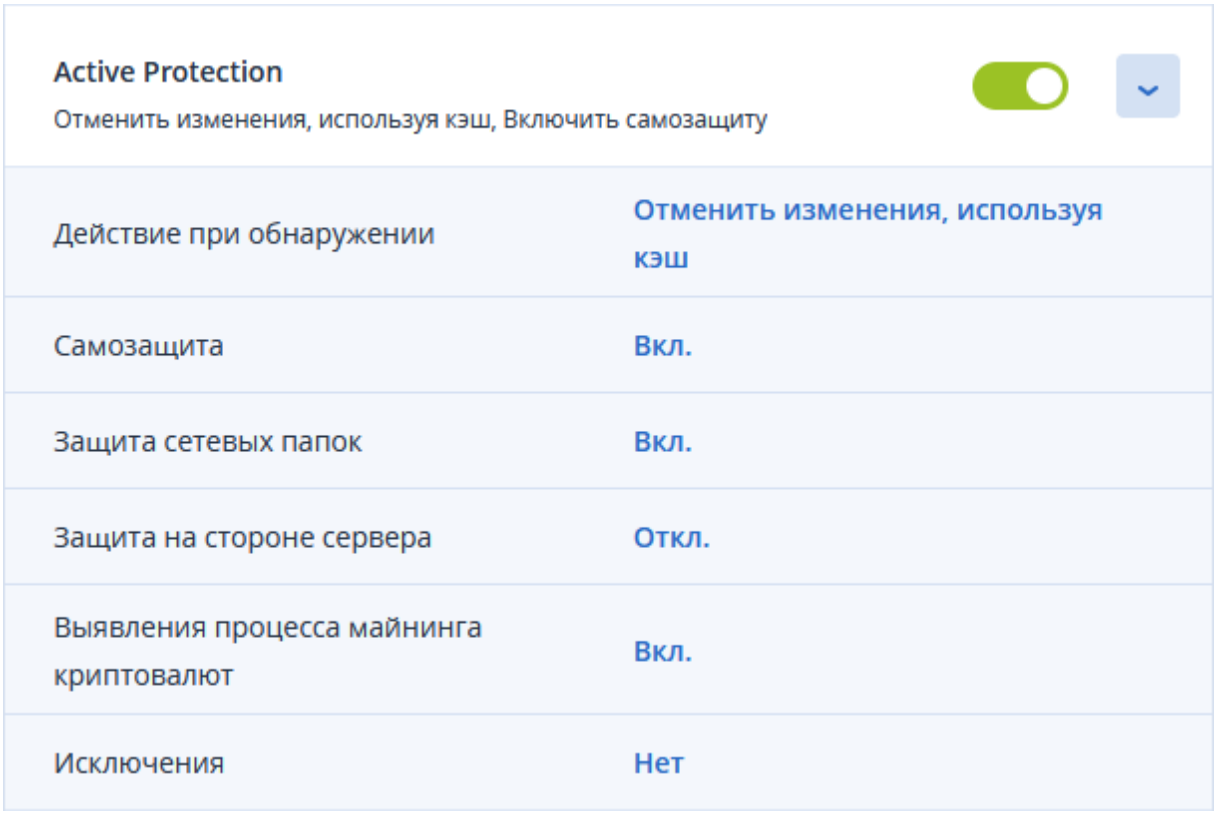
- Создавать, просматривать, изменять, клонировать, отключать, включать и удалять план защиты.
- Просматривать действия, относящиеся к каждому плану защиты.
- Просматривать оповещения, относящиеся к каждому плану защиты.
- Экспортировать план в файл.
- Импортировать ранее экспортированный план.

14 Active Protection (Активная защита)

Служба Active Protection обеспечивает защиту компьютера от вредоносных программ, таких как вирусы-вымогатели и программы майнинга криптовалют. Вирусы-вымогатели шифруют файлы и требуют платы от пользователя за ключ расшифровки. Программы майнинга криптовалют запускают математические вычисления в фоновом режиме, тем самым похищая вычислительную мощность и сетевой трафик.

Active Protection – это отдельный модуль в плане защиты. Этот модуль имеет следующие настройки:

- Действие при обнаружении;
- Самозащита;
- Защита сетевых папок;
- Защита на стороне сервера;
- Выявление процесса майнинга криптовалют;
- Исключения.



Служба Active Protection доступна для машин со следующими операционными системами:

- Windows Server 2012 R2 (64-разрядные версии) – все выпуски;
- Windows Server 2016 - 2022 (64-разрядные версии) – все выпуски, кроме Nano Server;

- Windows 10 (64-разрядные версии) — выпуски Home, Pro, Education, Enterprise, IoT Enterprise и LTSC (прежнее название LTSB);
- Windows 11 (64-разрядные версии) — все выпуски.

На машине должен быть установлен агент для Windows.

Для более подробного ознакомления с возможностями Active Protection см. "Настройка модуля Active Protection" (стр. 307).

Для ознакомления с возможностями Active Protection для Linux см. "Active Protection для Linux" (стр. 310).

Примечание
Набор настроек Active Protection для ОС Windows включает в себя настройки для ОС Linux. Список отображаемых при создании плана настроек Active Protection зависит от условий создания плана. Если план создается для одной машины с ОС Linux или Windows, то отображаются настройки для ОС Linux или, соответственно, Windows. Если план создается для нескольких машин с ОС Linux и Windows, то отображаются настройки для ОС Linux. Если план создается для статической или динамической группы машин, то отображаются настройки для ОС Windows.

14.1 Настройка модуля Active Protection

14.1.1 Принцип работы

Active Protection отслеживает процессы, запущенные на защищенном компьютере. Когда процесс сторонней программы пытается шифровать файлы или добывать криптовалюту, Active Protection создает оповещение и выполняет дополнительные действия, если они указаны в настройках.

Вдобавок 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 активной защите обнаруживать новые вредоносные программы по их типичному поведению.

Значение по умолчанию: **Выкл** (выключено).

14.1.2 Действие при обнаружении

В поле **Действие при обнаружении** выберите действие, которое будет выполняться при обнаружении подозрительной активности и затем нажмите **Готово**.

Вы можете выбрать один из следующих вариантов:

- **Только уведомить**

  Программа создаст оповещение о процессе.
- **Остановить процесс**

  Программа создаст оповещение о процессе и остановит процесс.
- **Отменить изменения, используя кэш**

  Программа создаст оповещение, остановит процесс и отменит изменения в файле, используя служебный кэш.

Значение по умолчанию: **Отменить изменения, используя кэш**.

14.1.3 Защита сетевых папок

Параметр **Защитите сетевые папки, назначенные как локальные диски** позволяет защитить от локальных вредоносных процессов сетевые папки, назначенные как локальные диски.

Этот параметр применяется к папкам, к которым предоставляется общий доступ по протоколам SMB или NFS.

Если файл изначально был расположен на подключенном диске, он не может быть сохранен в исходное местоположение при извлечении из кэша с помощью действия **Отменить изменения, используя кэш**. Вместо этого он будет сохранен в папку, указанную в настройках этой опции. Папка по умолчанию:

```
C:\ProgramData\Acronis\Restored Network Files
```

Если эта папка не существует, она будет создана. Если вы хотите изменить этот путь, укажите другую локальную папку. Сетевые папки, включая папки на подключенных дисках, не поддерживаются.

Значение по умолчанию: **Вкл** (включено).

14.1.4 Защита на стороне сервера (внешняя защита сетевых папок)

Этот параметр определяет, будут ли защищены от вредоносных программ сетевые папки, к которым вы предоставляете общий доступ, от внешних входящих подключений с других серверов в сети, которые потенциально могут представлять угрозы.

Значение по умолчанию: **Выкл** (выключено).

14.1.4.1 Настройка доверенных и заблокированных подключений

На вкладке **Доверенные** вы можете указать соединения, которым разрешено изменять любые данные. Необходимо указать имя пользователя и IP-адрес.

На вкладке **Заблокировано** вы можете указать соединения, которые не смогут изменять никакие данные. Необходимо указать имя пользователя и IP-адрес.

14.1.5 Самозащита

Параметр **Самозащита** предотвращает несанкционированные изменения в собственных процессах программного обеспечения, записях реестра, исполняемых и конфигурационных файлах и резервных копиях, расположенных в локальных папках. Мы не рекомендуем отключать эту функцию.

Значение по умолчанию: **Вкл** (включено).

14.1.5.1 Разрешить процессам изменять резервные копии

Параметр **Разрешить определенным процессам изменять резервные копии** можно задействовать, когда включена **Самозащита**.

Эта возможность относится к файлам, которые имеют расширения .tibx, .tib, .tia и расположены в локальных папках.

В настройках параметра можно указать процессы, которым разрешено изменять файлы резервных копий, даже если эти файлы защищены системой самозащиты. Это полезно, например, если вы удаляете файлы резервных копий или перемещаете их в другое место с помощью скрипта.

Если параметр отключен, 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.

Если эта функция включена, вы можете разрешить другим процессам изменять резервные копии. Укажите полный путь к исполняемому файлу процесса, начиная с буквы диска.

Значение по умолчанию: **Выключено**.

14.1.6 Выявление процессов майнинга криптовалют

Включение этого параметра позволяет обнаруживать вредоносное программное обеспечение для майнинга криптовалют.

Вредоносные программы для майнинга снижают производительность полезных приложений, увеличивают потребление электроэнергии, могут привести к сбоям системы и даже повреждению оборудования. Мы рекомендуем вам добавить вредоносные программы для майнинга в список вредоносных процессов, чтобы предотвратить их запуск.

Значение по умолчанию: **Вкл** (включено).

14.1.6.1 Настройки выявления процессов майнинга криптовалют

Выберите действие, которое программа будет выполнять при обнаружении активности майнинга криптовалют, а затем нажмите кнопку **Готово**. Вы можете выбрать один из следующих вариантов:

- **Только уведомить**

  Программа создает предупреждение о подозрительном процессе.
- **Остановить процесс**

  Программа создает предупреждение и останавливает подозрительный процесс.

Значение по умолчанию: **Остановить процесс**.

14.1.7 Исключения

Чтобы свести к минимуму ресурсы, используемые для поведенческого анализа, и исключить так называемые ложные срабатывания, когда доверенная программа рассматривается как программа-вымогатель, вы можете задать следующие настройки:

- На вкладке **Доверенные** вы можете указать:
  - Процессы, которые никогда не будут рассматриваться как вредоносные программы. Процессы, подписанные корпорацией Майкрософт, всегда являются надежными.
  - Папки, в которых не будут отслеживаться изменения файлов.
- На вкладке **Заблокировано** вы можете указать процессы, которые всегда будут заблокированы. Эти процессы не смогут запуститься до тех пор, пока на компьютере включен модуль Active Protection.

  Укажите полный путь к исполняемому файлу процесса, начиная с буквы диска. Например:

  ```
  C:\Windows\Temp\er76s7sdkh.exe
  ```

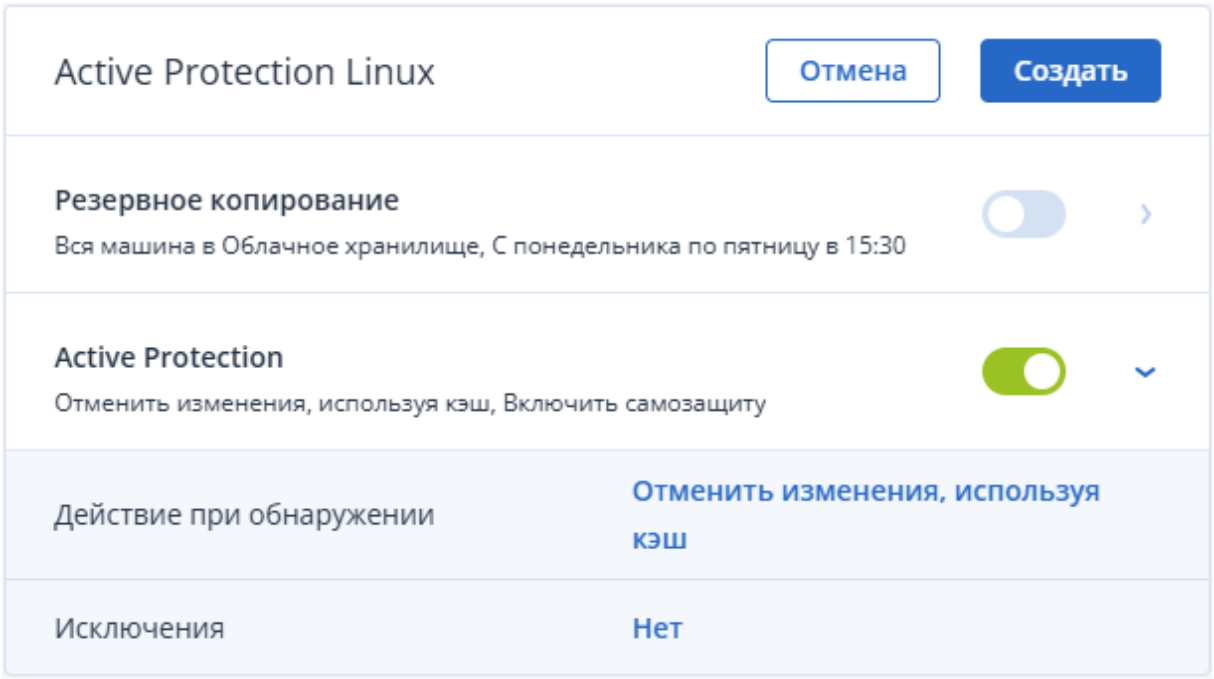
Значение по умолчанию: **Нет** (по умолчанию исключения не определены).

14.2 Active Protection для Linux

Служба Active Protection для Linux обеспечивает защиту компьютера под управлением Linux от вредоносных программ и позволяет настроить действия программы.

Active Protection – это отдельный модуль в плане защиты. Этот модуль имеет следующие настройки:

- Действие при обнаружении;
- Исключения.



Служба Active Protection доступна для машин Linux с версией ядра от 3.10 до 6.14, включая следующие дистрибутивы:

- Astra Linux Special Edition 1.6 – 1.7;
- Альт 8 СП;
- РОСА «КОБАЛЬТ» 7.9;
- Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS, 24.04 LTS;
- Debian 10, 11, 12;
- CentOS 7.x, 8.0, 8.1, 8.2, 8.3;
- AlterOS 7.5;
- ОСнова 2.7 – 2.10.

На машине должен быть установлен агент для Linux.

Требования и ограничения:

- 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 AstraLinux 1.7.x с ядром версии 6.1.90, а также ОС AstraLinux 1.8.x с ядрами версий 6.1.90, 6.6.28.
- Не поддерживается работа модуля в ОС Debian, Ubuntu, AstraLinux с защищенными (hardened) ядрами.

Для более подробного ознакомления с возможностями Active Protection см. "Настройка модуля Active Protection" (стр. 307).

15 Защита CommuniGate Pro

С помощью Кибер Бэкап Облачный можно выполнять резервное копирование данных CommuniGate Pro. Для резервного копирования понадобится Кибер Бэкап Облачный 25.07 или новее с лицензией для почтовых ящиков.

Для выполнения резервного копирования требуется установка агента Кибер Бэкап Облачный для операционной системы, которую вы используете (агент Windows или агент Linux), а также агента CommuniGate Pro.

15.1 Возможности

15.1.1 Резервное копирование

Кибер Бэкап Облачный обеспечивает:

- автоматическую и ручную синхронизацию ресурсов;
- резервное копирование данных;
- резервное копирование по расписанию;
- поддержку многоуровневого резервного копирования;
- перезапись данных хранилища по выбору;
- настраиваемые правила очистки хранилища.

15.1.2 Восстановление

Из резервной копии можно восстановить следующие элементы:

- почтовые ящики, включая папки и вложения;
- контакты;
- календари;
- заметки;
- задачи;
- настройки учетной записи.

Восстановление на новый хост возможно в случае, если на нем заранее создан домен с исходным именем. Восстановление в домен с новым именем невозможно.

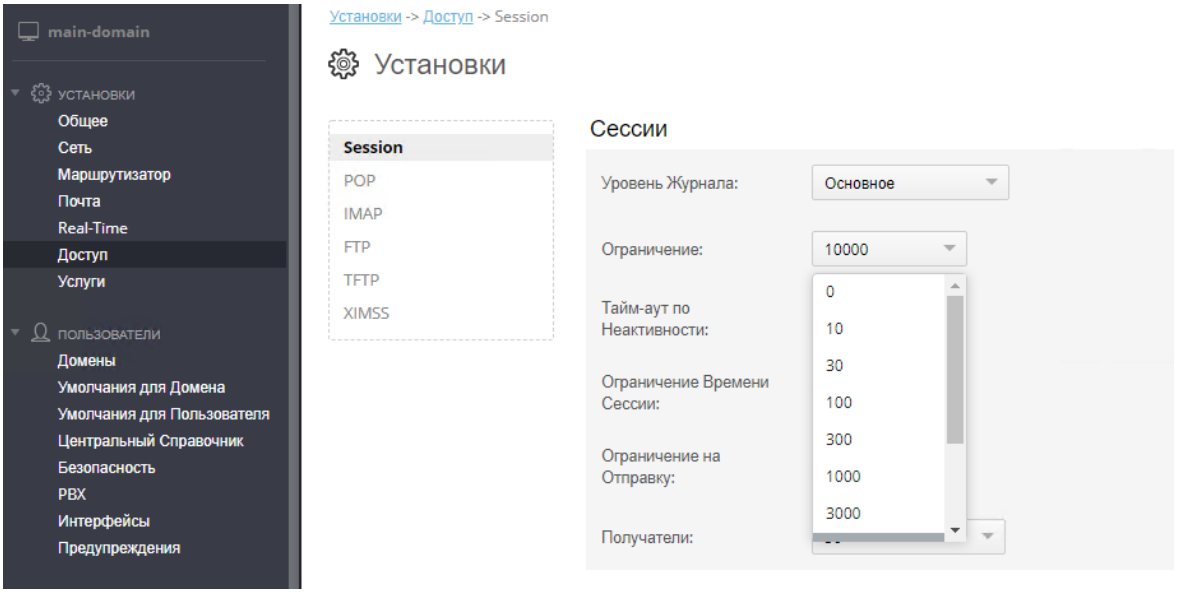
15.2 Предварительная настройка CommuniGate Pro

Перед началом резервного копирования данных CommuniGate Pro потребуется выполнить некоторые действия.

15.2.1 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 панель управления CommuniGate Pro.
2. Перейдите в раздел **Установки** -> **Доступ**.
3. В разделе **Сессии** в поле **Ограничение** установите значение, равное 10000.

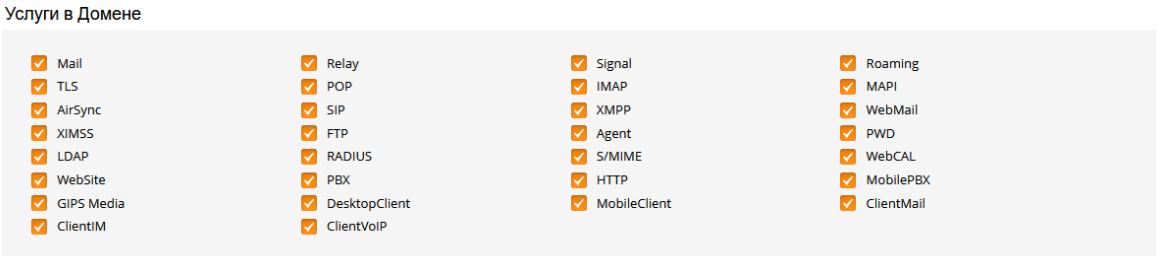


4. Нажмите **Модифицировать**, чтобы сохранить изменения.

15.2.2 Инициализация соединения вручную

Для инициализации соединения Кибер Бэкап Облачный с CommuniGate Pro (например, если интерфейс командной строки недоступен) выполните следующие действия:

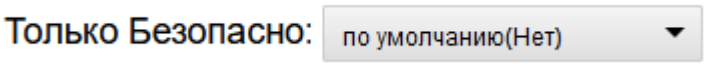
1. Откройте панель управления CommuniGate Pro.
2. Перейдите в раздел **Пользователи** -> **Умолчания для Домена** и убедитесь, что услуга PWD включена.



3. Перейдите в раздел **Пользователи** -> **Домены** -> **<Имя_домена>** -> **Установки Домена** и убедитесь, что в настройках домена включена услуга PWD.

4. Перейдите в раздел **Умолчания для пользователя** -> **Установки** и убедитесь, что в настройках пользователя включена услуга PWD.

5. Перейдите в раздел **Умолчания для пользователя** -> **Установки** и выберите **Нет** в параметре **Только безопасно**.



6. Для сохранения изменений нажмите **Модифицировать**.
7. Щелкните **Пользователи** и выберите из списка пользователя (домен), который используется для подключения к Кибер Бэкап Облачный.
8. Убедитесь, что в настройках пользователя (домена), используемого для подключения к Кибер Бэкап Облачный, включены все опции PWD.

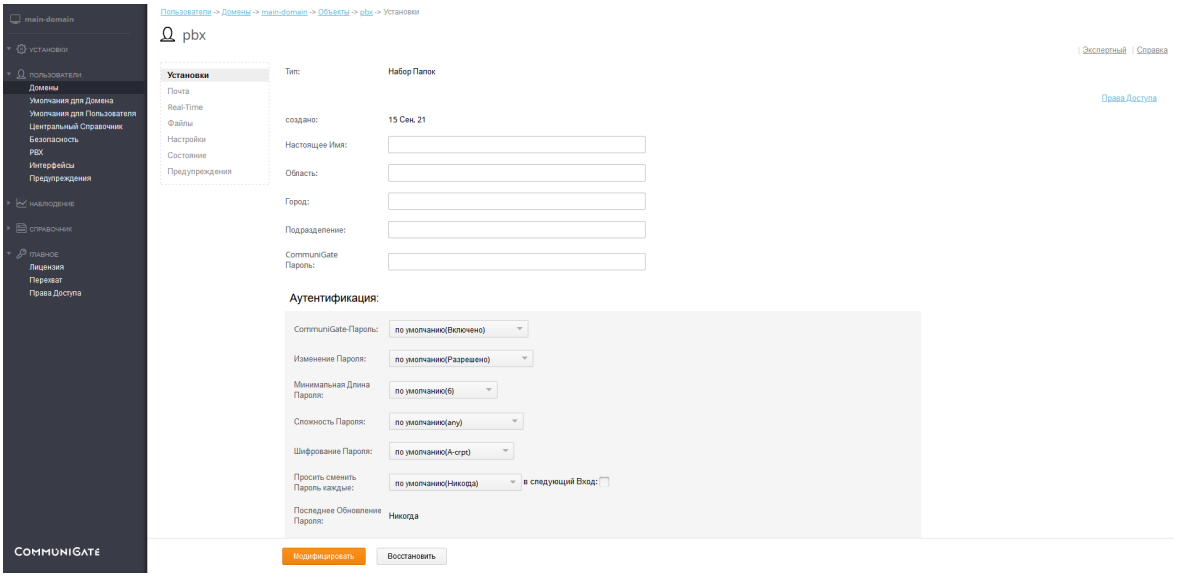
15.2.3 Установка прав пользователя

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.

Установка прав пользователя:

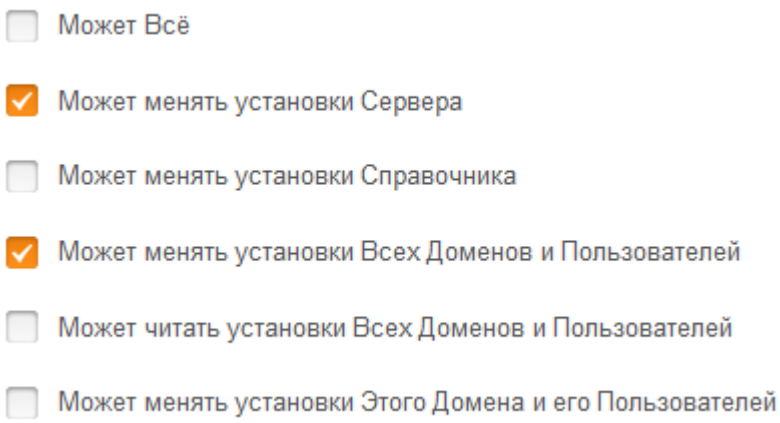
1. Откройте панель управления CommuniGate Pro.
2. Перейдите в раздел **Пользователи** -> **Домены** -> **Имя главного домена**.
3. Щелкните по имени пользователя в списке объектов.
4. На странице настроек пользователя нажмите справа вверху **Права доступа**.



5. Установите права пользователя следующим образом:

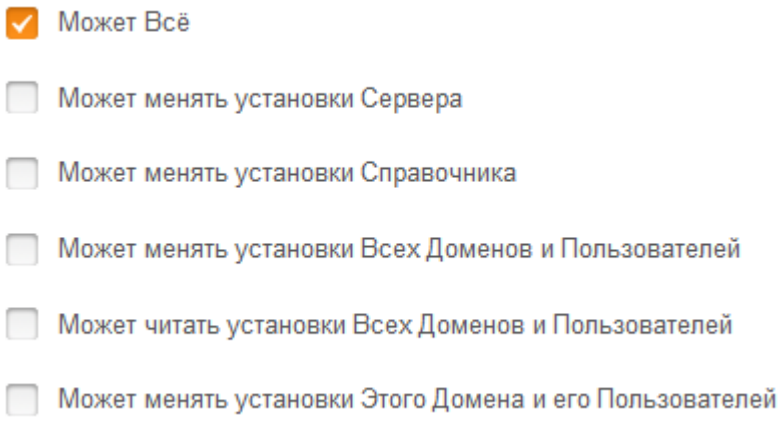
   Может менять установки Сервера и

   Может менять установки всех Доменов и Пользователей



   или

   Может Всё



6. Для сохранения изменений нажмите **Модифицировать**.

15.2.4 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):

- Через порт 106 по протоколу PWD происходит базовое подключение для регистрации и определения параметров сервера.
- 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.

15.2.5 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
)
```

15.3 Установка CommuniGate Pro

Установка включает в себя следующие шаги:

1. Установка агента Кибер Бэкап Облачный для операционной системы, которую вы используете (агент Windows или агент Linux), а также агента CommuniGate Pro.
2. Добавление в веб-консоли Кибер Бэкап Облачный хоста CommuniGate Pro.

Агент CommuniGate Pro может быть установлен на машину с почтовым сервером или на отдельно стоящую машину.

Для каждого хоста должен быть установлен отдельный агент.

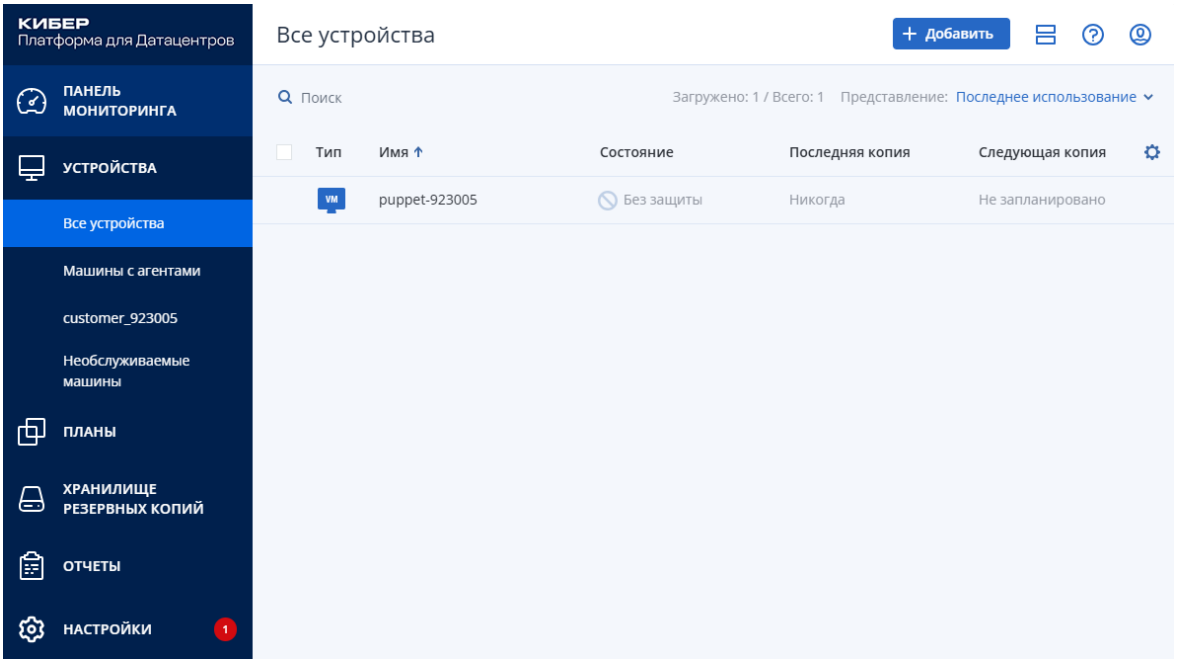
15.3.1 Установка агентов для CommuniGate Pro

Для установки агента для операционной системы, которую вы используете (агент Windows или агент Linux), и агента CommuniGate Pro обратитесь к разделу "Установка агентов" (стр. 43).

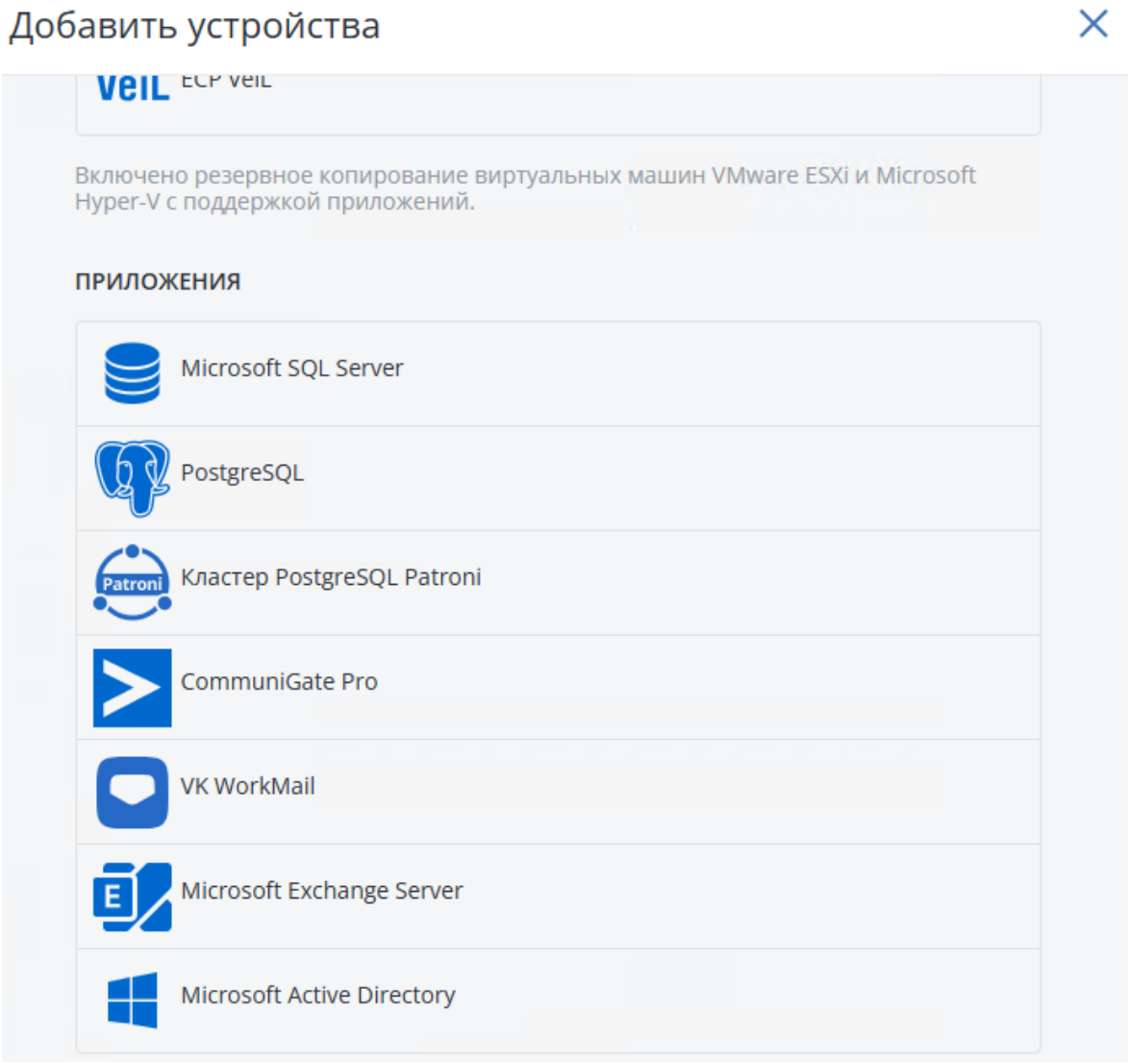
Для резервного копирования большого количества почтовых ящиков можно установить и использовать сразу несколько агентов.

15.3.2 Добавление хоста CommuniGate Pro

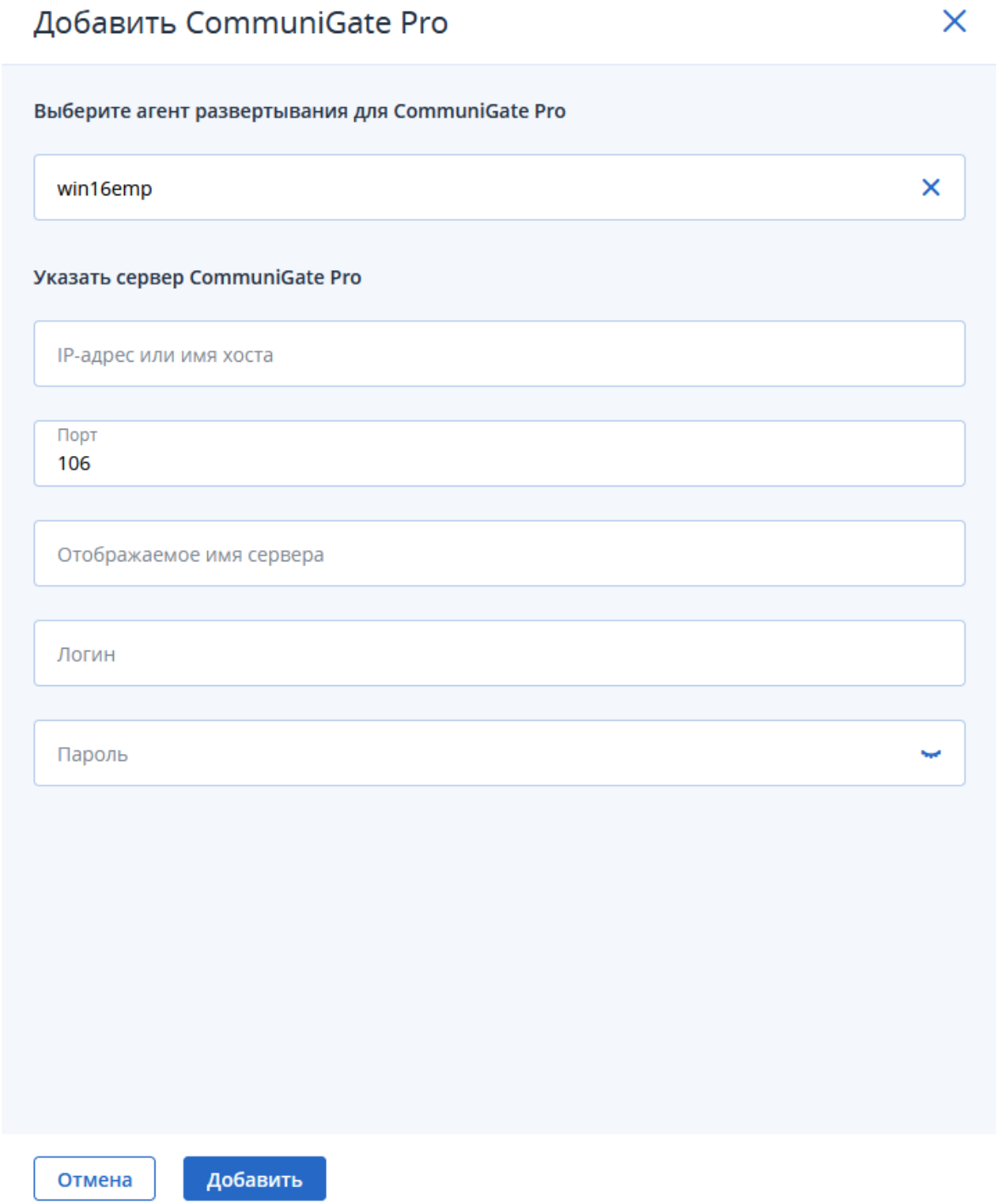
1. В веб-консоли перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.



2. В окне добавления нового устройства щелкните CommuniGate Pro.



3. Заполните поля:
   - в поле **Выберите агент развертывания для CommuniGate Pro** укажите имя устройства, на котором установлен агент CommuniGate Pro,
   - в поле **Указать сервер CommuniGate Pro** укажите IP-адрес или имя сервера CommuniGate Pro,
   - в поле **Отображаемое имя сервера** укажите имя, под которым сервер будет отображаться в системе,
   - в полях **Логин** и **Пароль** укажите имя и пароль пользователя.



4. По окончании ввода данных нажмите **Добавить**.

15.4 Резервное копирование CommuniGate Pro

Резервное копирование данных CommuniGate Pro позволяет защитить домены и отдельные почтовые ящики. Для защиты данных необходимо сначала создать план защиты.

15.4.1 Создание плана защиты для CommuniGate Pro

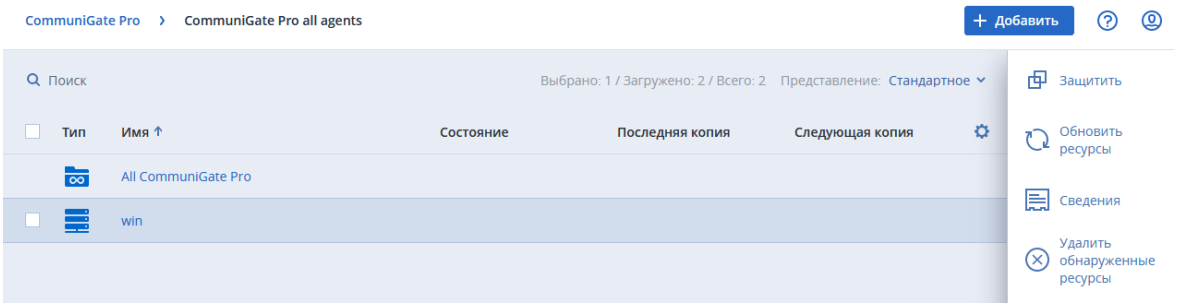
Для резервного копирования большого количества почтовых ящиков можно использовать сразу несколько агентов.

Для этого выполните следующие действия:

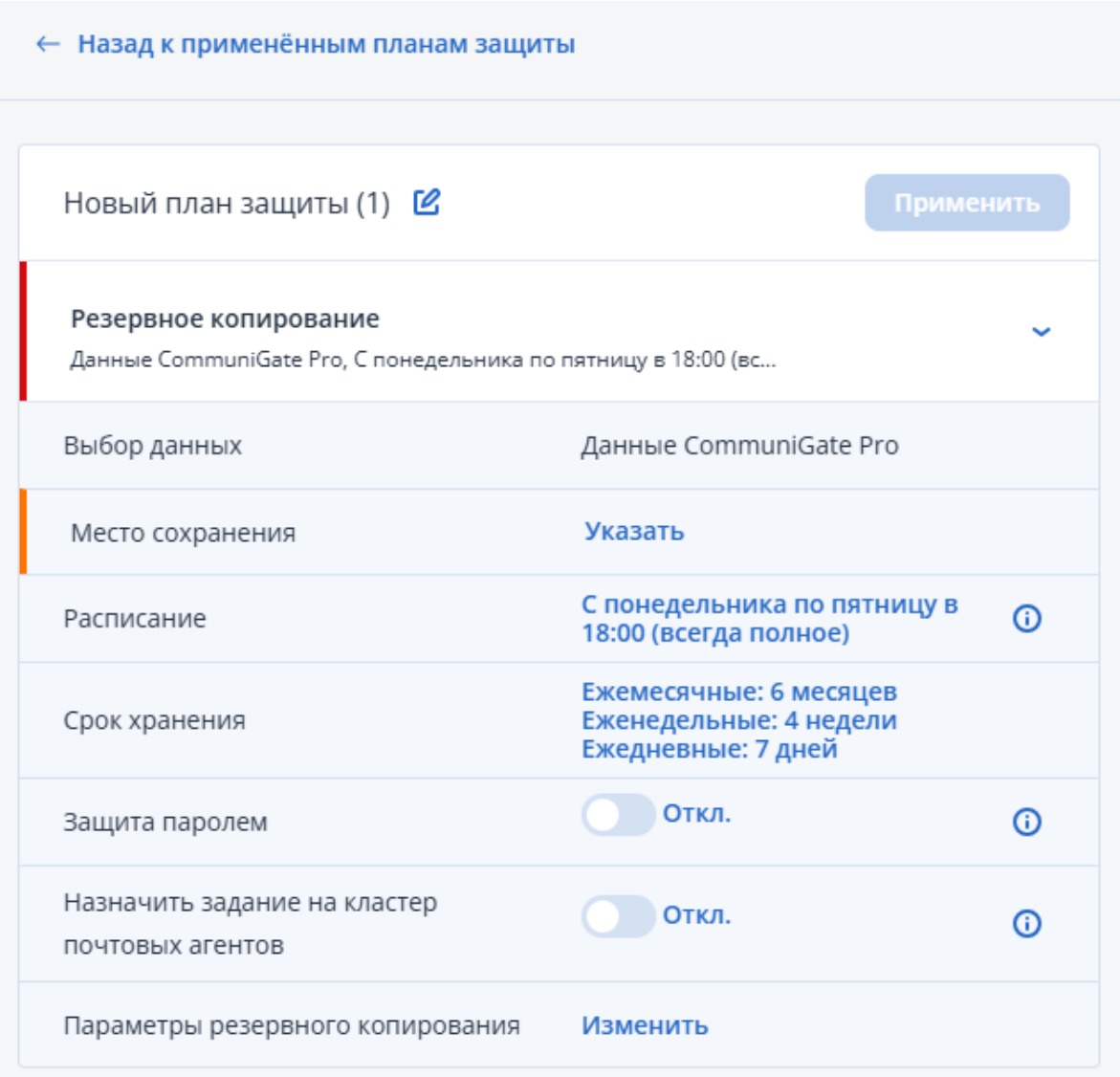
1. Установите необходимое количество агентов CommuniGate Pro.
2. Используйте опцию **Назначить задание на кластер почтовых агентов** при создании плана резервного копирования.

Для создания плана защиты выполните следующие действия:

1. Перейдите в раздел **Устройства**.
2. Выберите ресурсы CommuniGate Pro, для которых вы хотите создать план защиты.
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, папка NFS, облачное хранилище.

     Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 141).
   - 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** нажмите **Изменить** и укажите следующие параметры:

- **Еженедельная резервная копия**. Укажите день недели для создания еженедельной копии.
- **Имя файла резервной копии**. Укажите шаблон для наименований файлов резервных копий.
- **Обработка ошибок**. Укажите порядок обработки ошибок, возникающих при резервном копировании.
- **Уровень сжатия**. Укажите уровень сжатия данных при резервном копировании.

Подробнее см. в разделе "Параметры резервного копирования" (стр. 178).

Обратите внимание на то, что в случае изменения этих параметров следующее резервное копирование будет полным.

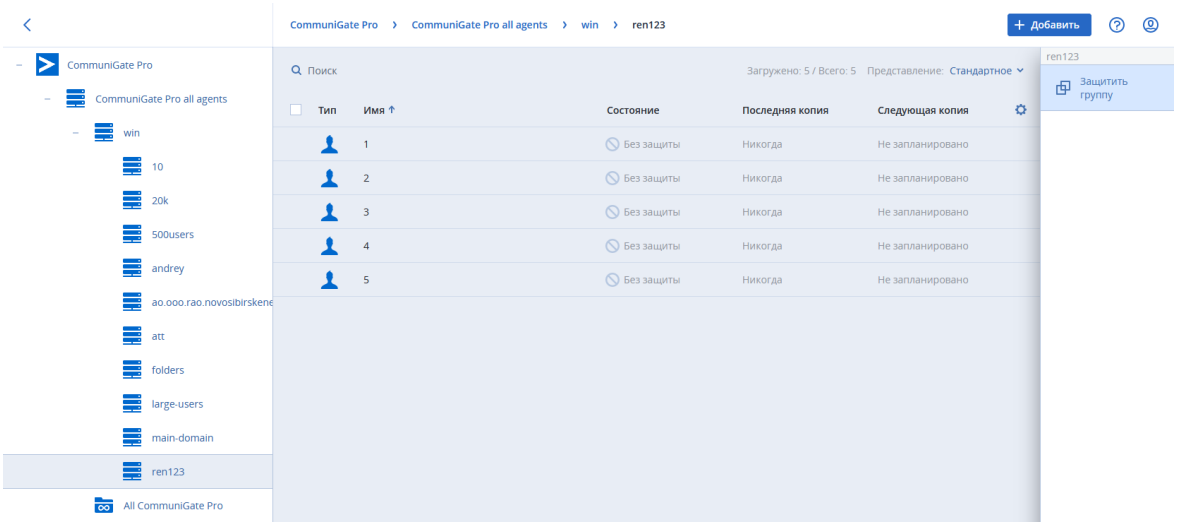
6. По окончании настройки плана нажмите **Применить**. Новый план защиты появится в списке планов.

См. также информацию в разделе "План защиты и модули" (стр. 128).

15.4.2 Резервное копирование данных CommuniGate Pro

Резервное копирование домена

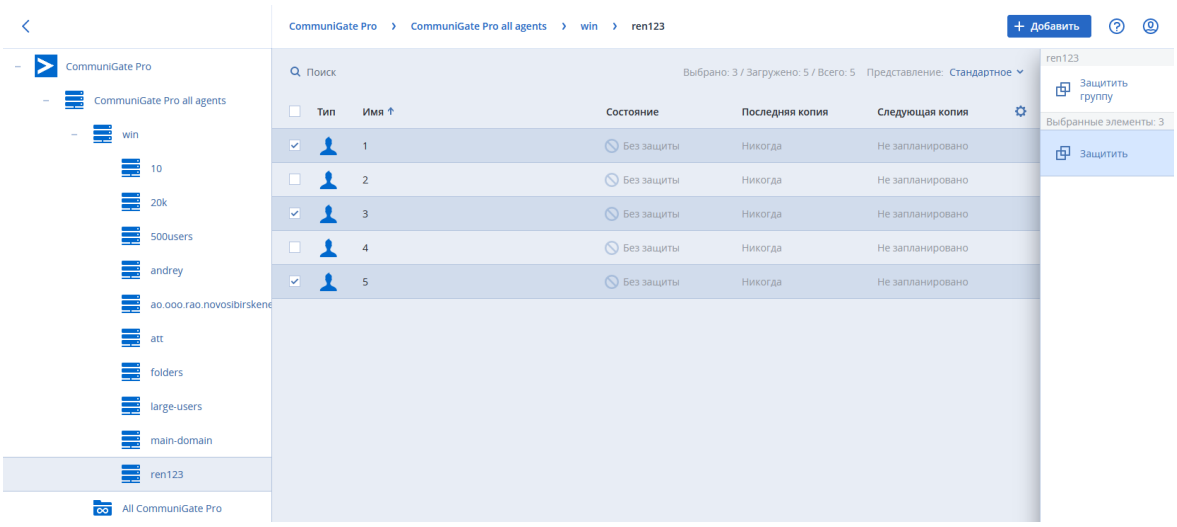
1. В списке доменов щелкните по строке, содержащей название домена, и перейдите на вкладку **Защитить группу** в меню справа.



2. В окне выбора плана защиты в списке планов защиты выберите подходящий план и щелкните **Применить**.

Резервное копирование почтового ящика

1. Чтобы защитить почтовый ящик, раскройте список почтовых ящиков в домене, щелкните по строке, содержащей имя домена, и перейдите на вкладку **Защитить** в меню справа.
2. Чтобы выбрать несколько почтовых ящиков, входящих в домен, щелкните 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.



3. В окне выбора плана защиты в списке планов защиты выберите подходящий план и щелкните **Применить**.

Резервное копирование по требованию

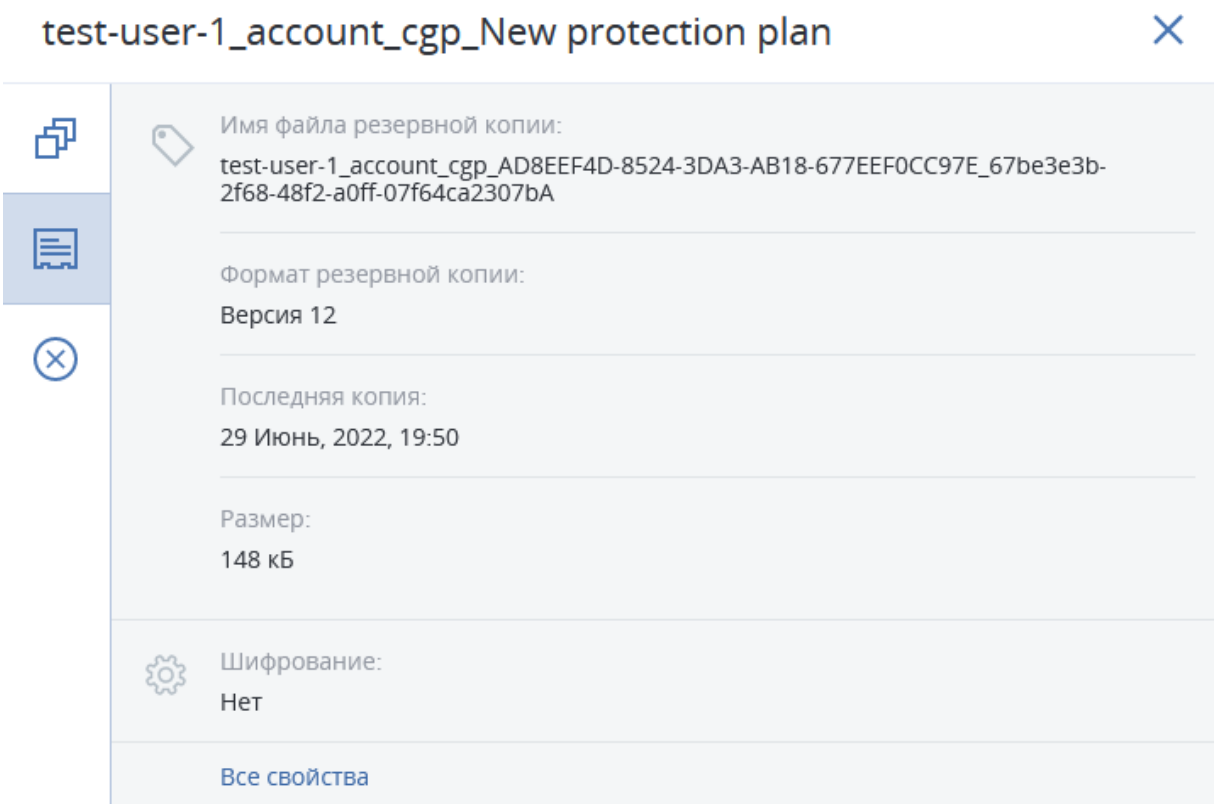
Резервное копирование по требованию представляет собой запуск выбранного плана защиты вне очереди. Чтобы выполнить резервное копирование по требованию:

1. Щелкните по строке, содержащей название почтового ящика или домена.
2. Перейдите на вкладку **Защитить** для почтового ящика или **Защитить группу** для домена в меню справа.
3. В строке **Резервное копирование** или в нижней части вкладки нажмите кнопку **Запустить сейчас**.

15.4.3 Резервные копии CommuniGate Pro

Чтобы посмотреть список резервных копий, перейдите на вкладку **Хранилище резервных копий** и выберите хранилище.

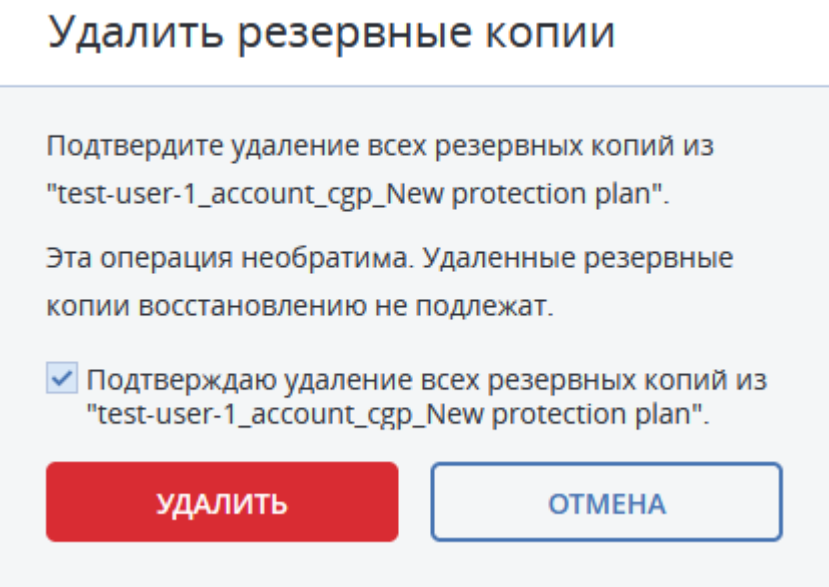
Чтобы посмотреть сведения о резервной копии, щелкните по строке, содержащей название резервной копии, и перейдите на вкладку **Сведения** в меню справа.



Подробная информация доступна по ссылке **Все свойства**.

Чтобы удалить резервную копию:

1. Перейдите на вкладку **Удалить** в меню справа.



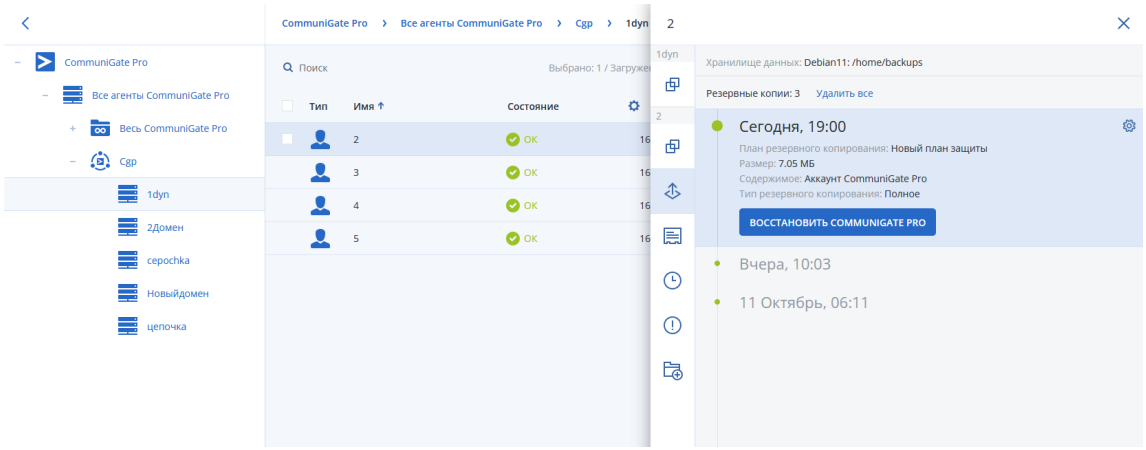
2. Для подтверждения удаления отметьте флажок в поле и нажмите **Удалить**.

   Выбранная резервная копия после удаления исчезнет из списка резервных копий.

15.5 Восстановление CommuniGate Pro

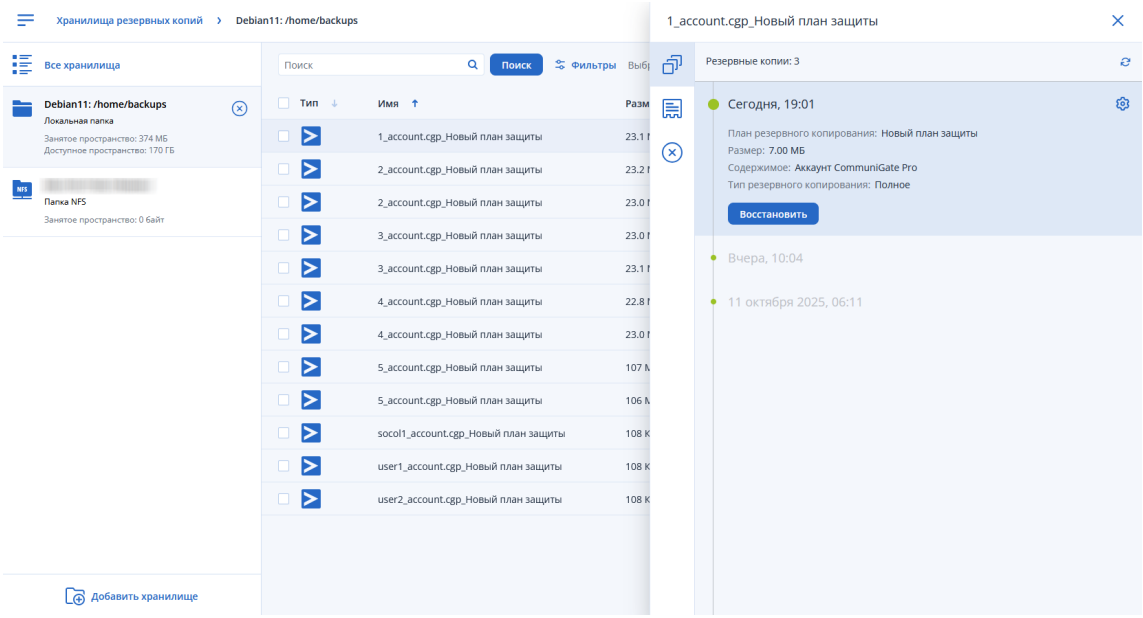
Восстановление данных CommuniGate Pro

1. Выполните одно из следующих действий:
   - Перейдите в **Устройства** -> **CommuniGate Pro**, щелкните кластер, сервер или домен, данные в котором хотите восстановить, выберите в списке нужный аккаунт (учетную запись), справа в меню щелкните **Восстановление** и далее **Восстановить CommuniGate Pro**.

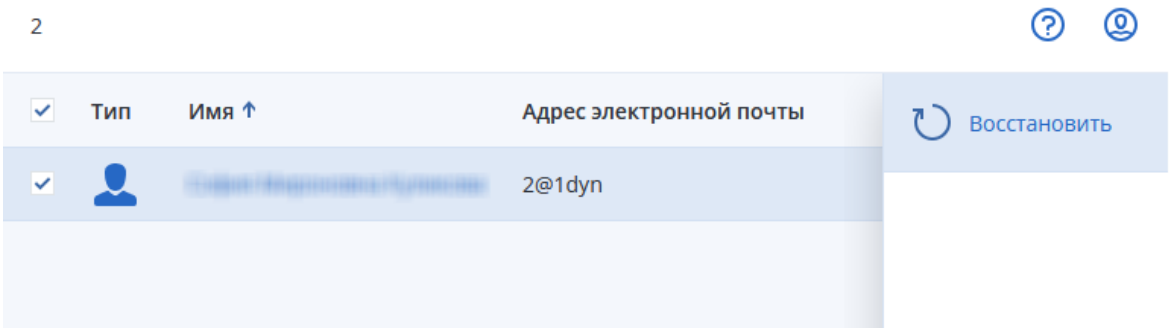


   - Перейдите в **Хранилище резервных копий**, щелкните хранилище с резервными копиями,

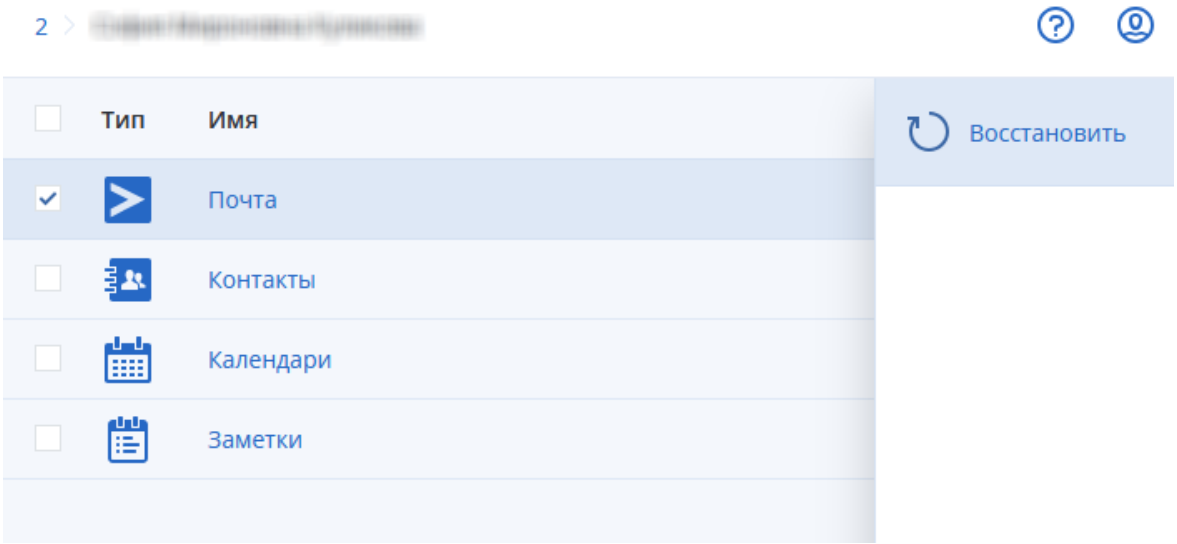
выберите в списке нужный аккаунт и нажмите **Восстановить**.



2. Для восстановления всех данных пользователя отметьте галочкой имя пользователя и нажмите **Восстановить**. Иначе просто щелкните имя пользователя.



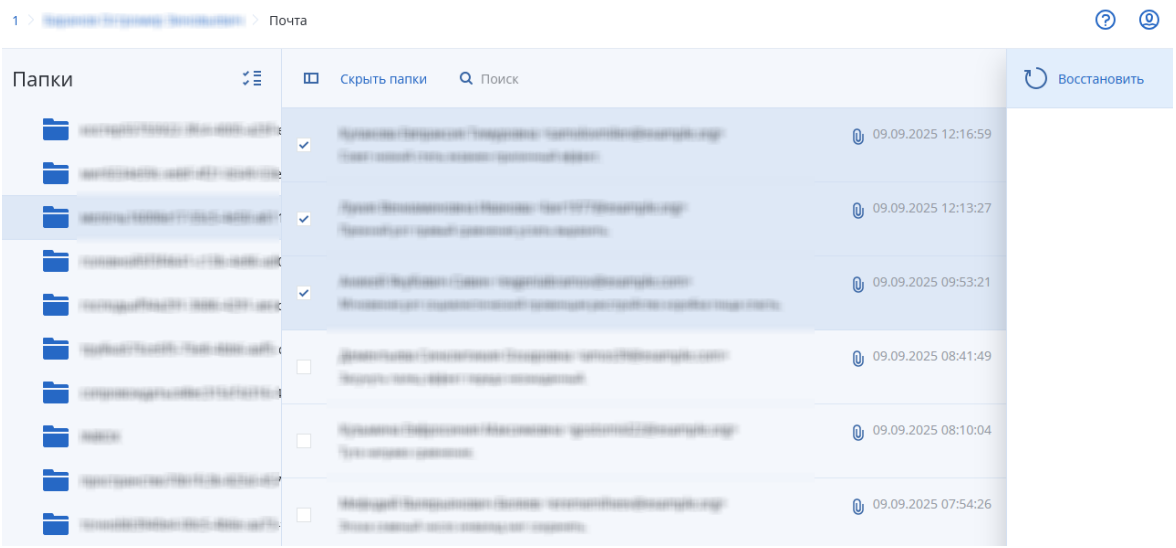
3. Для восстановления всех данных одного типа отметьте галочкой тип восстанавливаемых данных (**Почта**, **Контакты**, **Календари**, **Заметки**).



Для восстановления определенных данных щелкните на названии типа нужных данных (например, **Почта**) и далее в списке отметьте галочками те данные (например, письма), которые необходимо восстановить.

Примечание

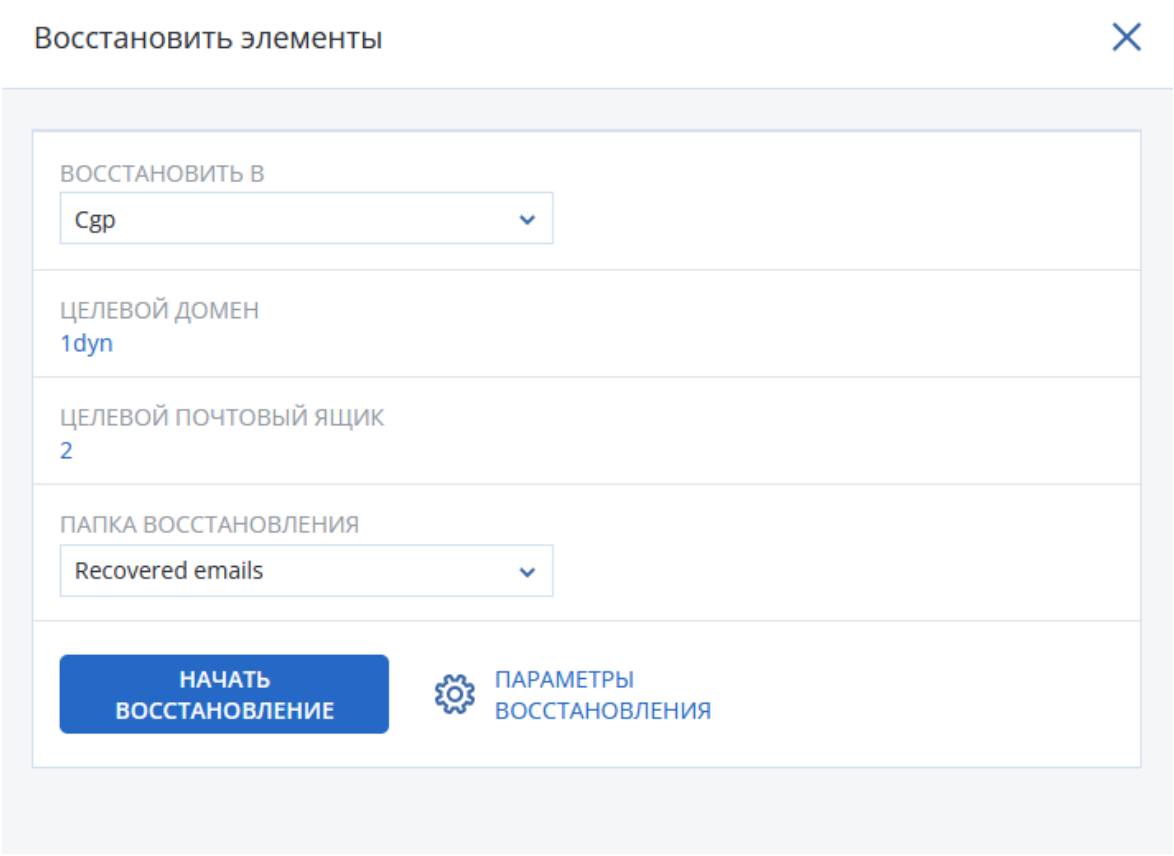
Восстановление на новый сервер можно выполнить только при восстановлении всех данных пользователя или всех данных одного типа.



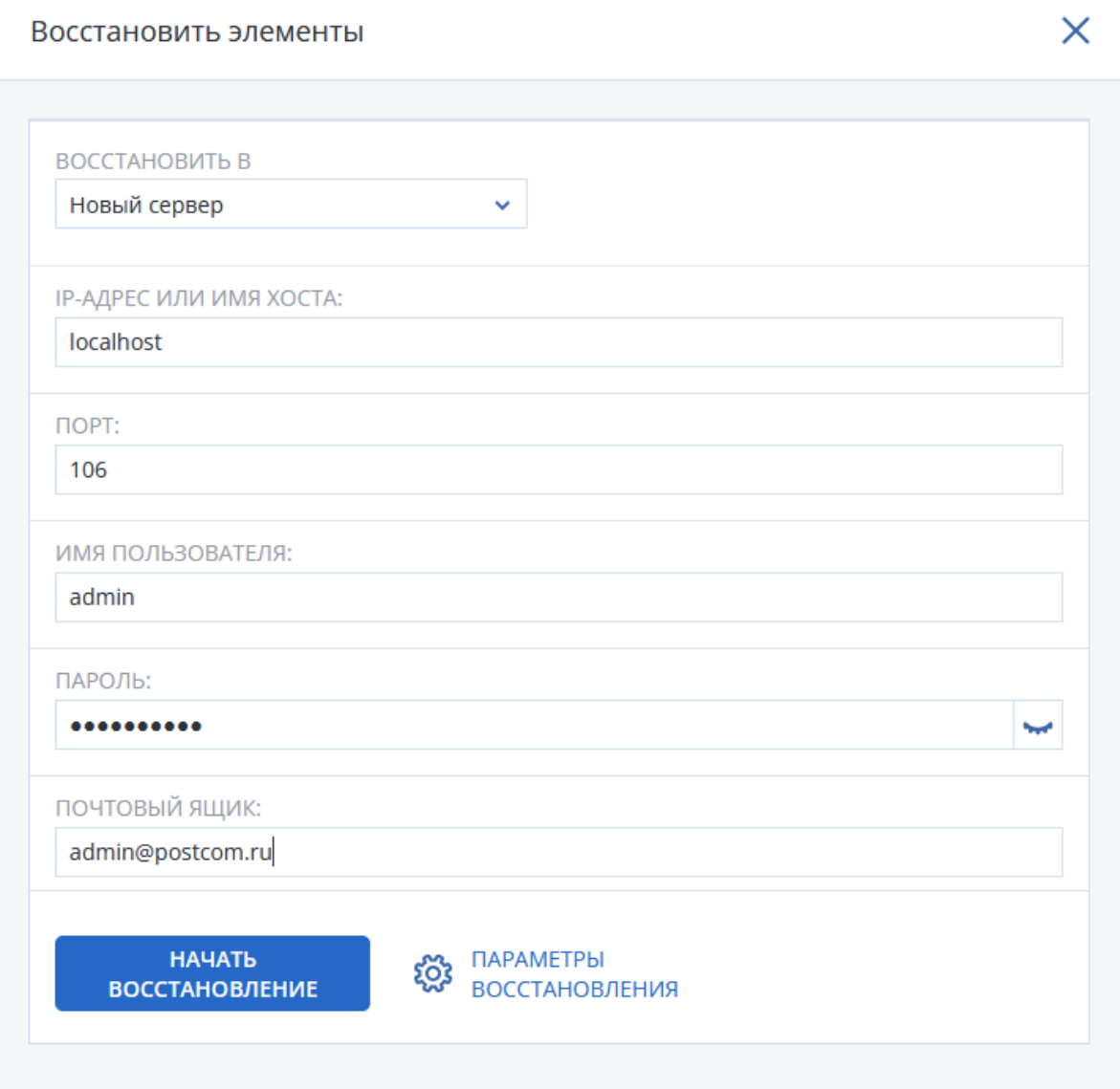
Для просмотра содержимого письма нажмите справа **Показать содержимое**. Для скачивания вложения щелкните по этому вложению.

Для поиска нажмите значок поиска сверху. Для почты доступен расширенный поиск, для его настройки нажмите значок выпадающего списка в строке поиска.

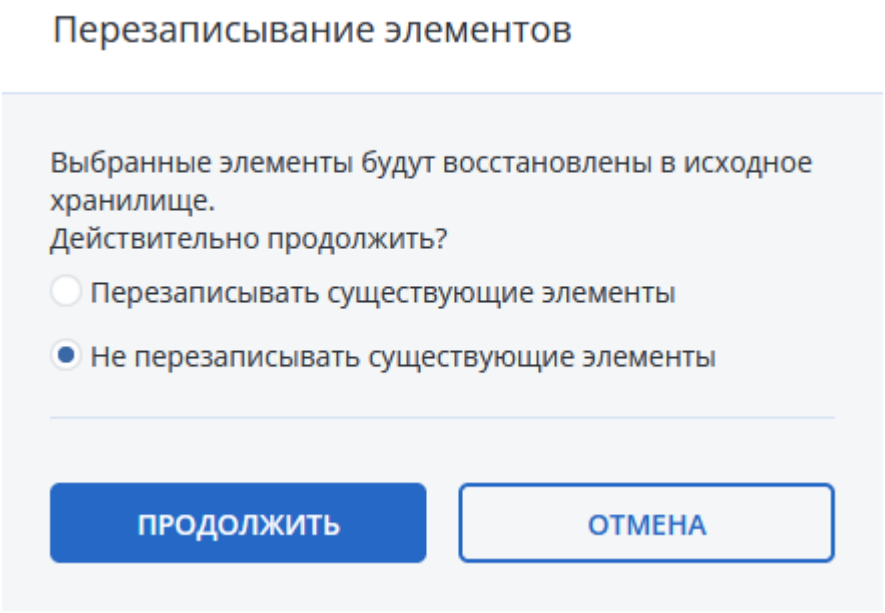
4. Нажмите **Восстановить**.
5. На экране **Восстановить элементы** укажите место для восстановления:
   a. Существующий сервер или новый сервер;
   b. Домен (из существующих);
   c. Почтовый ящик (из существующих);
   d. Папка для восстановления (если происходит восстановление выбранных вами данных 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.

Внимание
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. Щелкните на резервную копию, которую хотите удалить.
2. Щелкните значок настройки справа вверху.
3. Нажмите **Удалить**.

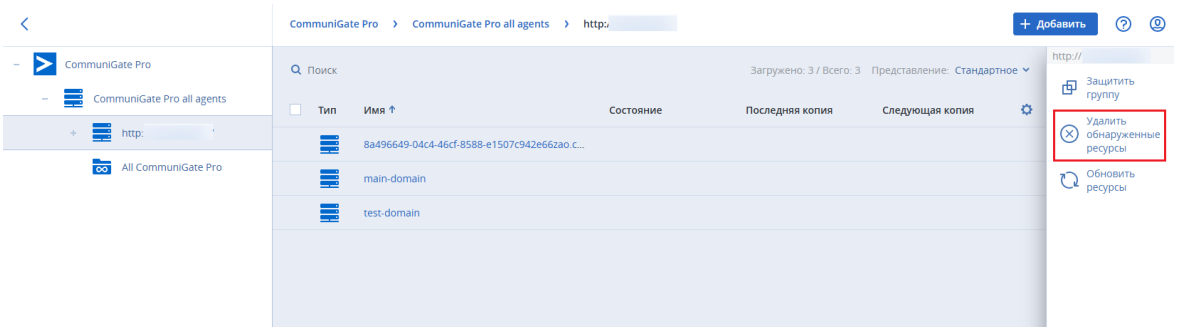
Чтобы удалить все резервные копии, во вкладке **Восстановление** щелкните ссылку **Удалить все**.

15.6 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 в раздел **Устройства** > **CommuniGate Pro**.
2. Отметьте хост CommuniGate Pro в списке.
3. В меню справа щелкните **Удалить обнаруженные ресурсы**.



4. В окне подтверждения удаления нажмите **Удалить**.

   Устройство будет удалено из списка.

Примечание

Удаление хоста не затрагивает агент CommuniGate Pro и существующие резервные копии.

16 Защита VK WorkMail и VK WorkDisk

16.1 Зачем обеспечивать защиту 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 Облачный 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 Облачный регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователей и различных сбоев. Удаленные элементы можно восстановить из резервной копии.

16.2 Что необходимо для резервного копирования

Для резервного копирования данных VK WorkMail и VK WorkDisk понадобятся установленные и настроенные продукты:

- Кибер Бэкап Облачный 24.11 или новее с лицензией для почтовых ящиков.
- VK WorkMail с подключенными ресурсами VK WorkDisk.

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 и среды" (стр. 16).

16.3 Возможности

Кибер Бэкап Облачный обеспечивает резервное копирование и восстановление:

- почтовых ящиков пользователей VK WorkMail,
- отдельных писем пользователей VK WorkMail,

- данных пользователя VK WorkDisk,
- серверов VK WorkMail и VK WorkDisk.

Также возможно скачивать отдельные файлы или данные пользователей из существующих резервных копий.

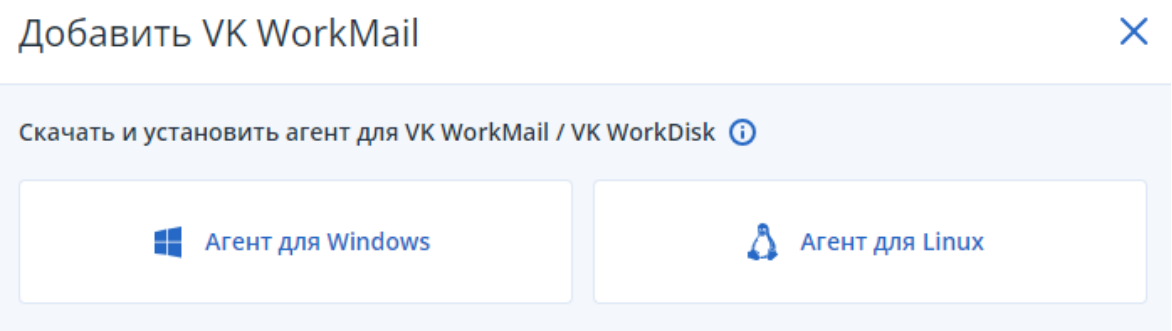
16.4 Установка VK WorkMail

Установка VK WorkMail включает в себя установку агента Кибер Бэкап Облачный и добавление хоста VK WorkMail. Добавление хоста возможно лишь после установки агента.

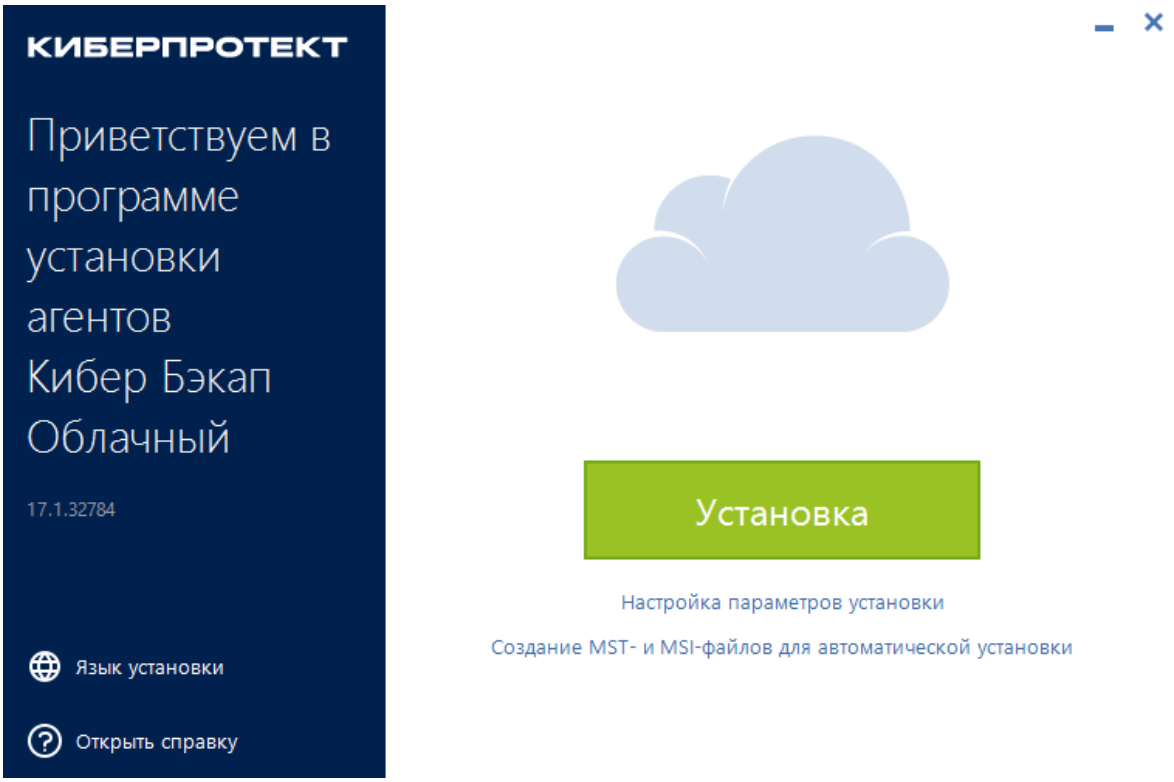
16.4.1 Установка агента для VK WorkMail

В этом разделе рассмотрена установка агента Кибер Бэкап Облачный для Windows. Для установки агента для Linux обратитесь к разделу "Установка агентов" (стр. 43).

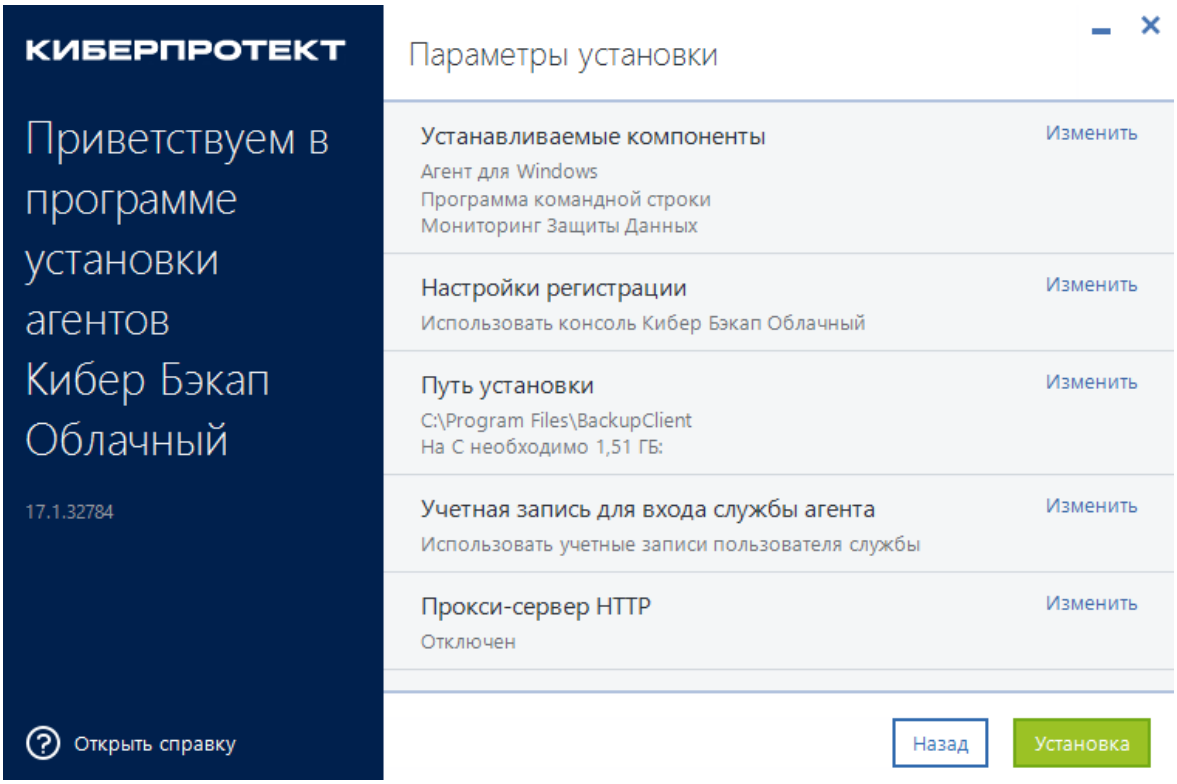
1. Перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.
2. В разделе **Приложения** нажмите **VK WorkMail**.
3. В окне добавления нового устройства нажмите **Агент для Windows**.



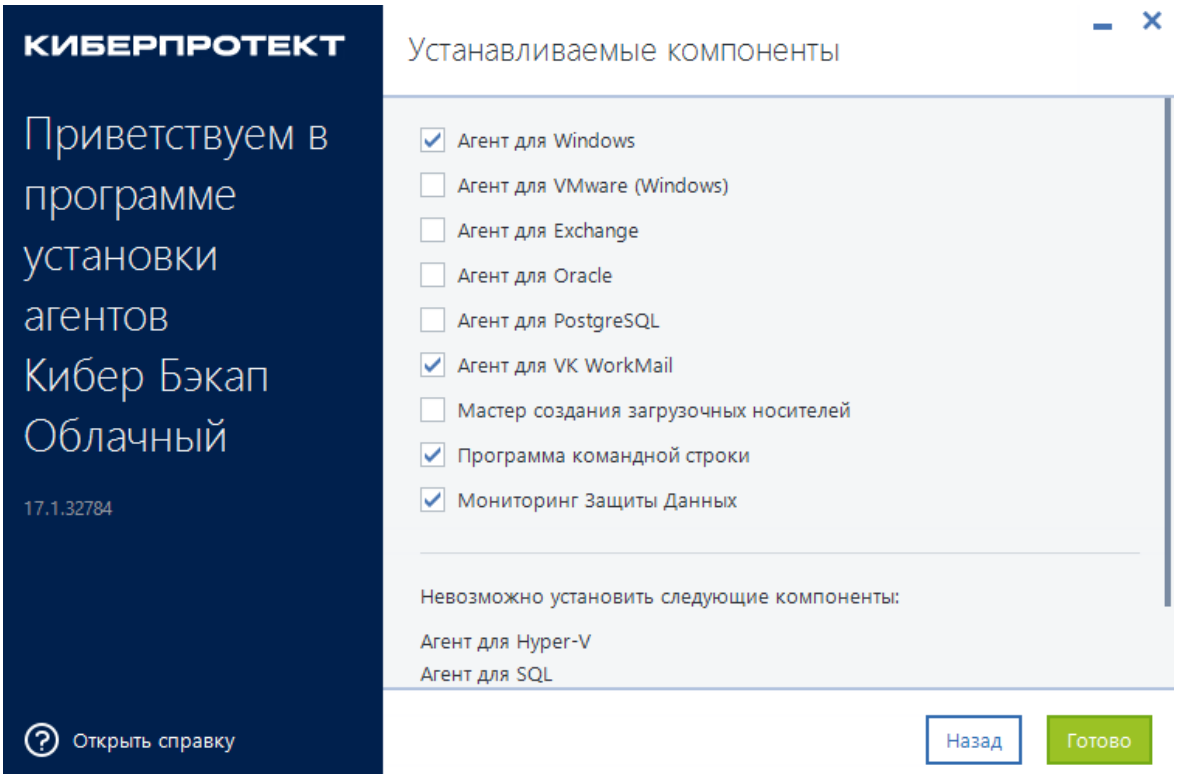
4. Выберите **Настройка параметров установки**.



5. В блоке **Устанавливаемые компоненты** выберите **Изменить**.



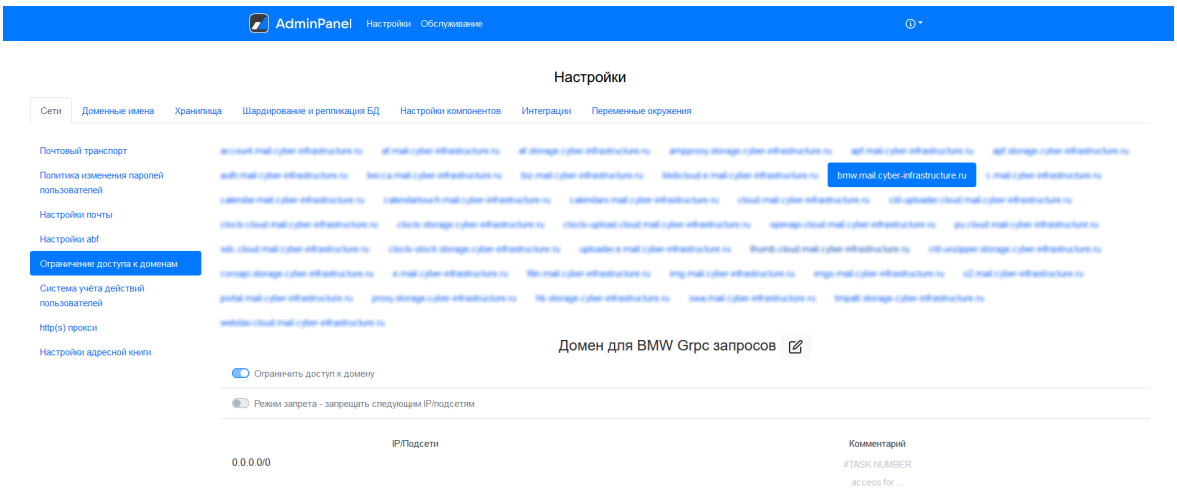
6. Отметьте в списке **Агент для VK WorkMail**.



7. Нажмите **Готово**.
8. Нажмите **Установка**. После завершения установки нажмите кнопку **Закрыть**.

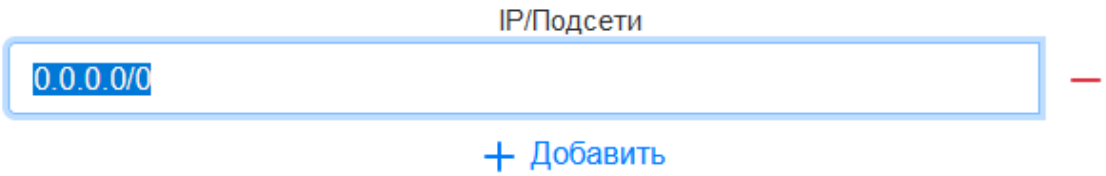
16.4.2 Настройка в панели администрирования VK WorkMail

1. Укажите настройки в панели администрирования VK WorkMail аналогично следующему примеру:

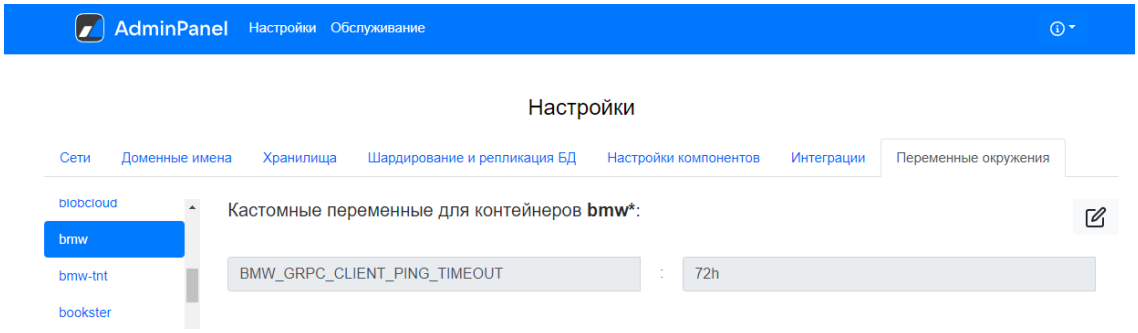


2. Для настройки IP-адреса нажмите значок редактирования

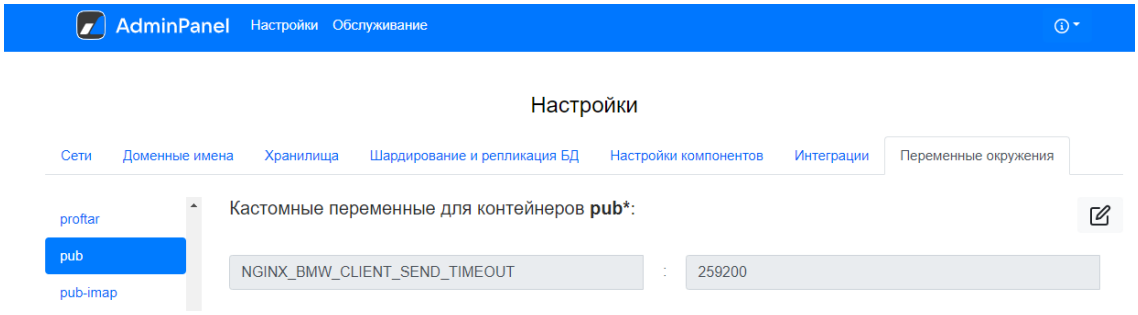
и введите IP-адрес компьютера, на который установлен агент для VK WorkMail.



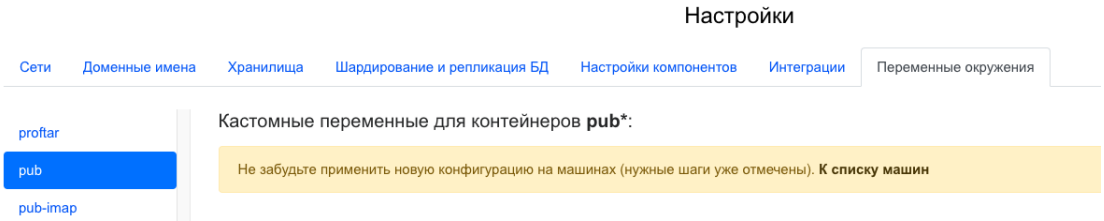
3. Нажмите **Сохранить**.
4. Добавьте переменные окружения:
   a. Перейдите в раздел **Настройки** и откройте вкладку **Переменные окружения**.
   b. В списке слева выберите контейнер **bmw**, создайте переменную BMW_GRPC_CLIENT_PING_TIMEOUT и укажите для нее значение 72h.



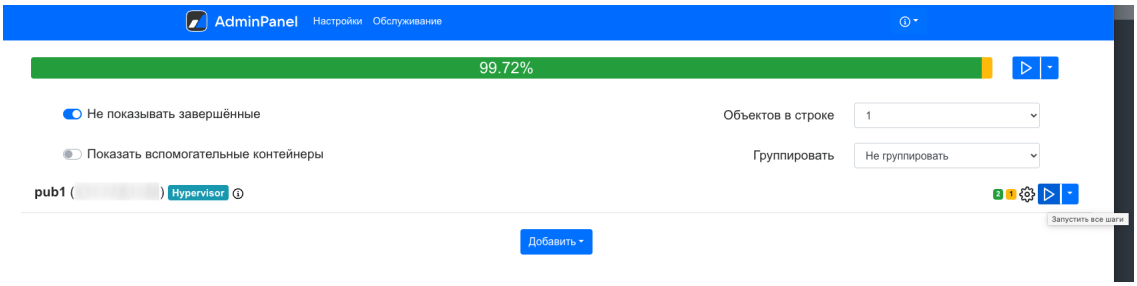
   c. В списке слева выберите контейнер **pub**, создайте переменную NGINX_BMW_CLIENT_SEND_TIMEOUT и укажите для нее значение 259200.



   d. Откройте экран со списком машин, перейдя по ссылке **К списку машин**.

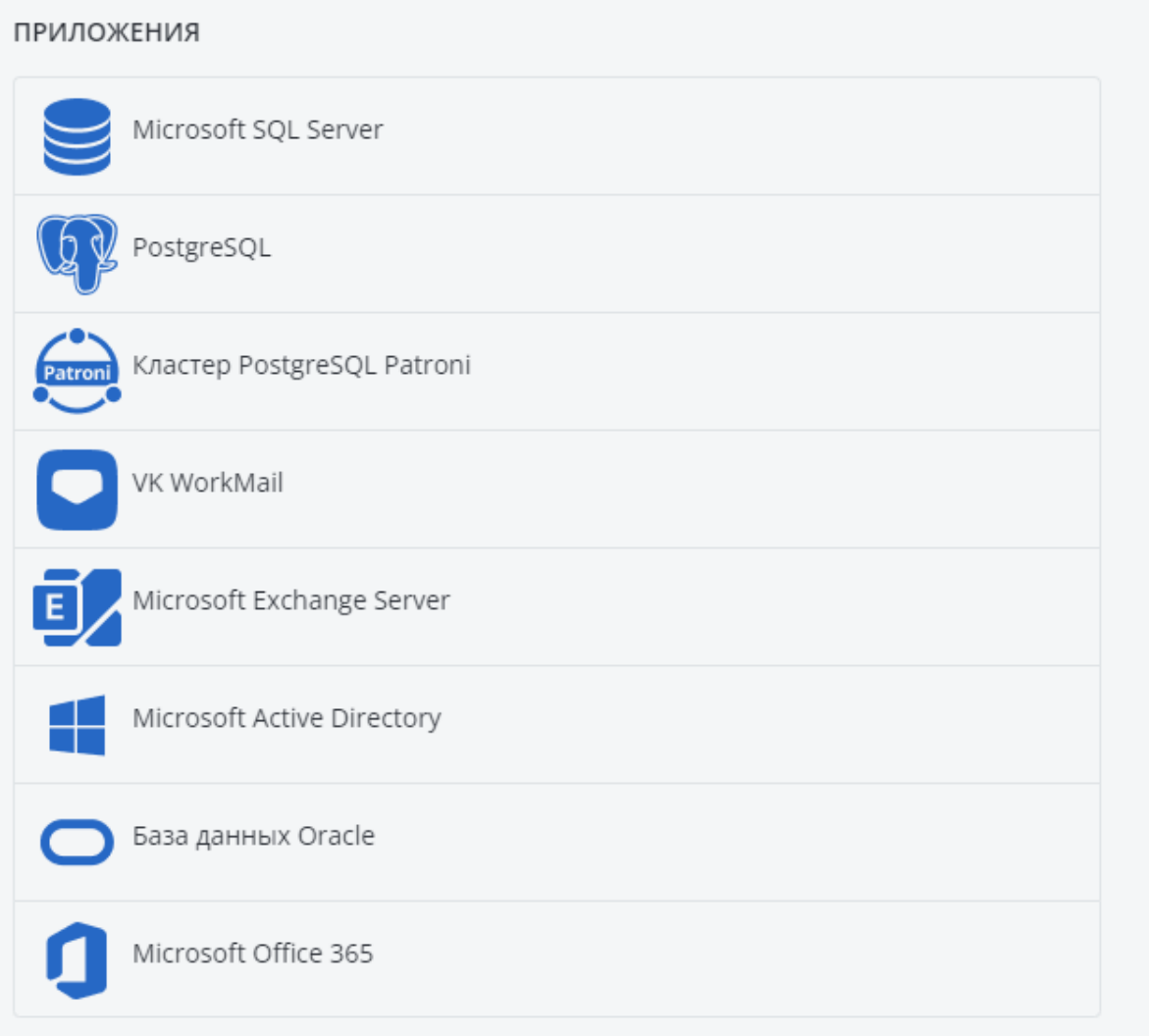


e. Примените изменения для обоих типов контейнеров, нажав на значок запуска  .



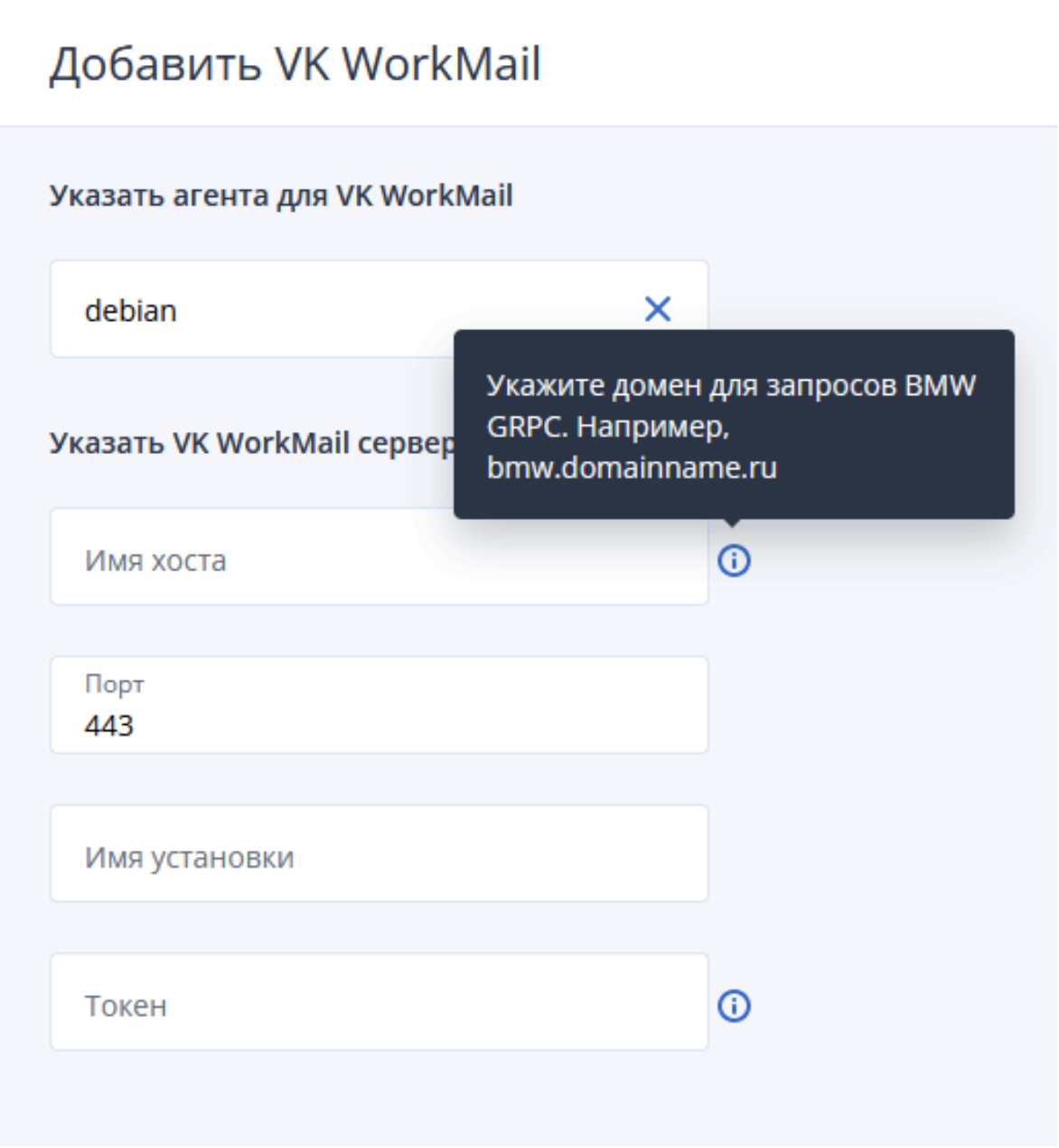
16.4.3 Добавление хоста VK WorkMail

1. Перейдите на вкладку **Устройства** и нажмите в правом верхнем углу **Добавить**.
2. В окне добавления нового устройства щелкните 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.



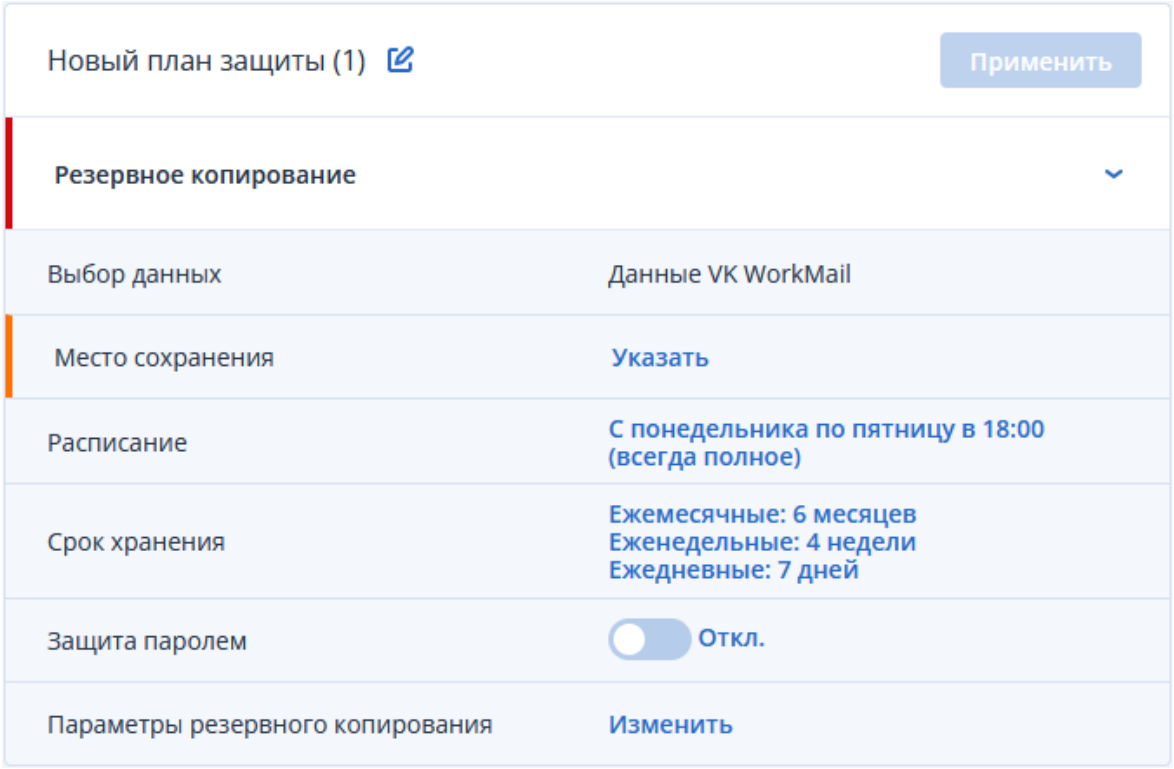
4. По окончании ввода данных нажмите **Добавить**.

16.5 Резервное копирование VK WorkMail и VK WorkDisk

16.5.1 Резервное копирование данных пользователей VK WorkMail

Для создания плана защиты выполните следующие действия:

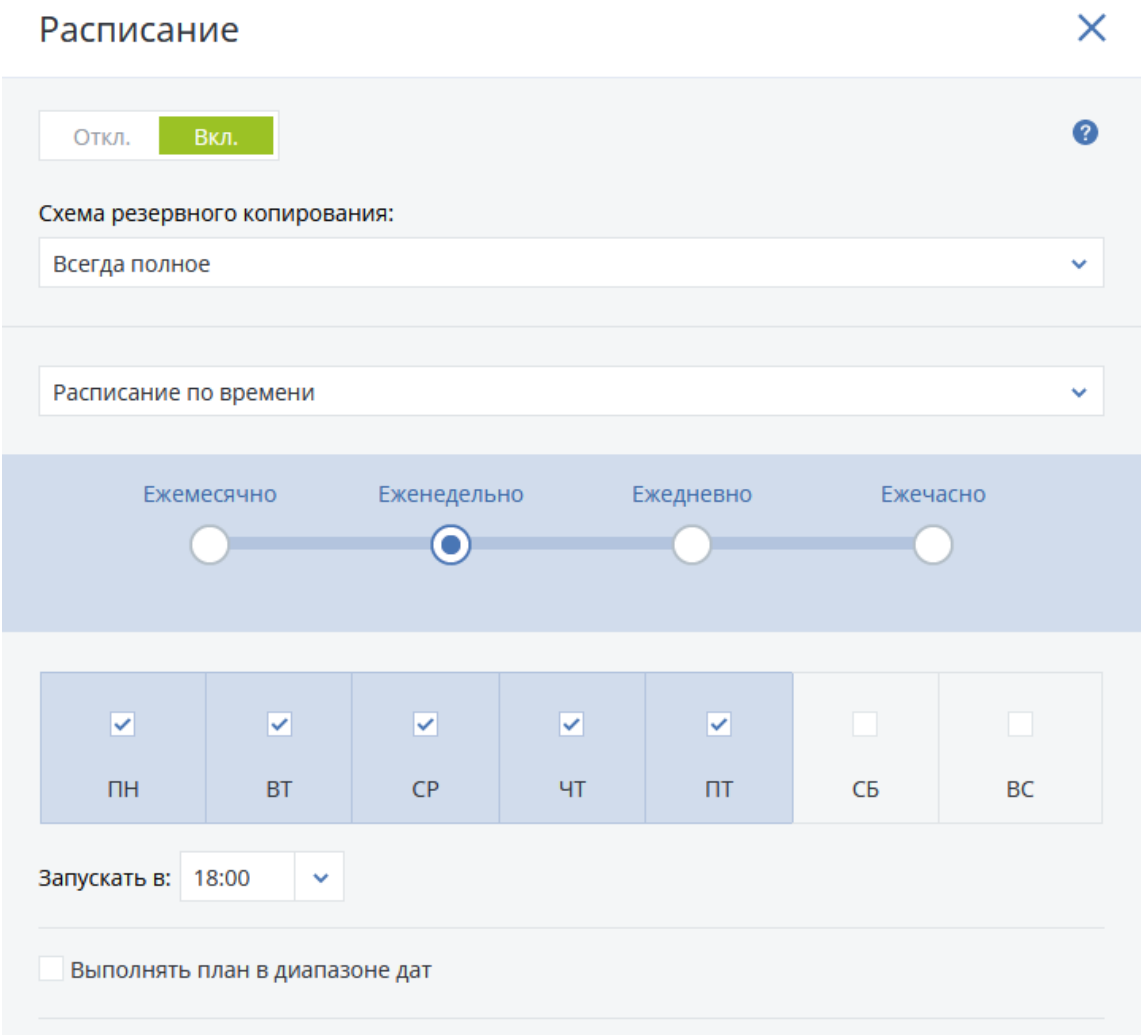
1. Перейдите в **Устройства** -> **VK WorkMail**.
2. Выберите из списка обнаруженных ресурсов VK WorkMail пользователя, для которого вы хотите создать защиту, и щелкните по строке, в которой находится имя этого пользователя.
3. Перейдите на вкладку справа **Защитить** для защиты почтового ящика или группы почтовых ящиков (домена).



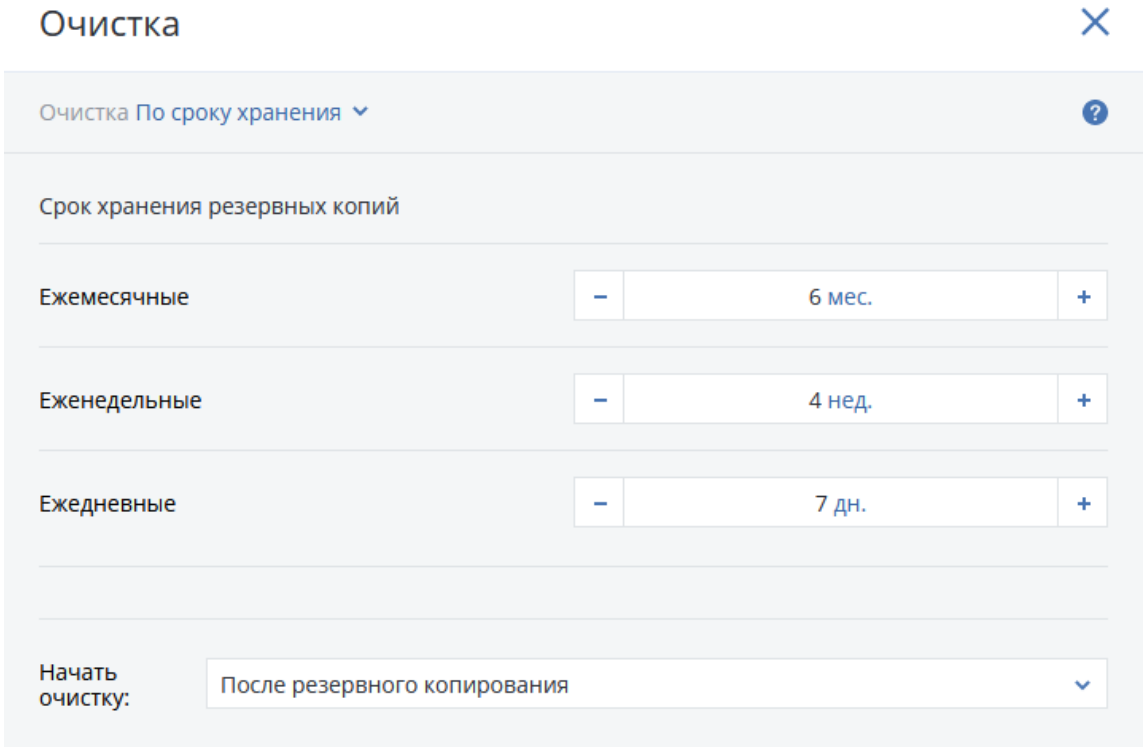
4. Заполните данные в окне создания плана защиты:
   - В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: облачное хранилище данных, локальная папка, сетевая папка, папка NFS.

     Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 141).

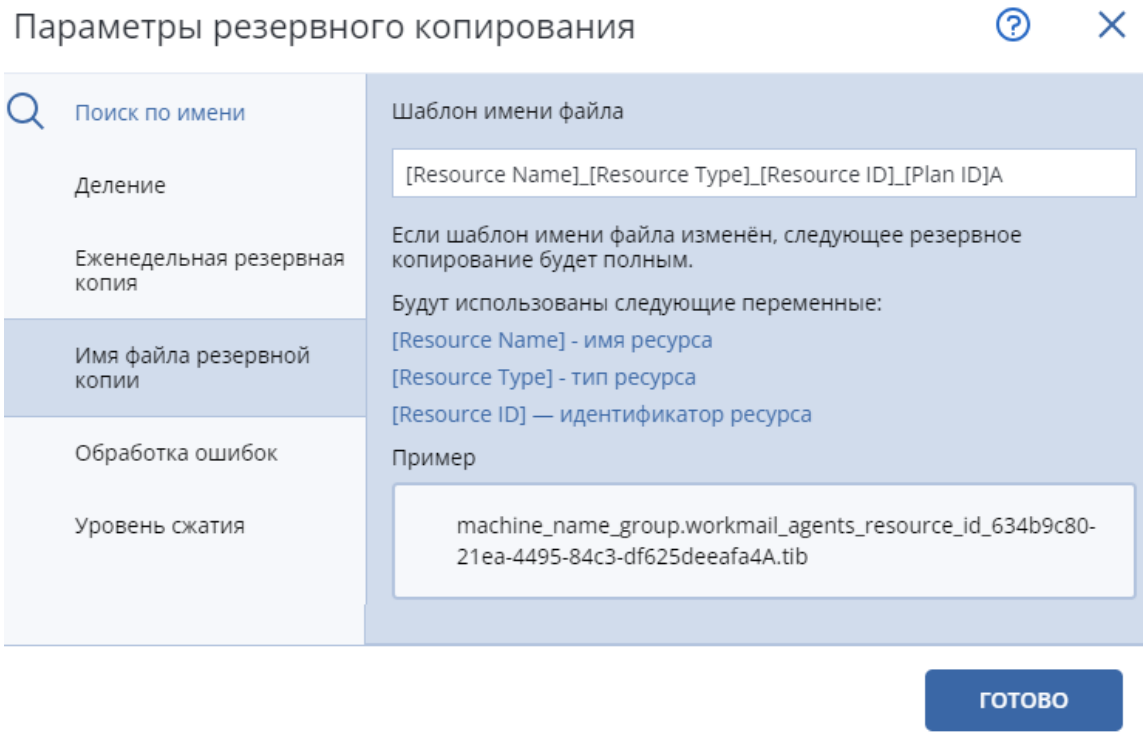
- В поле **Расписание** укажите схему и периодичность выполнения резервного копирования.



- В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.



- [Необязательно] В поле **Параметры резервного копирования** укажите метод разбиения резервных копий на меньшие по размеру фрагменты, параметры обработки ошибок и уровень сжатия резервных копий.



Примечание
Параметр «Деление» недоступен при резервном копировании в облачное хранилище данных.

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" (стр. 128).

16.5.2 Резервное копирование больших объемов данных

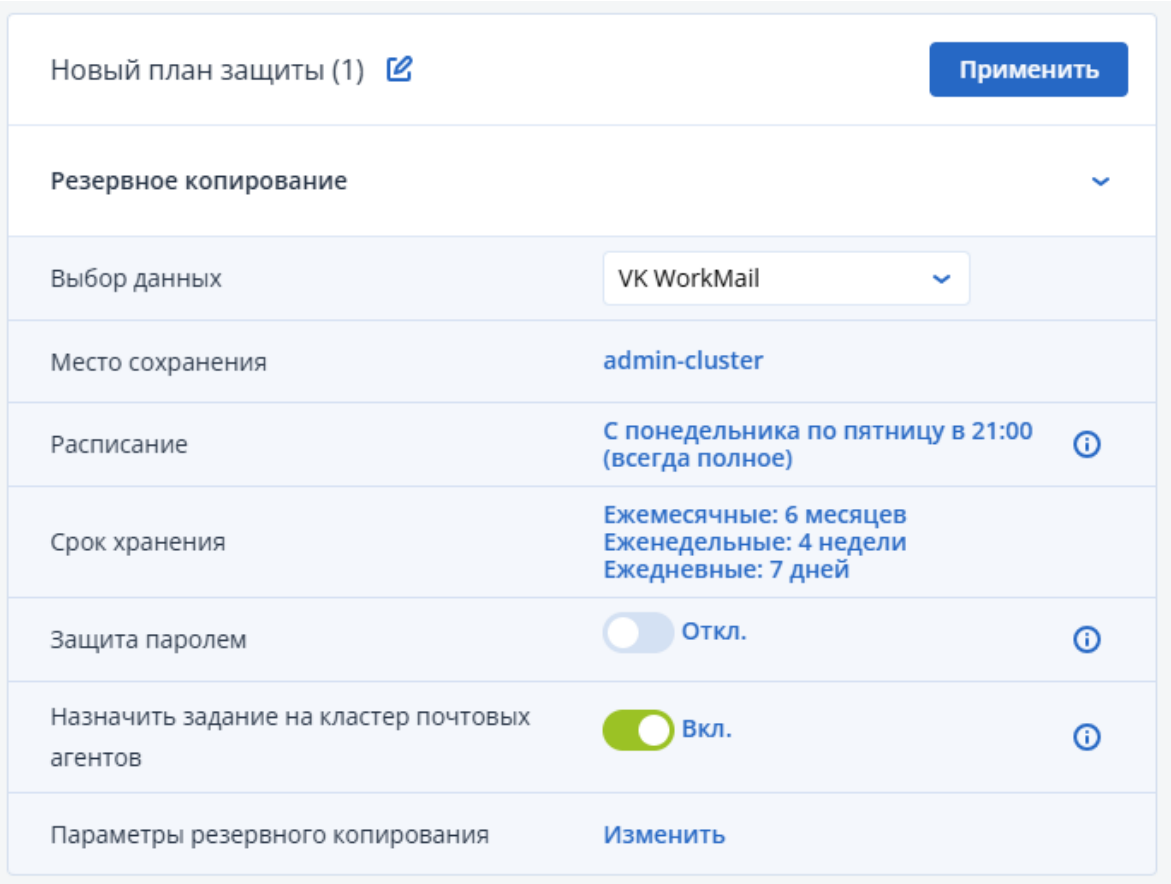
Для резервного копирования большого количества (более 6000) почтовых ящиков необходимо использовать сразу несколько агентов.

Для этого выполните следующие действия:

1. Зарегистрируйте необходимое количество агентов VK WorkMail (см. раздел "Установка VK WorkMail" (стр. 335)). Агенты должны быть версии 17.3 или новее.
2. Создайте план резервного копирования для агентов. В резервном копировании будут участвовать все агенты VK WorkMail, зарегистрированные в Кибер Бэкап Облачный.

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** -> **VK WorkMail**.
2. Выберите ресурсы VK WorkMail, 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: облачное хранилище данных, сетевая папка, папка NFS (только для Linux).

     Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 141).
   - 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.

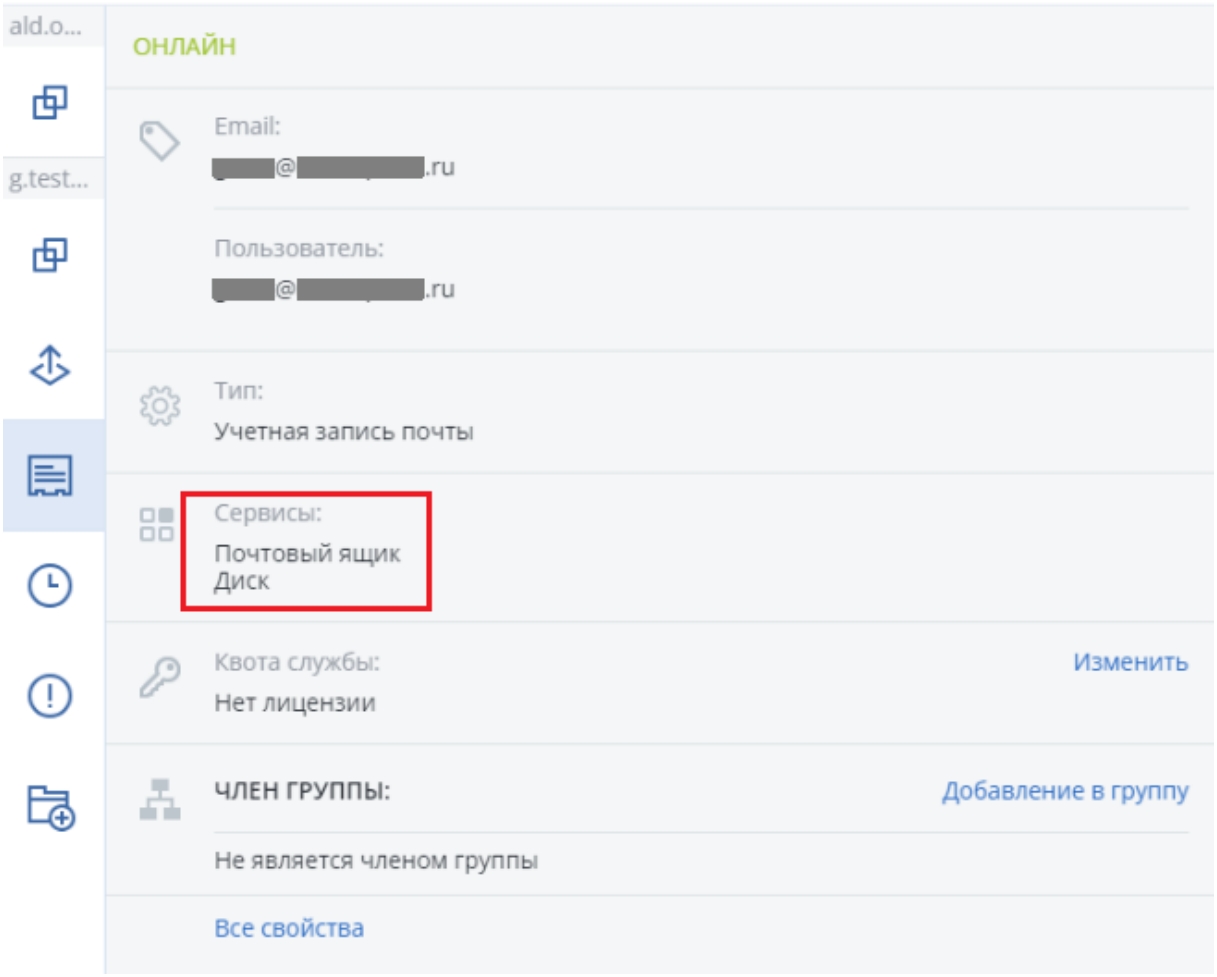
     Примечание
     Параметр «Деление» недоступен при резервном копировании в облачное хранилище данных.

5. По окончании настройки плана нажмите **Применить**.

При резервном копировании несколькими агентами балансировка нагрузки происходит в режиме циклического перебора (round robin).

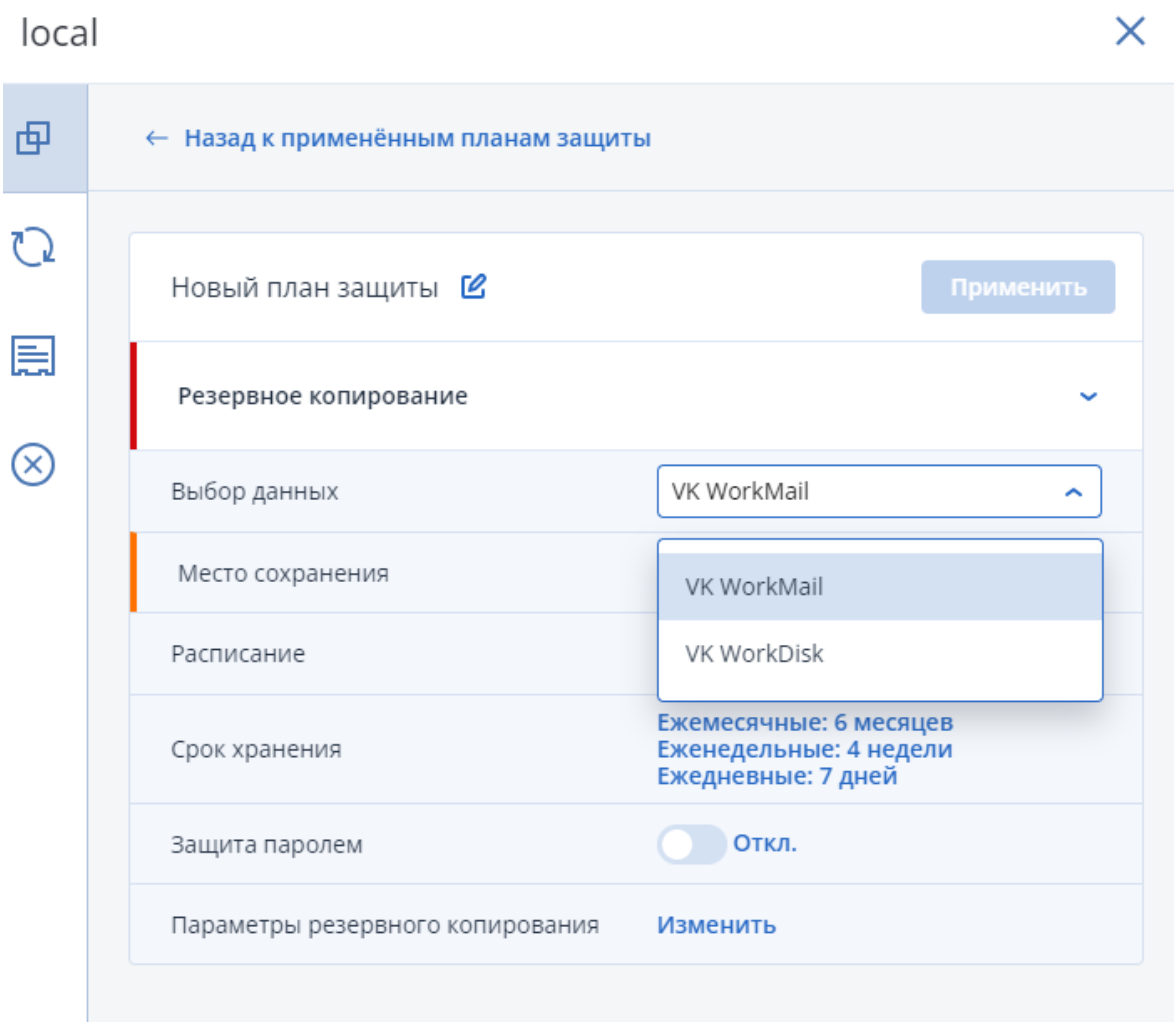
16.5.3 Резервное копирование данных пользователей VK WorkDisk

Выбор данных VK WorkDisk доступен, если у пользователя подключен сервис «Диск».



Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** -> **VK WorkMail**.
2. Выберите из списка пользователя, данные которого вы хотите защитить, и щелкните 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: облачное хранилище данных, локальная папка, сетевая папка, папка NFS.

     Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 141).
   - 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 WorkDisk выбранного пользователя.

См. также информацию в разделе "План защиты и модули" (стр. 128).

16.5.4 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:

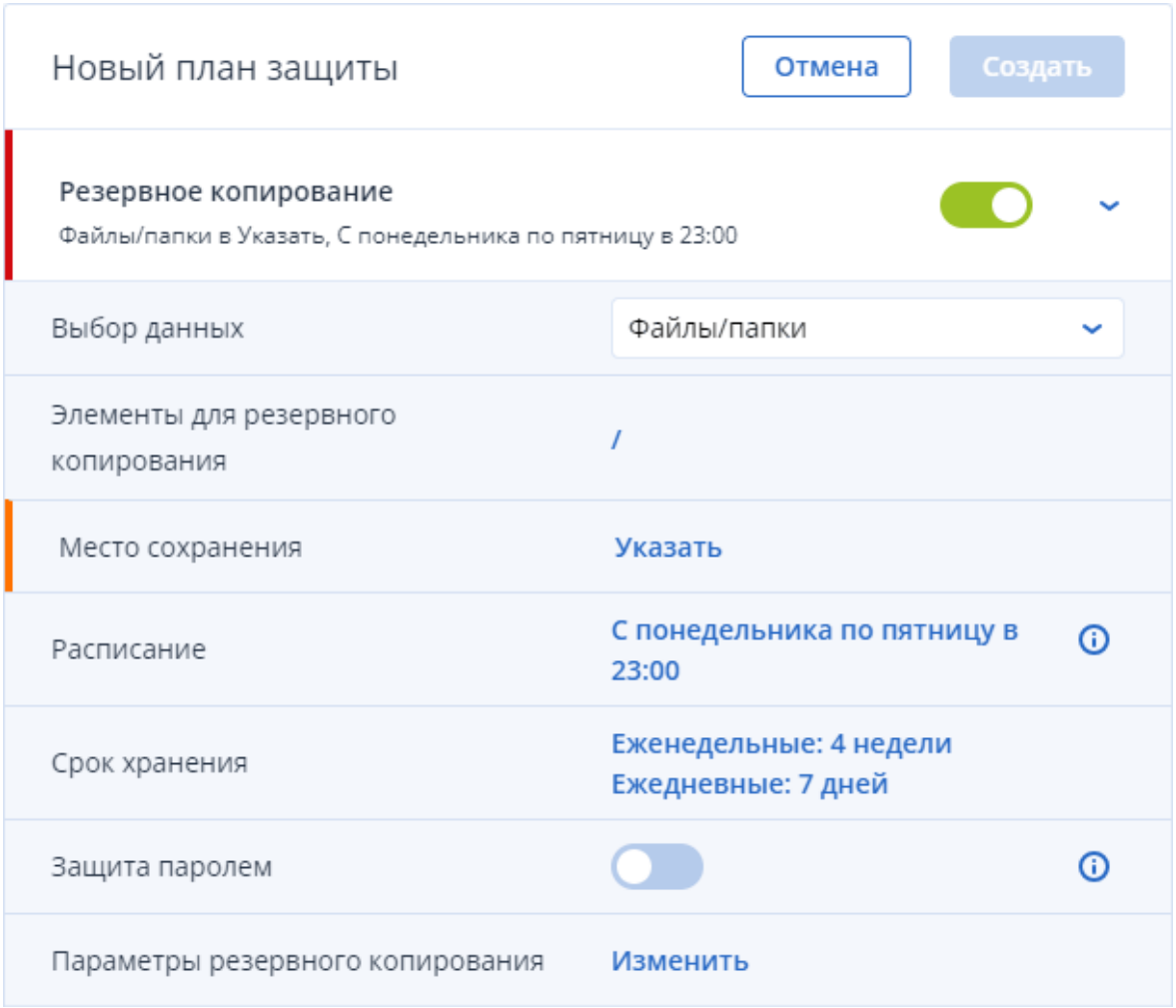
   ```
   chmod +x pre-command.sh
   ./pre-command.sh
   ```

   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** -> **Все устройства**.
6. Выберите из списка сервер VK WorkMail, который вы хотите защитить, и щелкните 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 **OK**.
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**.

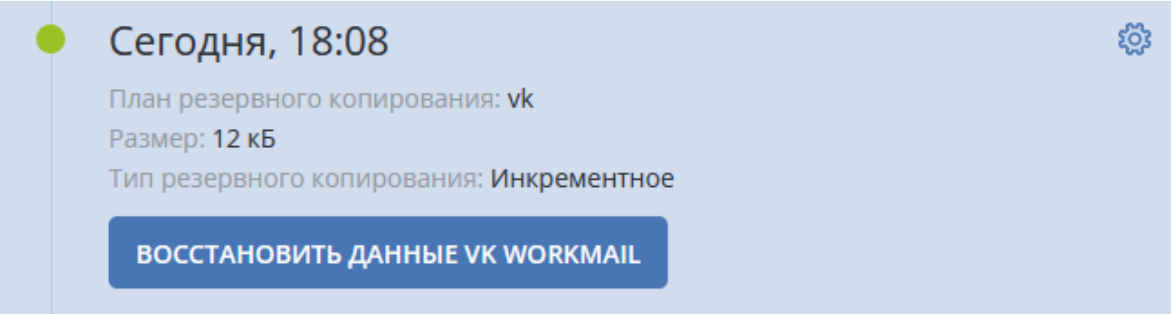
Внимание
Поскольку вы используете команды "до или после", убедитесь, что код возврата скрипта от VK является корректным. В противном случае возможна неверная интерпретация результатов резервного копирования.

16.6 Восстановление VK WorkMail и VK WorkDisk

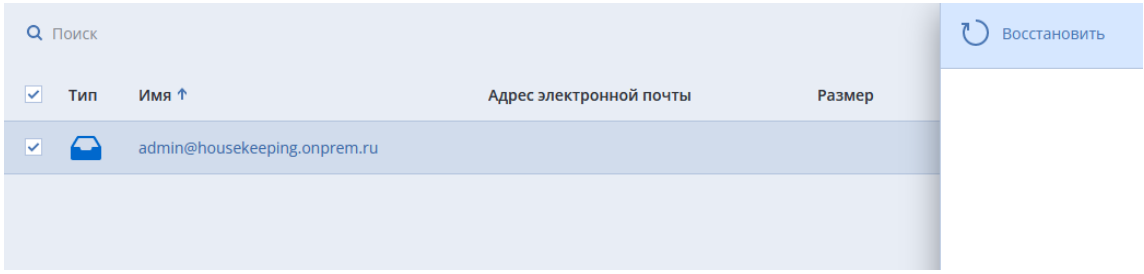
16.6.1 Восстановление данных пользователей VK WorkMail

Чтобы восстановить данные пользователей VK WorkMail, выполните следующие действия:

1. Перейдите в **Хранилище резервных копий**.
2. Выберите в списке нужную резервную копию и нажмите справа **Показать резервные копии**.
3. Нажмите **Восстановить данные VK WorkMail**.

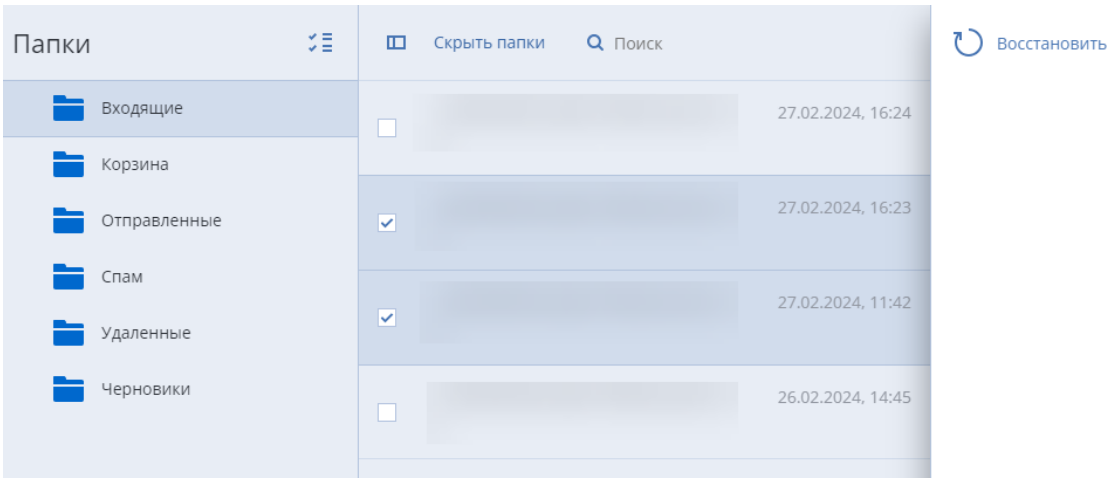


4. Выберите данные для восстановления:
   - Если необходимо восстановить весь почтовый ящик, отметьте галочкой в списке имя почтового ящика, затем выберите справа **Восстановить**.

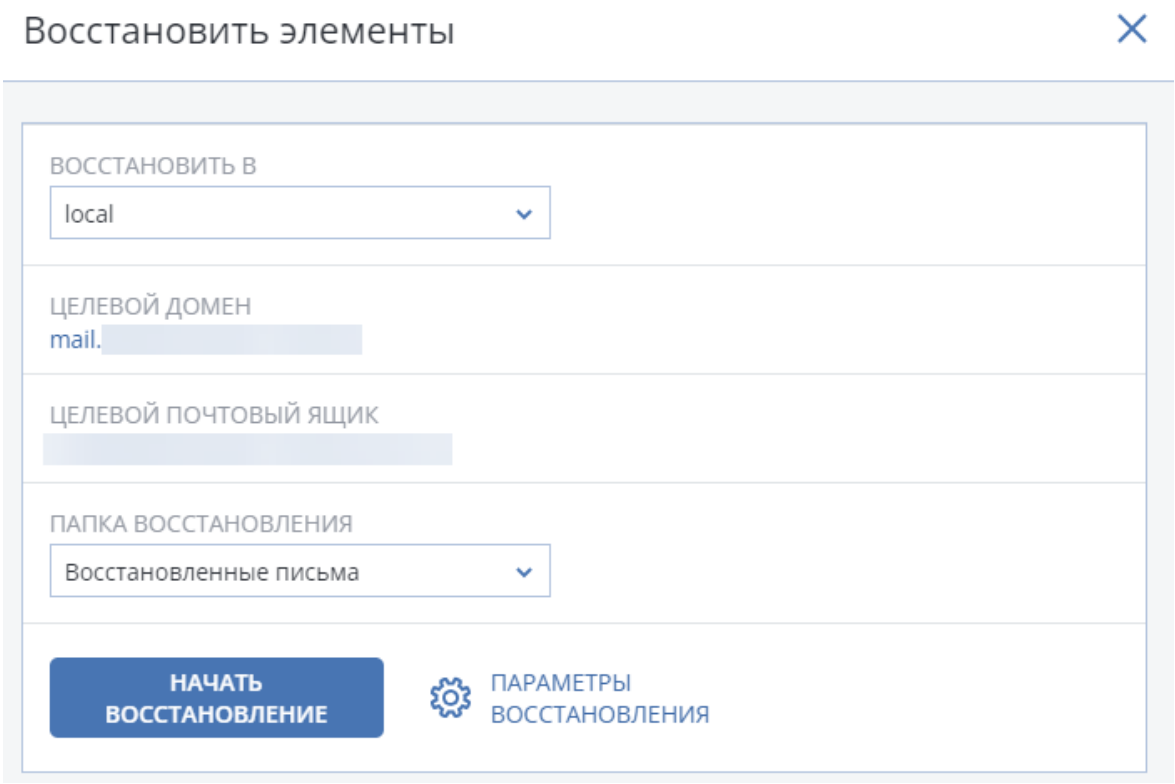


   - Если необходимо восстановить отдельные письма, нажмите на имя резервной копии и

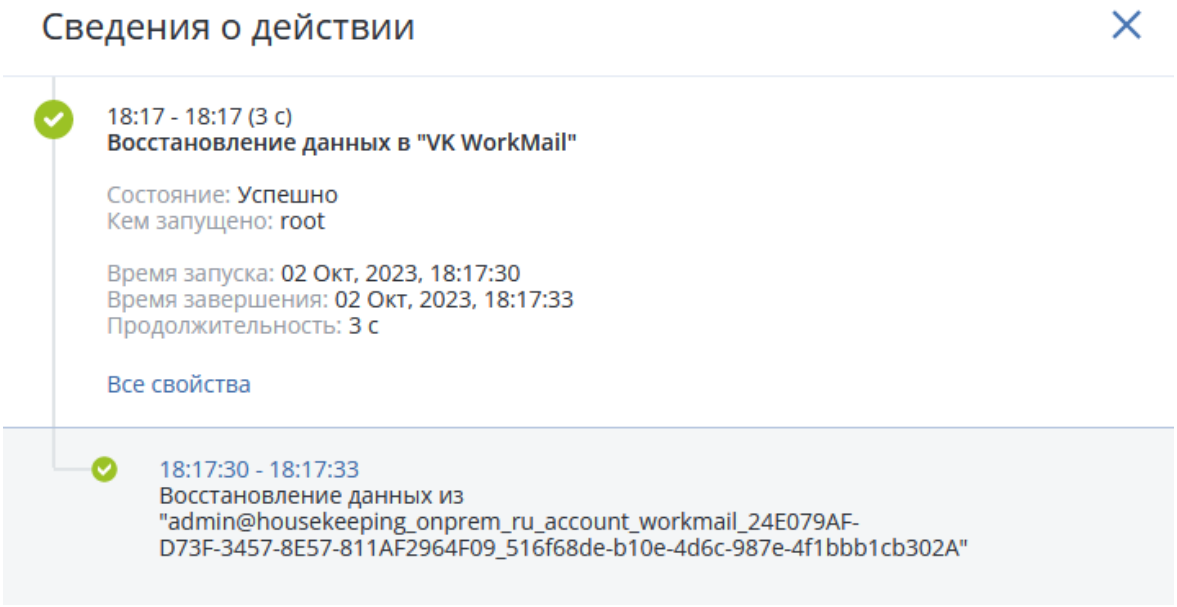
выберите письма, затем нажмите справа **Восстановить**.



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**.



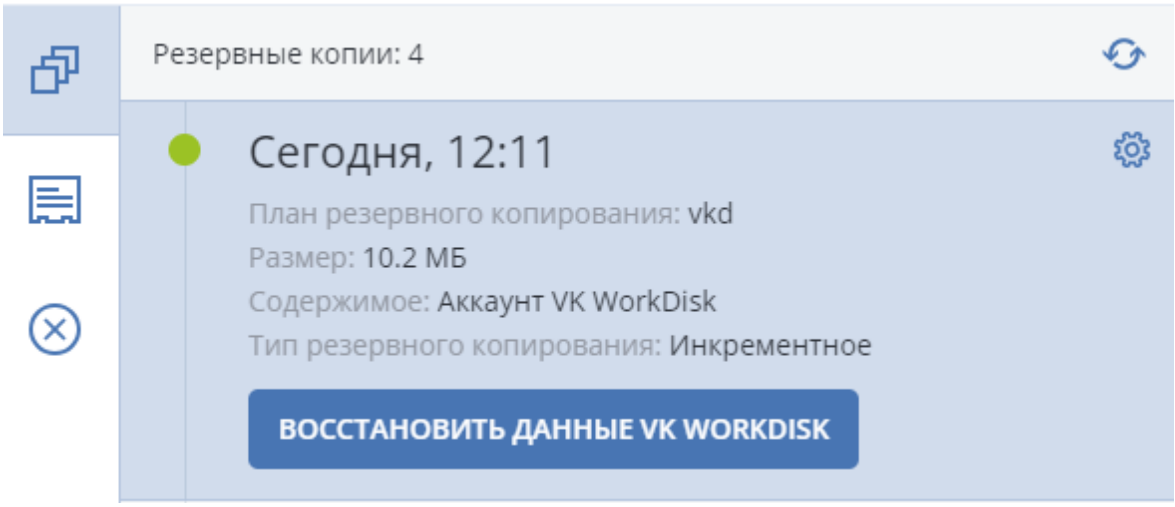
7. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.



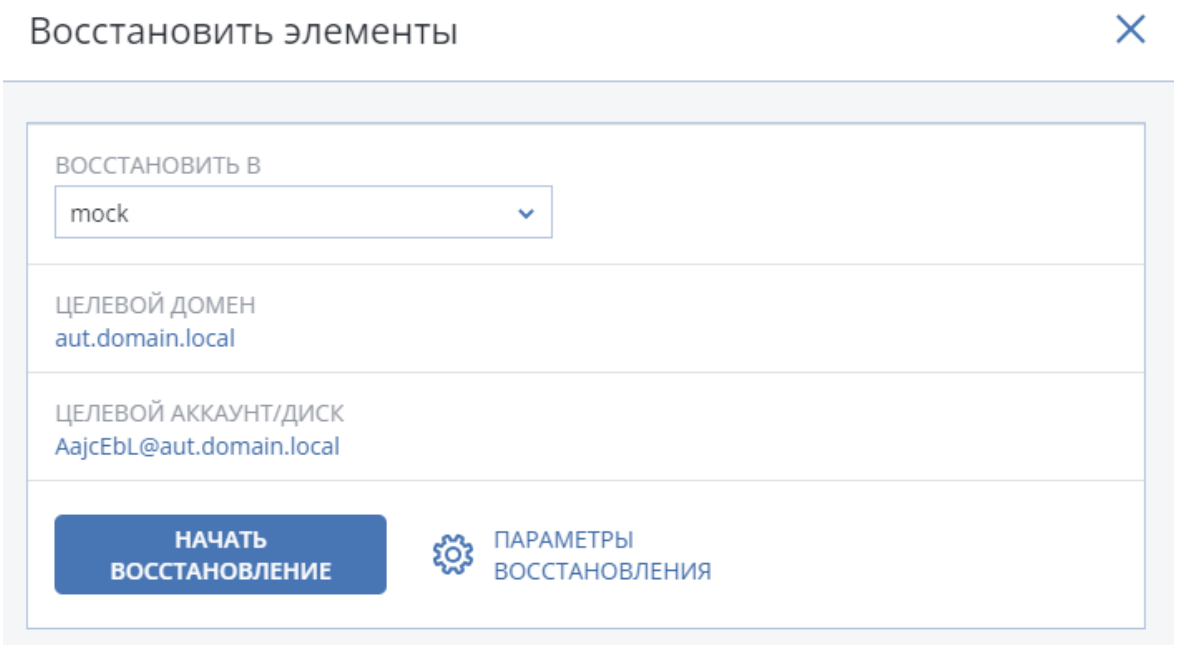
16.6.2 Восстановление данных пользователей VK WorkDisk

Чтобы восстановить данные пользователей VK WorkDisk, выполните следующие действия:

1. Перейдите в **Хранилище 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**.

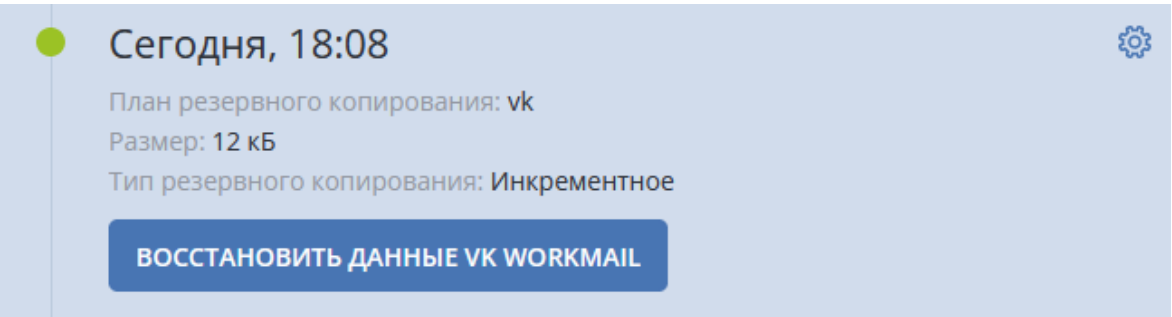


7. Процесс восстановления и результат будут отображены во вкладке **Сведения о действии**.

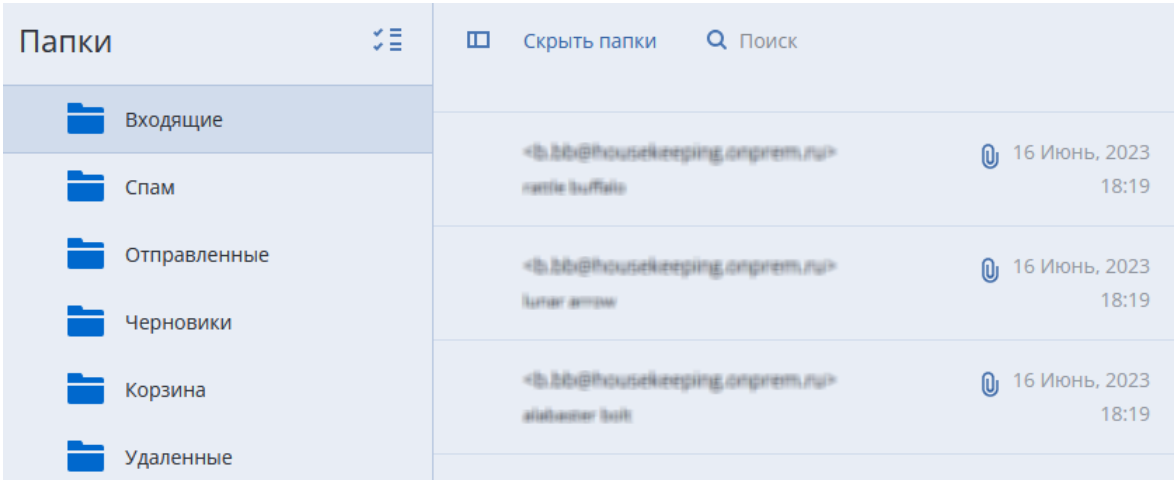
16.6.3 Просмотр писем VK WorkMail

Чтобы просмотреть письма пользователя VK WorkMail, выполните следующие действия:

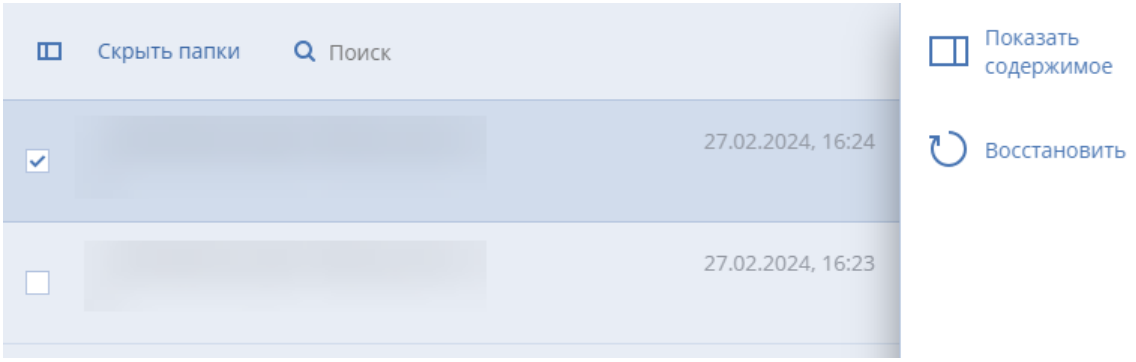
1. Перейдите в **Хранилище резервных копий**.
2. Выберите нужное хранилище, щелкните в списке нужную резервную копию.
3. Выберите справа **Показать резервные копии**.
4. Щелкните **Восстановить данные VK WorkMail**.



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**.

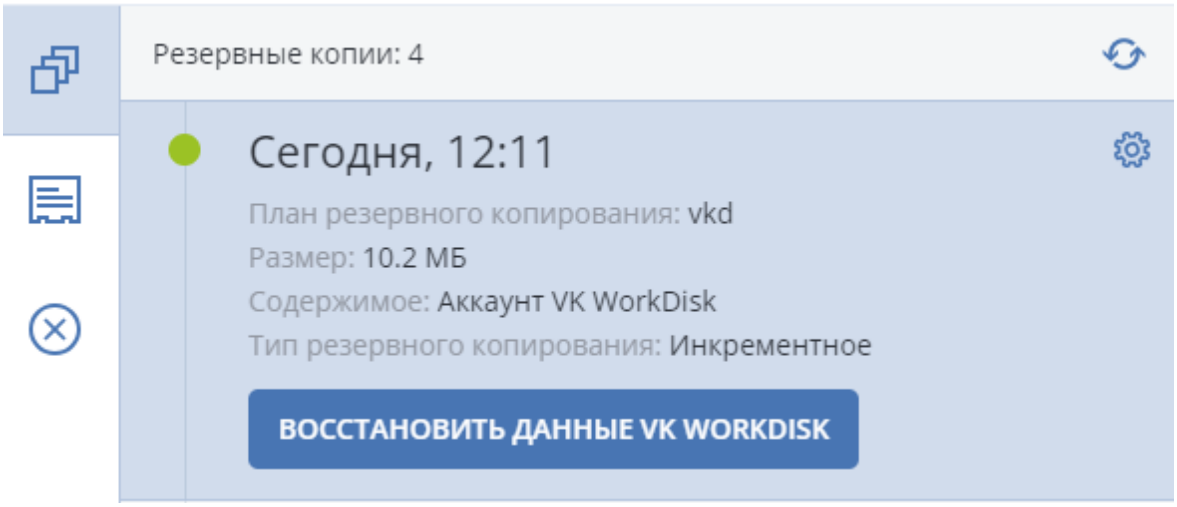


8. Для скачивания файла, приложенного к письму, щелкните по нему.

16.6.4 Скачивание файлов из архива VK WorkDisk

Чтобы скачать файлы из архива VK WorkDisk, выполните следующие действия:

1. Перейдите в **Хранилище резервных копий**.
2. Выберите нужное хранилище, щелкните 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 Облачный, используйте новую вкладку браузера, иначе скачивание файла может быть прервано.

16.6.5 Восстановление серверов VK WorkMail и VK WorkDisk

16.6.5.1 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" (стр. 348), 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 Облачный для Linux.
4. Восстановите данные в соответствующие директории, следуя шагам в разделе "Восстановление гипервизора" инструкции, предоставленной VK.

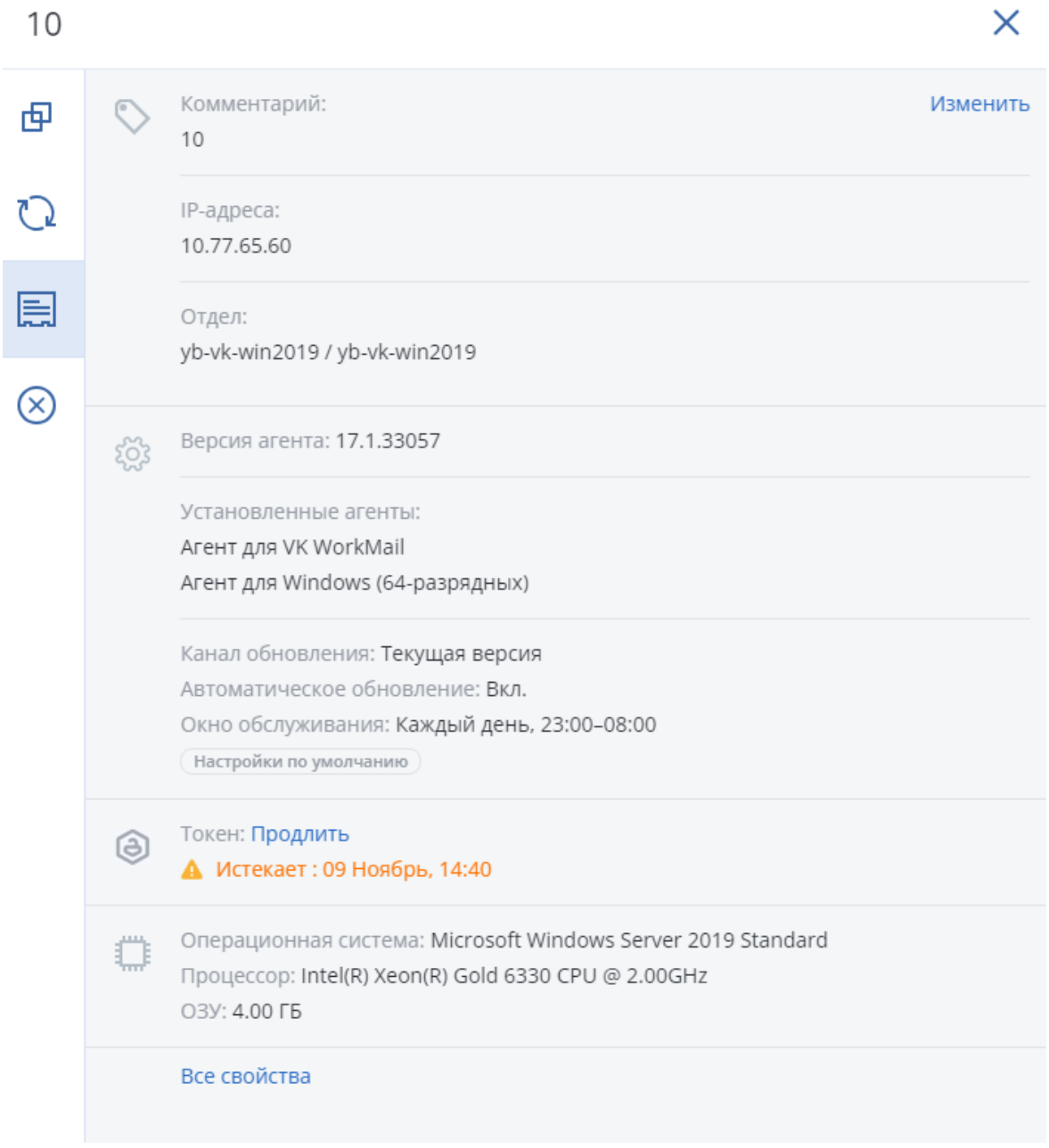
16.7 Обновление токена VK WorkMail

Для обнаружения, резервного копирования и восстановления данных устройства VK WorkMail Кибер Бэкап Облачный использует gRPC API, предоставляемый VK WorkMail, при обращениях к которому Кибер Бэкап Облачный передает токен для авторизации запросов. Токен обладает

ограниченным сроком действия, поэтому его необходимо заблаговременно обновлять. Кибер Бэкап Облачный будет оповещать пользователей за месяц до истечения срока действия токена, а также при истечении этого срока.

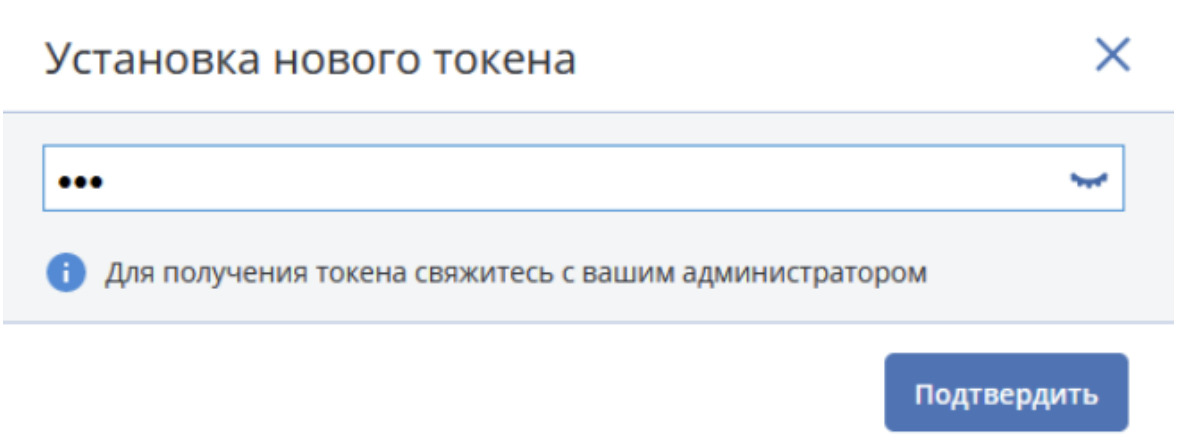
Чтобы узнать дату окончания срока действия токена и обновить его при необходимости, выполните следующие шаги:

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, щелкните **Продлить**, укажите новый токен и нажмите

Подтвердить.



17 Защита баз данных PostgreSQL

Кибер Бэкап Облачный поддерживает резервное копирование баз PostgreSQL, Postgres Pro, а также кластера PostgreSQL на базе Patroni.

Вы можете выполнять резервное копирование баз PostgreSQL следующих версий:

- PostgreSQL 11, 12, 13, 14, 15, 16
- Postgres Pro Standard 11, 12, 13, 14, 15, 16
- Postgres Pro Enterprise 11, 12, 13, 14, 15, 16
- Patroni 3.0-3.2.1
- Proxima DB 2.0, 3.0
- СУБД Jatoba (без поддержки подключения томов и гранулярного восстановления)
- СУБД Tantor

17.1 Предварительная настройка PostgreSQL

17.1.1 Создание учетной записи пользователя на сервере PostgreSQL

Создайте учетную запись пользователя на сервере PostgreSQL, с помощью которой Кибер Бэкап Облачный 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.

17.1.2 Настройка аутентификации в PostgreSQL

Чтобы настроить соединение между Кибер Бэкап Облачный 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.

17.1.2.1 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).

17.1.2.2 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 Облачный, укажите метод аутентификации trust.

За более подробной информацией о конфигурационном файле pg_hba.conf обратитесь к официальной документации PostgreSQL (например, файл pg_hba.conf).

17.1.2.3 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
```

После внесения изменений в файлы конфигурации перезапустите службу PostgreSQL:

```
systemctl restart postgresql
```

17.2 Установка и настройка

Установка и настройка включает в себя следующие шаги:

1. Установка агента Кибер Бэкап Облачный для операционной системы, которую вы используете (агент Windows или агент Linux), а также агента PostgreSQL.
2. Добавление в веб-консоли Кибер Бэкап Облачный устройства PostgreSQL.

17.2.1 Установка агентов для PostgreSQL

Для установки агента для операционной системы, которую вы используете (агент Windows или агент Linux), и агента PostgreSQL обратитесь к разделу "Установка агентов" (стр. 43).

Агент PostgreSQL может быть установлен как на сервер, на котором находятся базы PostgreSQL, так и на другую машину.

Если вы устанавливаете агент 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.

17.2.2 Добавление в веб-консоли Кибер Бэкап Облачный устройства PostgreSQL

1. В веб-консоли Кибер Бэкап Облачный перейдите **Все устройства** > **Добавить** и выберите приложение:
   a. Если необходимо добавить сервер PostgreSQL, в списке **Приложения** выберите **PostgreSQL**.
   b. Если необходимо добавить кластер PostgreSQL, в списке **Приложения** выберите **Кластер PostgreSQL Patroni**.
2. Укажите настройки соединения с PostgreSQL:
   a. Введите имя хоста или IP-адрес сервера PostgreSQL и порт подключения (по умолчанию для сервера PostgreSQL используется порт 5432, для кластера PostgreSQL – порт 8008), имя пользователя и пароль учетной записи для подключения к PostgreSQL и нажмите кнопку **Добавить**.
   b. Убедитесь, что при настройке параметров аутентификации вы настроили метод аутентификации trust.

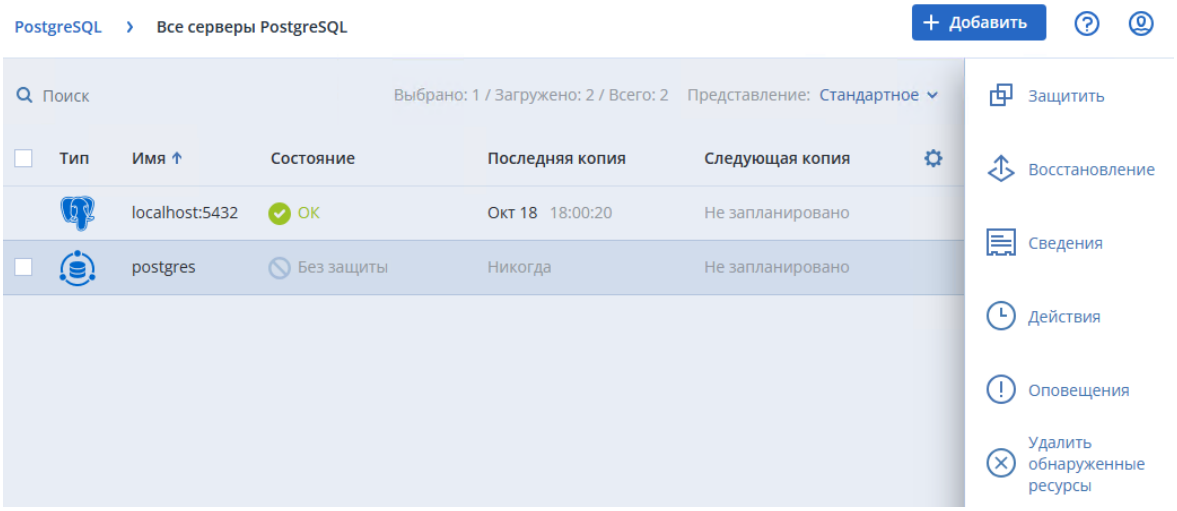
В списке устройств отобразится раздел PostgreSQL с добавленным сервером или кластером.

Для кластера PostgreSQL в разделе **Сведения** отобразится информация об IP-адресах/именах узлов, доступность (Online/Offline) и статусы узлов (Leader/Replica).

17.3 Резервное копирование PostgreSQL

Для создания плана защиты выполните следующие действия:

1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите сервер PostgreSQL, который вы хотите защитить.
3. Перейдите на вкладку справа **Защитить**.

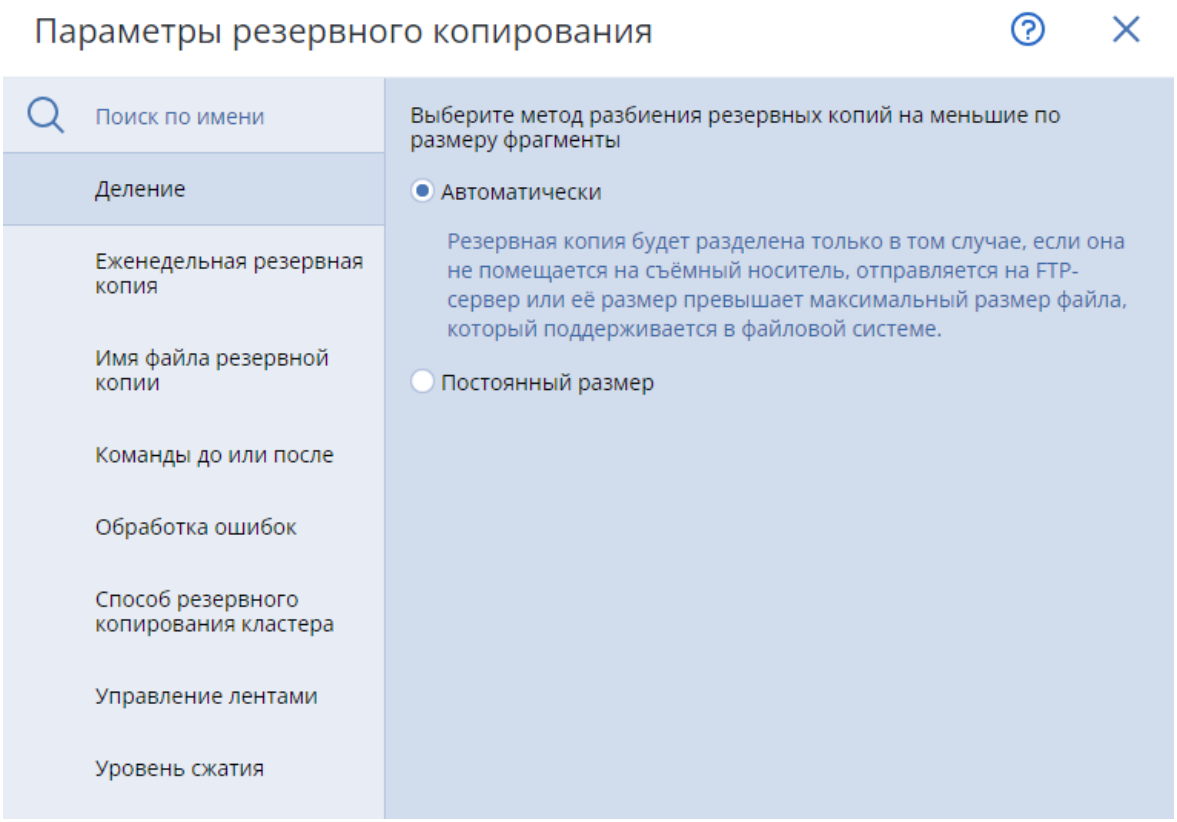


4. В поле **Место сохранения** нажмите **Указать** и выберите место хранения резервных копий. Выберите существующее хранилище или нажмите **Добавить хранилище** и укажите другое. Возможные варианты хранения резервных копий: локальная папка, сетевая папка, облачное хранилище, папка NFS.

   Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 141).
5. В поле **Расписание** укажите схему и периодичность выполнения резервного копирования. В текущей версии доступны полное резервное копирование и инкрементное резервное копирование.
   Подробнее см. в разделе "Расписание" (стр. 146).
6. В поле **Срок хранения** укажите срок хранения резервных копий и правила очистки хранилища.
   Подробнее см. в разделе "Правила хранения" (стр. 159).
7. При необходимости защитите резервные копии 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.

     Примечание
     Параметр недоступен при резервном копировании в облачное хранилище данных.

- **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.
- **Обработка ошибок**. Укажите порядок обработки ошибок, возникающих при резервном копировании.
- **Способ резервного копирования кластера**. Подробнее см. в разделе "Способ резервного копирования кластера" (стр. 187).
- **Уровень сжатия**. Укажите уровень сжатия данных при резервном копировании.



Подробнее см. в разделе "Параметры резервного копирования" (стр. 178).

9. Нажмите **Применить**. Новый план защиты появится в списке планов.

В результате вы сможете:

- Выполнять резервное копирование баз PostgreSQL. Подробнее см. в разделе "Резервное копирование и восстановление" (стр. 132).
- Выполнять восстановление баз PostgreSQL из резервных копий.

17.4 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.

17.4.1 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:

```
aakore restart
```

Для подключения экземпляра базы данных 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 **Хранилище 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.

17.5 Восстановление баз данных PostgreSQL

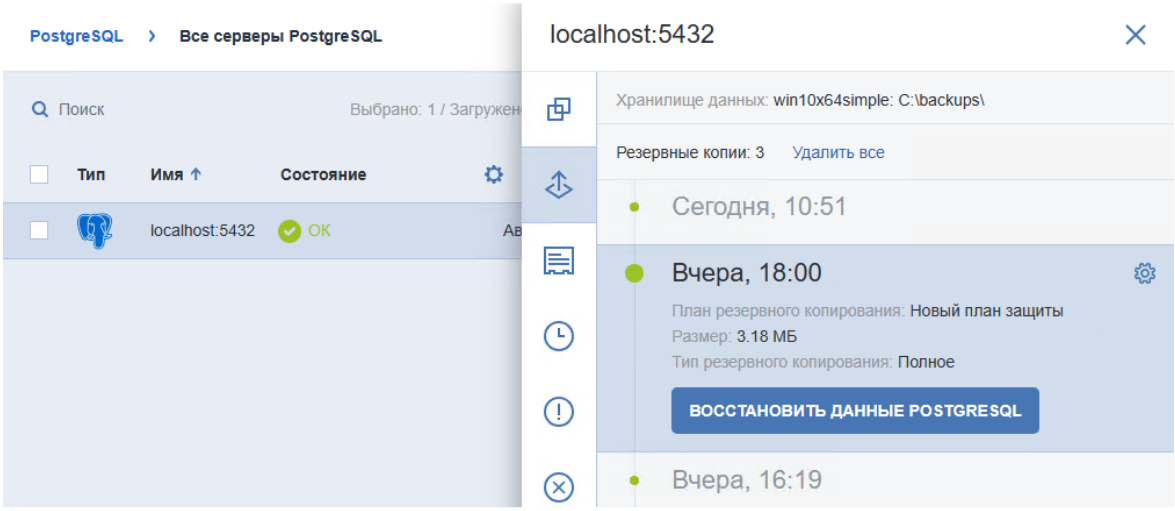
Для восстановления всего экземпляра базы данных PostgreSQL:

1. Перейдите в **Устройства** > **PostgreSQL**.
2. Выберите экземпляр PostgreSQL, который нужно восстановить.

3. Перейдите на вкладку справа **Восстановление**.

> **Примечание**
> Либо перейдите в **Хранилище 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, проверьте остальные настройки и нажмите **Начать восстановление**.

Ход выполнения восстановления показан на вкладке **Действия**.

17.5.1 Гранулярное восстановление отдельных баз данных PostgreSQL

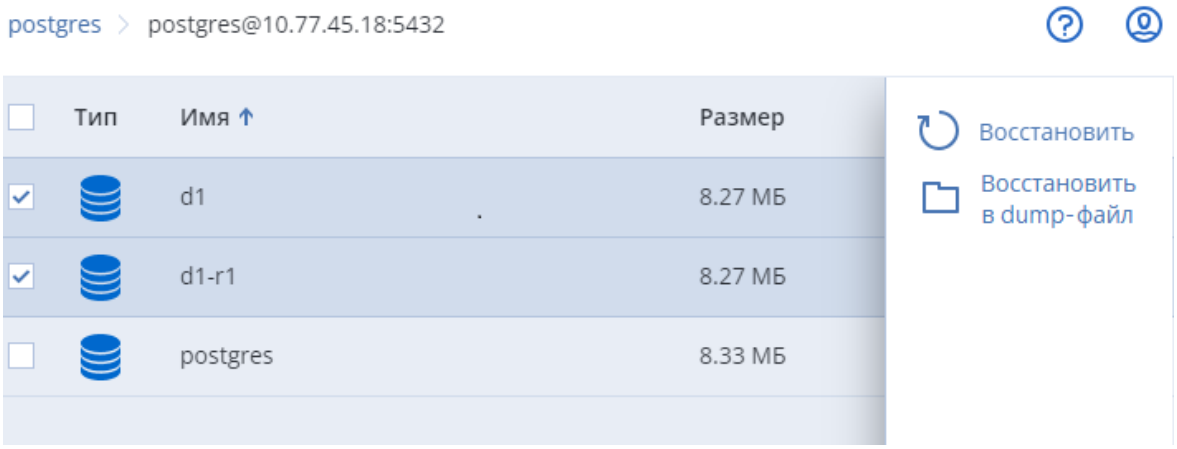
Гранулярное восстановление доступно только для баз данных PostgreSQL, установленных на машинах под управлением ОС Linux. Доступно восстановление отдельных баз данных из единого архива резервной копии.

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 **Хранилище резервных копий**, выберите необходимое хранилище и перейдите на вкладку справа **Показать резервные копии**.

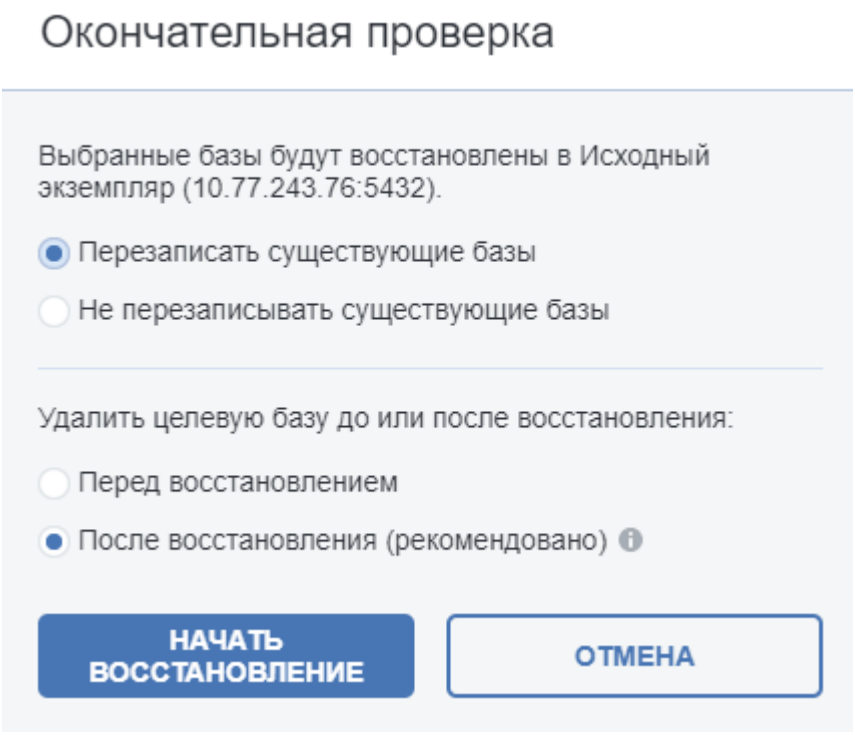
4. Нажмите на имя резервной копии и выберите необходимые для восстановления базы из архива.



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 с момента создания резервной копии.
   - Экземпляр базы данных PostgreSQL, куда будет происходить восстановление.

     Примечание
     Версия экземпляра PostgreSQL, куда будет происходить восстановление, должна быть не ниже восстанавливаемой. Редакции экземпляров баз данных должны совпадать. Экземпляр базы данных, 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 с момента создания резервной копии.
   - 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**.

17.6 Ограничения

- Не поддерживается гранулярное восстановление на машинах под управлением ОС Windows.

17.7 Известные проблемы и их решения

17.7.1 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')

18 Защита Kubernetes

Кибер Бэкап Облачный позволяет выполнять резервное копирование и восстановление пространств имен, групп пространств имен и постоянных томов кластеров Kubernetes версии 1.24 или выше.

Для резервного копирования данных кластера Kubernetes:

- В кластере Kubernetes должны быть установлены CSI-драйвер с поддержкой функций Snapshot и Raw Block и контроллер моментальных снимков томов (см. раздел "Предварительная настройка Kubernetes" (стр. 370)).
- 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 Облачный" (стр. 386)).

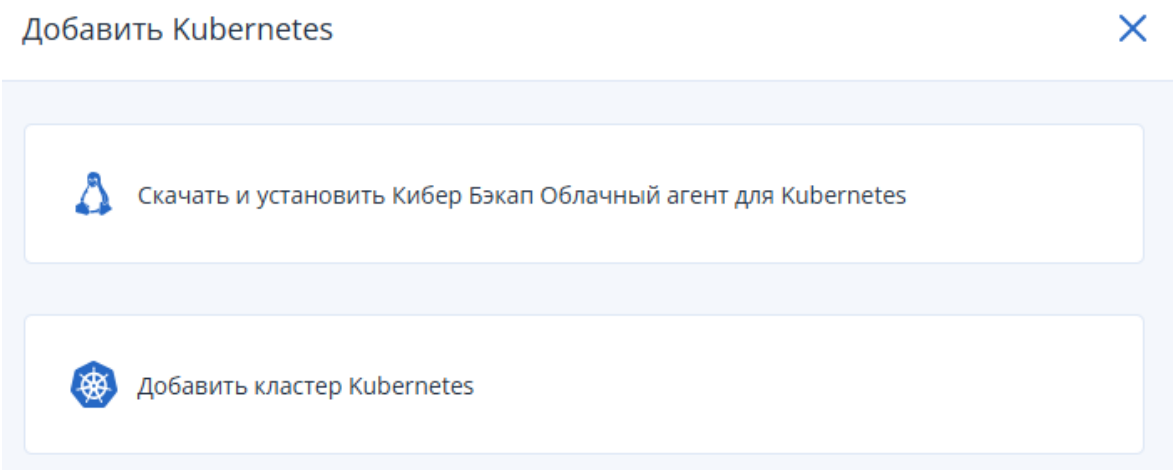
Для выполнения резервного копирования требуется установка агента (см. раздел "Установка агента для Kubernetes" (стр. 369)).

18.1 Установка агента для Kubernetes

Список поддерживаемых операционных систем Linux см. в разделе "Поддерживаемые операционные системы и среды" (стр. 16).

Чтобы установить агент для Kubernetes:

1. В веб-консоли Кибер Бэкап Облачный перейдите в раздел **Устройства** > **Физические и виртуальные машины**.
2. Справа вверху щелкните **Добавить** и в разделе **Хосты виртуализации** выберите **Kubernetes**.
3. Выберите **Скачать и установить Кибер Бэкап Облачный агент для Kubernetes** и укажите место сохранения установщика.



4. Запустите установщик Кибер Бэкап Облачный от имени привилегированного пользователя на сервере, на котором планируете установить агент.

5. Следуя инструкциям на экране, установите агент для Kubernetes и, если необходимо, прочие компоненты.

Если агенту не удалось подключиться к серверу управления, выполните это подключение вручную, как описано в статье Ручная регистрация агента на сервере управления.

18.2 Предварительная настройка Kubernetes

Перед добавлением кластера в Кибер Бэкап Облачный подготовьте его, как описано в этом разделе.

18.2.1 Требования к CSI-драйверу

В кластере должен быть установлен CSI-драйвер с поддержкой функций Snapshot и Raw Block. Список CSI-драйверов и сведения о поддерживаемых ими функциях см. в документации Kubernetes.

18.2.2 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.

18.2.3 Настройка для защиты пользовательских пространств имен Kubernetes

18.2.3.1 Создание учетной записи 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:
  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: [""]
  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
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: ["*"]
  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
  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. Получите и сохраните токен служебной учетной записи cyberprotect:

```
kubectl -n cyberprotect describe secret cyberprotect
```

18.2.3.2 Подготовка конфигурационного файла kubeconfig

1. Загрузите на рабочую машину конфигурационный файл kubeconfig по умолчанию. Путь к конфигурационному файлу 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 при создании 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
  name: myk8scluster
contexts:
- context:
    cluster: myk8scluster
    user: cyberprotect
  name: default
current-context: default
kind: Config
preferences: {}
users:
- name: cyberprotect
```

```
user:
  token: <...>
```

18.2.4 Настройка для защиты системных пространств имен Deckhouse

18.2.4.1 Создание учетной записи для агента Kubernetes

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

   Type:  kubernetes.io/service-account-token

   Data
   ====
   ca.crt:     1107 bytes
   namespace:  9 bytes
   token:      <...>
   ```

18.2.4.2 Подготовка конфигурационного файла kubeconfig

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 при создании учетной записи для агента Kubernetes.

3. Сохраните внесенные изменения.

Пример файла, который должен получиться в итоге:

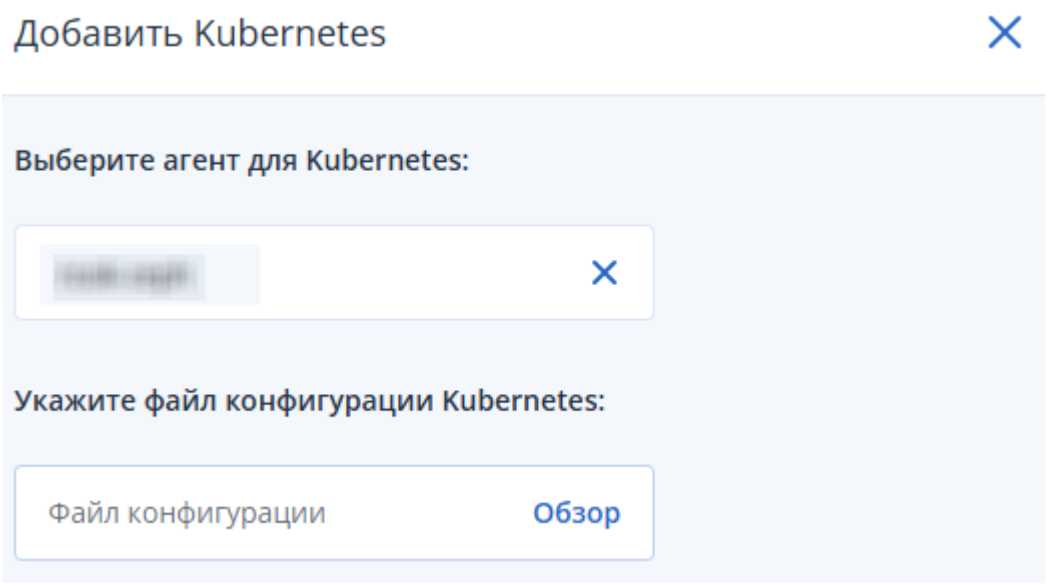
```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data: <...>
    server: https://10.11.12.13:6443
  name: deckhouse
contexts:
- context:
    cluster: deckhouse
    user: deckhouse
  name: deckhouse@deckhouse
current-context: deckhouse@deckhouse
kind: Config
preferences: {}
users:
- name: deckhouse
  user:
    token: <...>
```

18.3 Добавление кластера Kubernetes

Добавьте кластер Kubernetes в Кибер Бэкап Облачный:

1. В веб-консоли Кибер Бэкап Облачный перейдите в раздел **Устройства** > **Физические и виртуальные машины**.
2. Справа вверху щелкните **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 "Предварительная настройка Kubernetes" (стр. 370).

   Для подключения к кластеру Kubernetes файл конфигурации должен содержать адрес кластера, имя пользователя и токен.



5. После заполнения полей нажмите **Добавить** и дождитесь окончания установки.

В веб-консоли перейдите в раздел **Устройства** и убедитесь, что кластер Kubernetes добавлен в вашу конфигурацию.

В веб-консоли перейдите в раздел **Настройки** > **Агенты** и убедитесь, что агент для Kubernetes отображается в списке агентов.

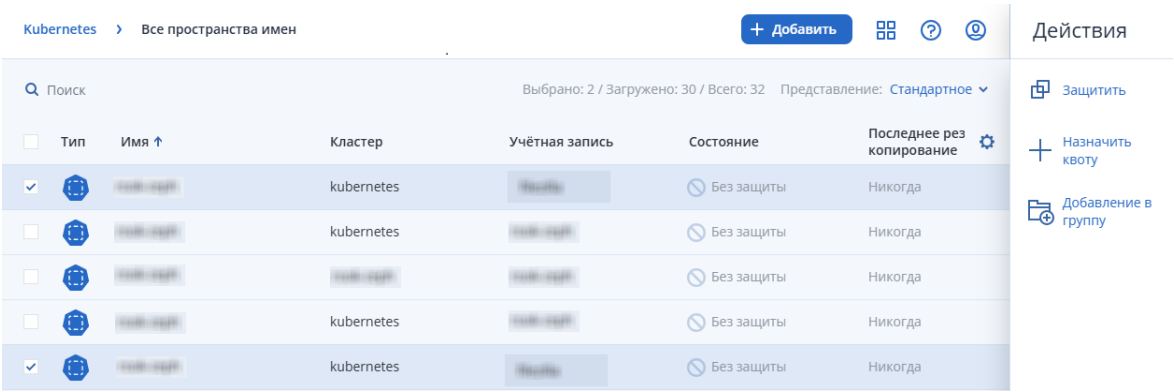
18.4 Резервное копирование Kubernetes

18.4.1 Создание плана защиты

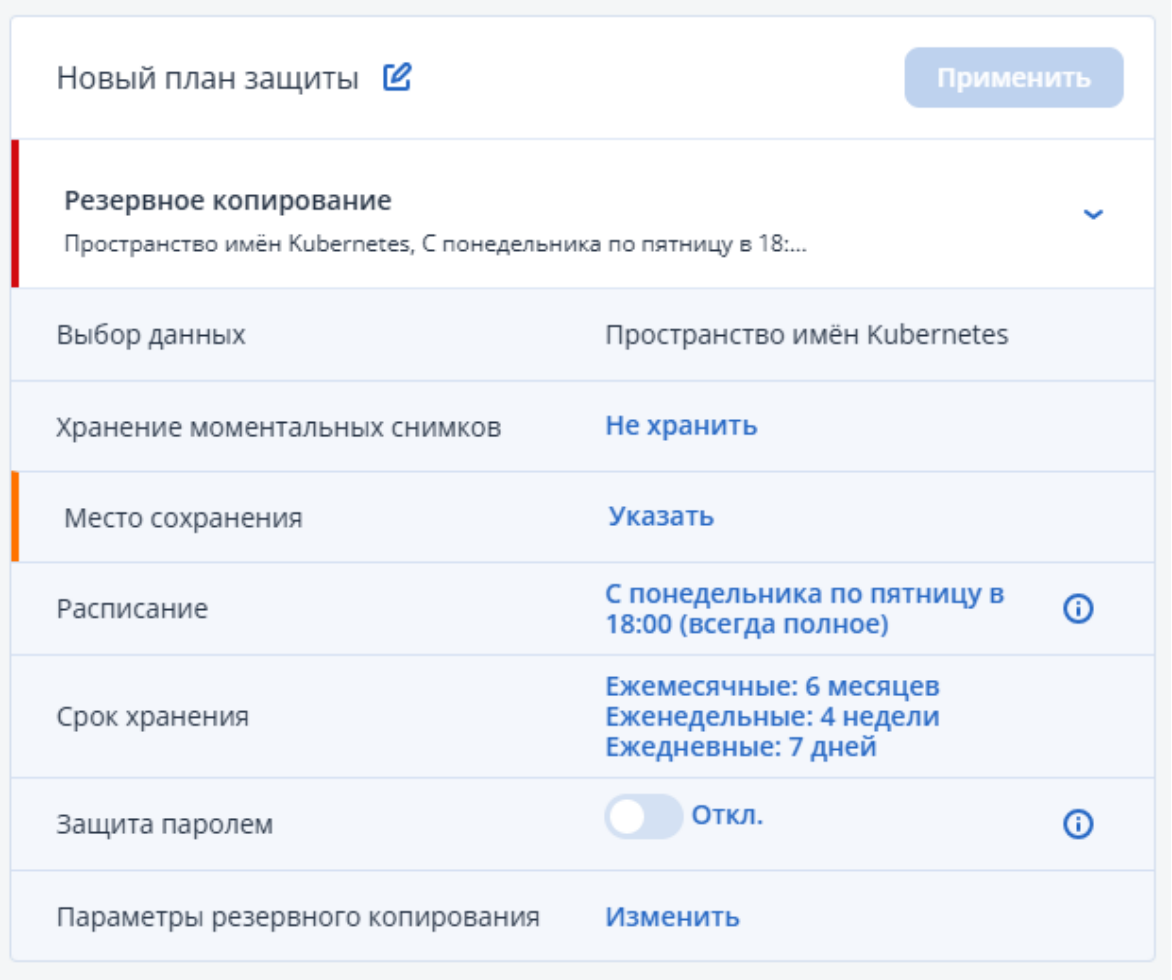
Создание плана защиты из веб-консоли возможно двумя способами: через пункт веб-консоли **Устройства** и через пункт **Планы** (см. также "Создание плана защиты" (стр. 128)).

Создание плана через пункт веб-консоли Устройства

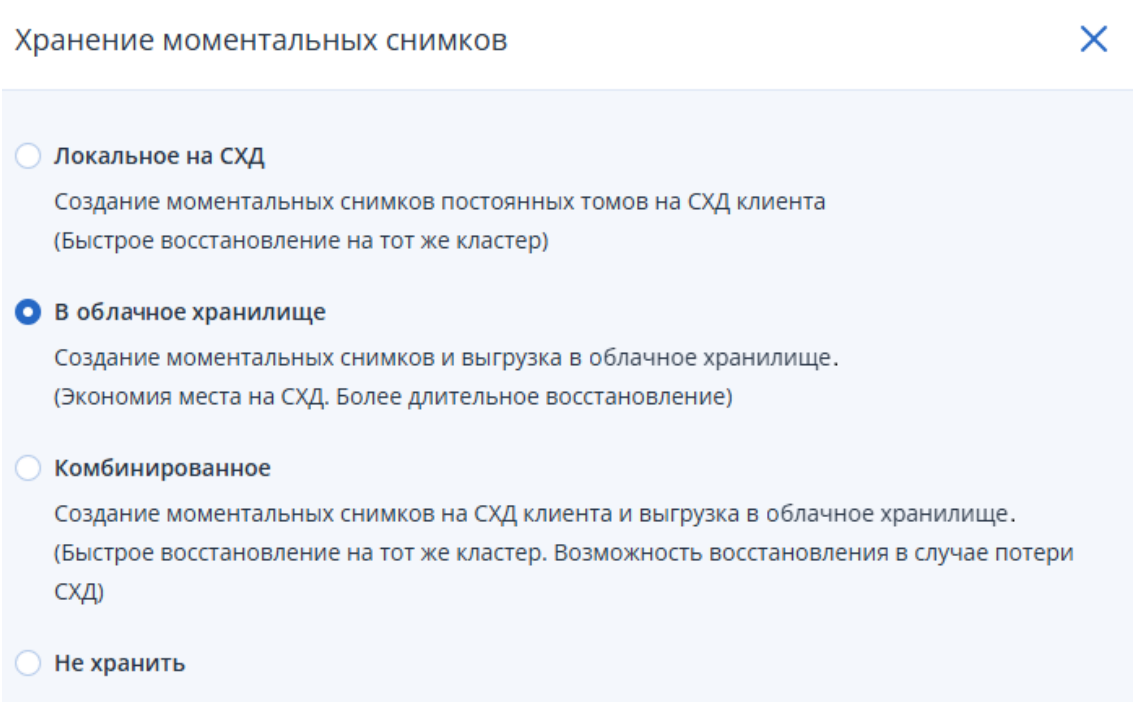
1. В веб-консоли Кибер Бэкап Облачный перейдите в раздел **Устройства** > **Kubernetes**.
2. Выберите пространства имен (или группу с пространствами имен) для защиты.



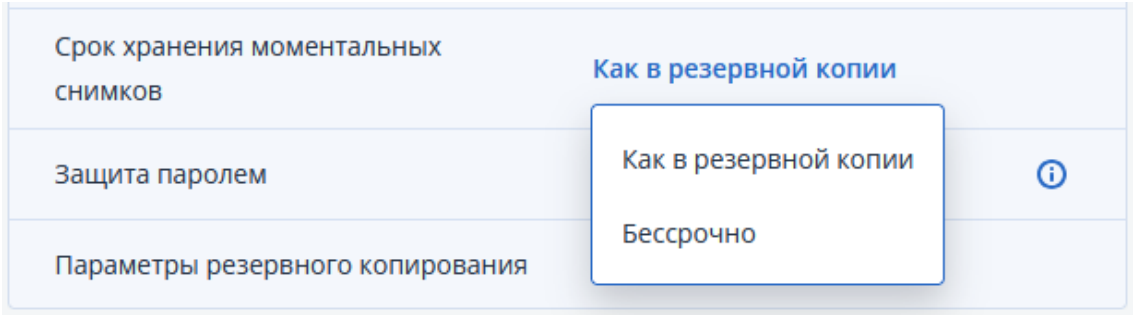
3. Нажмите справа вверху **Защитить** для защиты узла Kubernetes или **Защитить группу** для защиты группы пространств имен.
4. Щелкните **Создать план**.
5. Выберите необходимые вам настройки плана защиты, заполнив соответствующие поля:



   a. **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**.



b. **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: облачное хранилище, локальная папка, сетевая папка, папка NFS.

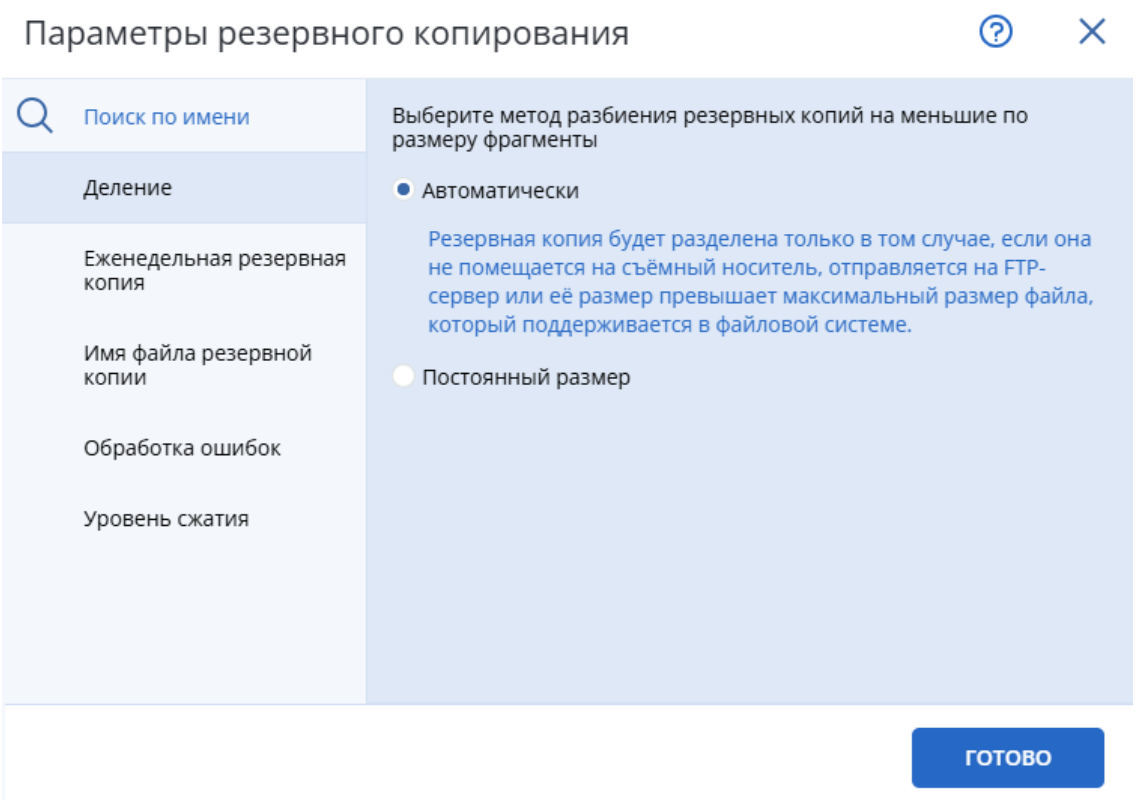
   Подробнее о выборе места хранения резервных копий см. в разделе "Выбор места назначения" (стр. 141).

c. [Необязательно] **Расписание**. Задайте расписание резервного копирования.

d. [Необязательно] **Срок хранения**. Укажите срок хранения резервных копий.

e. [Необязательно] **Защита паролем**. Активируйте защиту паролем при необходимости.

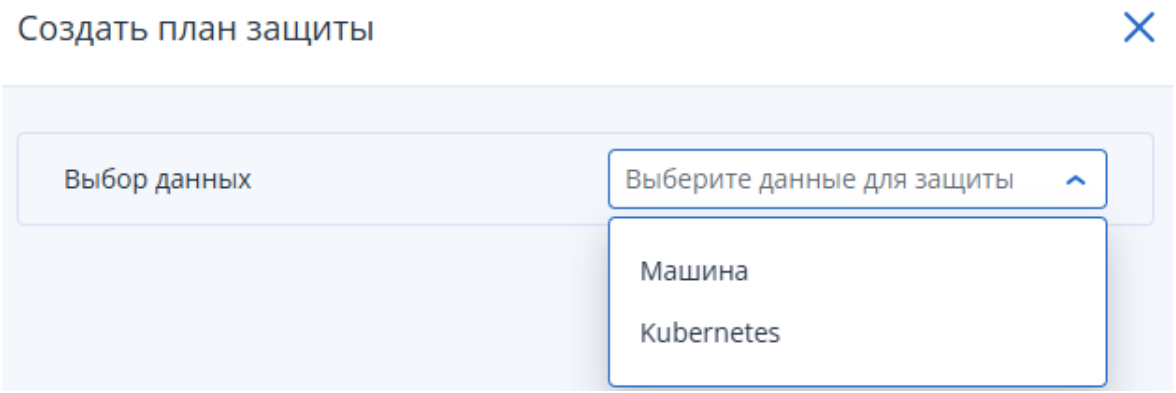
f. [Необязательно] **Параметры резервного копирования**. Выберите параметры резервного копирования (см. также "Параметры резервного копирования" (стр. 178)).



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**.



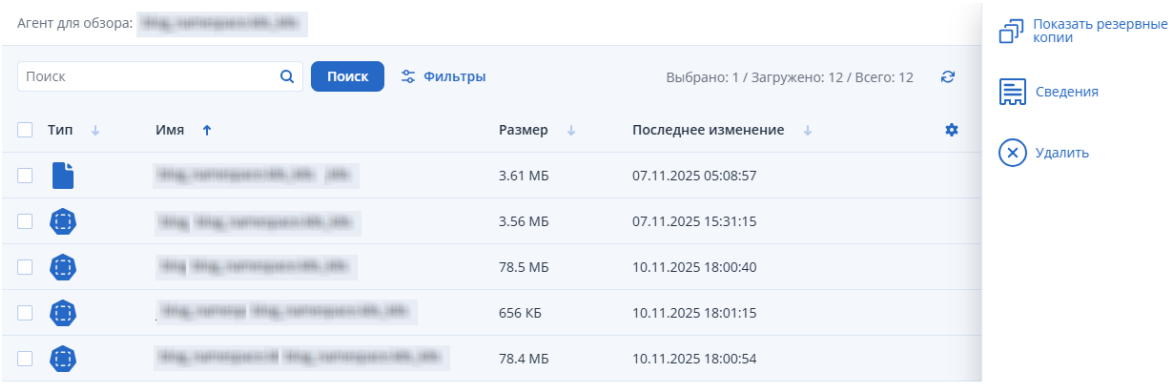
4. В окне создания плана настройте план нужным вам образом и нажмите **Создать**.

18.5 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 щелкните **Восстановить все пространство**.

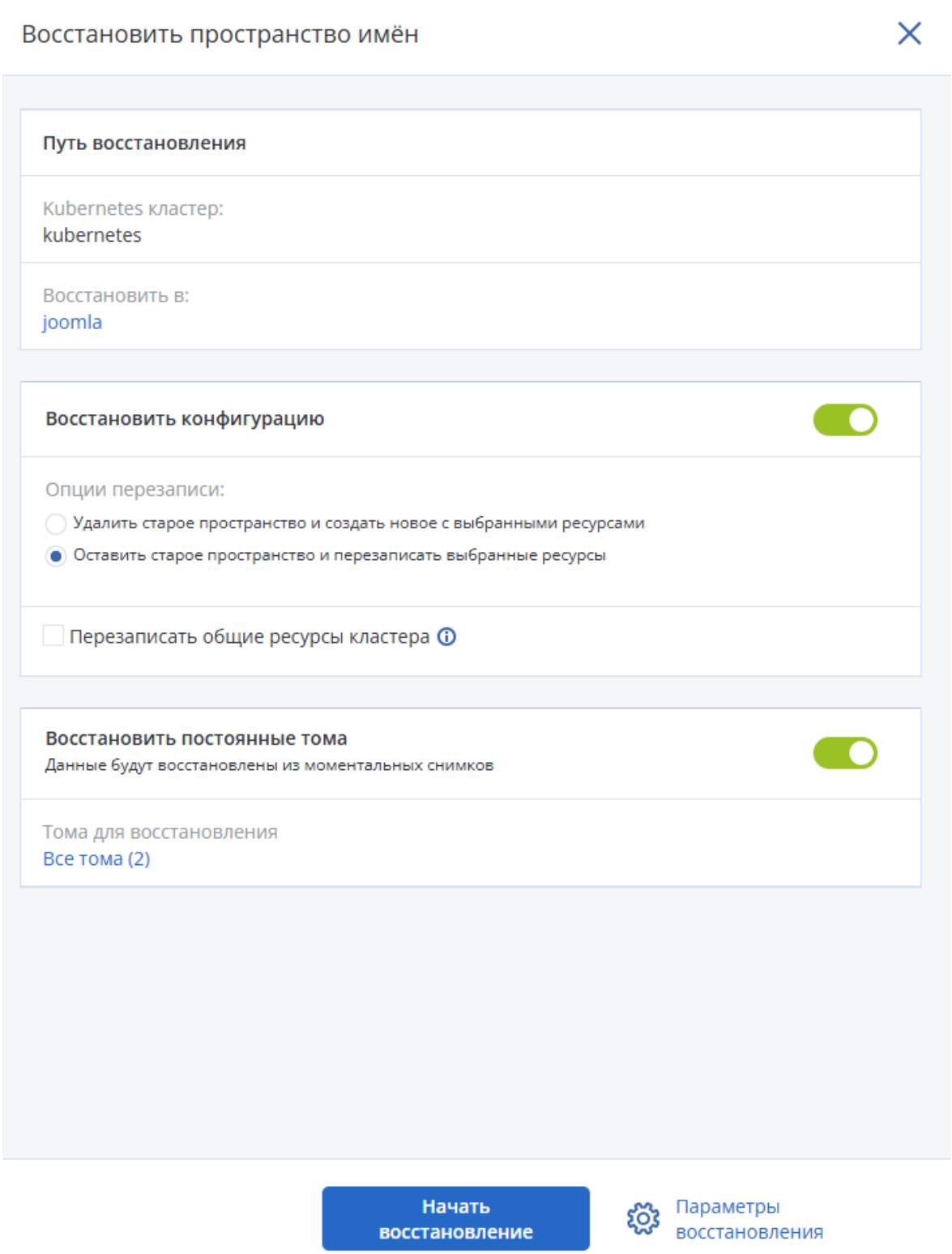
   Для просмотра списка постоянных томов щелкните **Постоянные тома**.

   Для просмотра сведений о конфигурации:

   a. щелкните **Конфигурация**;

   b. отметьте в списке необходимый элемент;

   c. 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.

- Установите галочку **Перезаписать общие ресурсы кластера** для перезаписи ресурсов, принадлежащих всему кластеру.
- 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**.

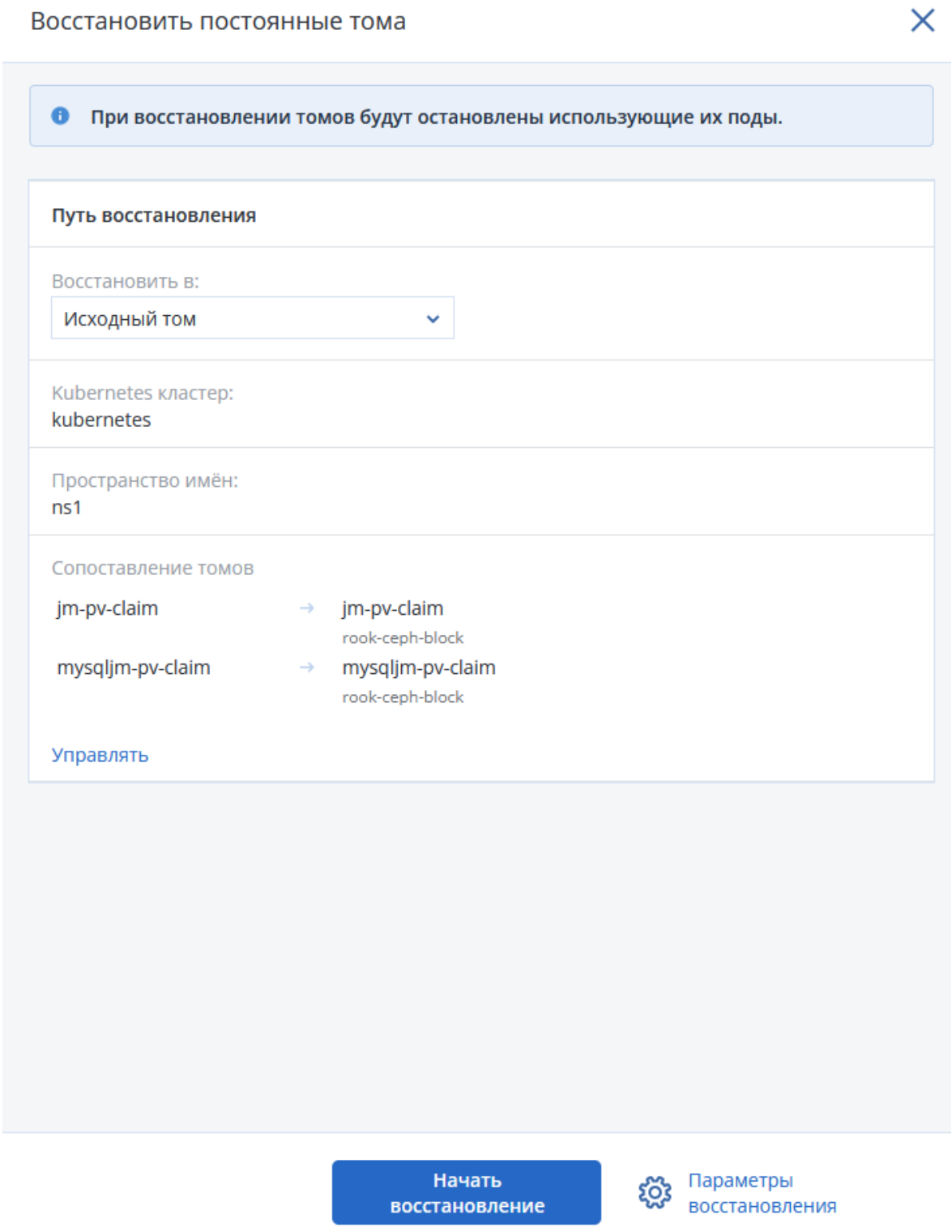
  Примечание
  При восстановлении тома с новым именем исходный том не удаляется из кластера.

  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. Щелкните **Постоянные тома** и выберите тома, которые необходимо восстановить.
5. Справа вверху щелкните **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, щелкнув **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.

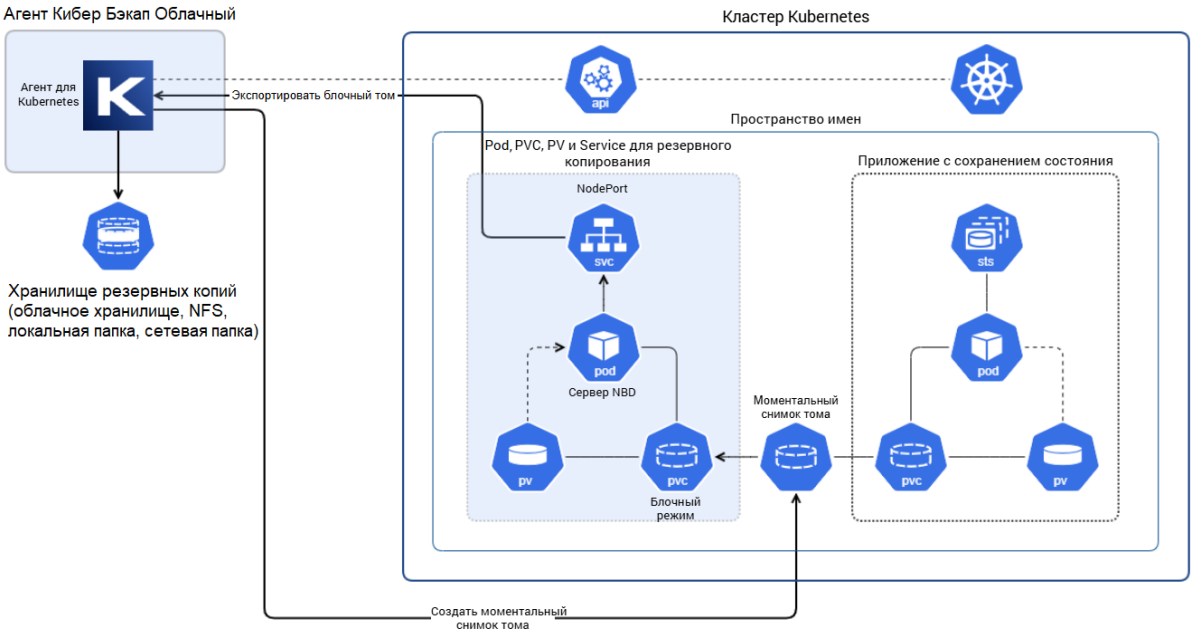
7. Нажмите **Начать восстановление**. Подтвердите еще раз восстановление в открывшемся окне и дождитесь его окончания.

18.6 Резервное копирование постоянных томов в хранилище Кибер Бэкап Облачный

18.6.1 Резервное копирование

Резервное копирование постоянного тома (PersistentVolume) в хранилище Кибер Бэкап Облачный выполняется следующим образом:

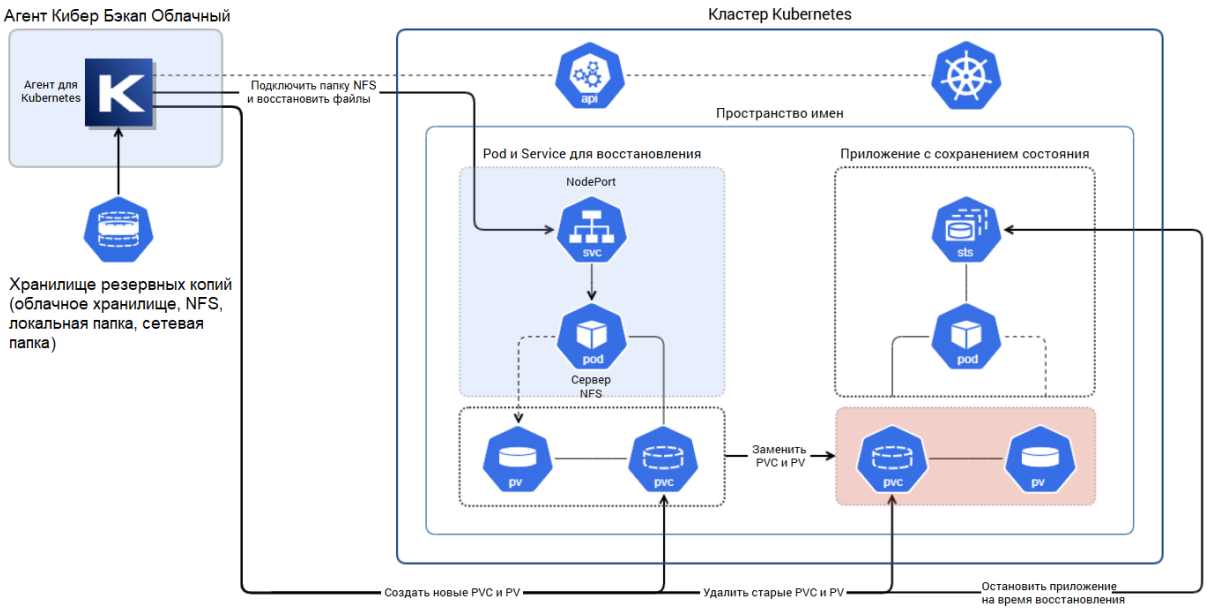
1. Создается моментальный снимок исходного тома (VolumeSnapshotContent).
2. Создается временный том в блочном режиме на основе моментального снимка.
3. Создается временный под (Pod) с сервером NBD на основе Docker-образа k8s-backup-and-restore, к которому подключен временный том. Под создается в том же самом пространстве имен, что и поды, к которым подключен исходный том.
4. Создается сервис (Service) типа NodePort, посредством которого агент для Kubernetes может получить данные временного тома. Сервис создается в том же самом пространстве имен, что и поды, к которым подключен исходный том.
5. Агент для Kubernetes получает данные временного тома, создается резервная копия тома в хранилище Кибер Бэкап Облачный.
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 Облачный** либо оставляется в кластере при использовании режима **Комбинированное**.



18.6.2 Восстановление из резервной копии

Восстановление тома из размещенной в хранилище Кибер Бэкап Облачный резервной копии происходит следующим образом:

1. Останавливаются использующие восстанавливаемый том приложения (число реплик устанавливается равным нулю или удаляются поды).
2. Создаются новый том и временный под 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.
4. Агент для Kubernetes монтирует папку NFS и записывает данные из резервной копии на новый том.
5. Сервис и временный под удаляются.
6. Новый том подключается к требуемым подам, восстанавливается исходное число реплик приложений.



18.6.3 Требования

- В кластере Kubernetes должен быть установлен CSI-драйвер, поддерживающий функцию Raw Block. Эта функция позволяет подключить постоянный том к поду как блочное устройство. 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.

18.6.4 Настройка доступа в Docker-репозиторий в закрытой среде

При отсутствии доступа в Docker-репозиторий по умолчанию (например, если Кибер Бэкап Облачный 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**
     a. 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
     ```

     b. 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**
     a. 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>
     ```

     b. Разместите полученный файл с учетными данными на машине с агентом для Kubernetes.
     c. 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
```

19 Загрузочный носитель

Загрузочный носитель – это компакт-диск, DVD-диск, флеш-накопитель USB или другой съемный носитель, который позволяет запускать агент Кибер Бэкап Облачный в среде Linux или среде предустановки Windows (WinPE) или среде восстановления Windows (WinRE) без использования самой операционной системы. Основная задача, для которой применяются такие носители, – восстановление операционной системы, которую не удается загрузить.

Примечание
Загрузочный носитель не поддерживает гибридные диски.

19.1 Настраиваемый или готовый загрузочный носитель?

Используя мастер создания загрузочных носителей, можно создать настраиваемый загрузочный носитель (на основе Linux или на основе WinPE) для компьютеров на Windows и Linux. В настраиваемых загрузочных носителях как на основе Linux, так и на основе WinPE/WinRE, можно задать дополнительные настройки, например автоматическую регистрацию, сетевые параметры или настройки прокси-сервера. В настраиваемом загрузочном носителе на основе WinPE/WinRE можно также добавить дополнительные драйверы.

Как вариант, можно скачать готовый загрузочный носитель (только на основе Linux). Готовый загрузочный носитель можно использовать для операций восстановления и доступа к Universal Restore.

19.2 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE/WinRE?

19.2.1 На основе Linux

Загрузочный носитель на основе Linux содержит агент Кибер Бэкап Облачный на основе ядра Linux. Этот агент может выполнять загрузку и операции на любом ПК-совместимом оборудовании, включая «голое железо» и машины с поврежденными или неподдерживаемыми файловыми системами.

19.2.2 На основе WinPE/WinRE

Загрузочный носитель на основе WinPE содержит минимальную систему Windows, которая называется средой предустановки Windows (WinPE), и подключаемый модуль Кибер Бэкап Облачный для WinPE, то есть модификацию агента Кибер Бэкап Облачный, запускаемую в среде предустановки. Загрузочный носитель на основе WinRE использует среду восстановления Windows. Для него не нужно устанавливать дополнительные пакеты Windows.

WinPE – самое удобное загрузочное решение в больших средах с разнообразным оборудованием.

Преимущества:

- Использование Кибер Бэкап Облачный 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 Облачный, но и команды и сценарии PE, а также 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 выполнять 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).

19.3 Создание физического загрузочного носителя

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 Кибер Бэкап Облачный.

С помощью одного носителя можно восстановить как ОС Windows, так и Linux.

Порядок создания загрузочного носителя в Windows и Linux

1. Создайте ISO-файл настраиваемого загрузочного носителя или скачайте готовый ISO-файл.

   Чтобы создать настраиваемый ISO-файл, используйте "Мастер создания загрузочных носителей" (стр. 393).

   Чтобы скачать готовый ISO-файл, в консоли службы Кибер Бэкап Облачный выберите машину и последовательно выберите пункты **Восстановить** > **Другие способы восстановления...** > **Загрузить ISO-образ**.
2. [Необязательно] В консоли службы Кибер Бэкап Облачный сгенерируйте маркер регистрации. Маркер регистрации отображается автоматически при скачивании готового ISO-файла.

   Этот маркер позволят загрузочному носителю получить доступ к облачному хранилищу данных. При этом для вас не будет выводиться запрос на ввод учетных данных.
3. Создайте физический загрузочный носитель одним из следующих способов:
   - Запишите ISO-файл на компакт- или DVD-диск.
   - 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.

Если необходимо восстановить виртуальную машину, можно подключить к ней ISO-файл в качестве CD/DVD-дисковода.

19.4 Мастер создания загрузочных носителей

Мастер создания загрузочных носителей – это специальное средство для создания загрузочных носителей. Он устанавливается как дополнительный компонент на машине с агентом Кибер Бэкап Облачный.

19.4.1 Для чего используется мастер создания загрузочных носителей?

Готовый загрузочный носитель, доступный для скачивания в консоли службы, основан на ядре Linux. В отличие от среды Windows PE, он не позволяет вводить пользовательские драйверы на лету.

Мастер создания загрузочных носителей позволяет создавать настраиваемые образы загрузочных носителей на основе Linux и WinPE.

19.4.2 Загрузочные носители на основе Linux

Как создать загрузочный носитель на основе Linux

1. Запустите **мастер создания загрузочных носителей**.

   Примечание
   На машинах с ОС Windows мастер создания загрузочных носителей расположен в папке C:\Program Files\Common Files\Acronis\MediaBuilder\.

2. В поле **Тип загрузочного носителя** выберите **По умолчанию (носители на основе Linux)**.
3. Выберите способ представления томов и сетевых ресурсов:
   - На загрузочном носителе с представлением томов по типу Linux тома отображаются как, например, hda1 и sdb2. Перед началом восстановления предпринимается попытка реконструировать MD-устройства и логические тома (LVM).
   - На загрузочном носителе с представлением томов по типу Windows тома отображаются как, например, C: и D:. Это обеспечивает доступ к динамическим томам.
4. [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" (стр. 394).
5. [Необязательно] Выберите язык для загрузочного носителя.
6. [Необязательно] Выберите режим загрузки (BIOS или UEFI), который Windows будет использовать после восстановления.

7. Выберите компонент для размещения на носителе: загрузочный агент Кибер Бэкап Облачный.
8. [Необязательно] Укажите время ожидания для меню загрузки. Если эта настройка не задана, загрузчик ждет пока вы выберите, 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. Дополнительную информацию о сценариях см. в разделе "Сценарии на загрузочных носителях" (стр. 396).
10. [Необязательно] Выберите способ регистрации загрузочного носителя в службе Кибер Бэкап Облачный при загрузке. Дополнительную информацию о настройках регистрации см. в разделе "Регистрация загрузочного носителя" (стр. 405).
11. Укажите сетевые параметры для сетевых адаптеров загруженной машины или оставьте в силе автоматическую настройку DHCP.
12. [Необязательно] Если в сети включен прокси-сервер, укажите его имя хоста или IP-адрес и порт.
13. Выберите тип файла для создаваемого загрузочного носителя:
    - Образ ISO
    - ZIP-файл
14. Укажите имя файла загрузочного носителя.
15. Проверьте настройки в итоговом окне и щелкните **Приступить**.

19.4.2.1 Параметры ядра

Можно указать один или несколько параметров ядра Linux, которые будут автоматически применяться 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.

Параметры

Если задается несколько параметров, они должны быть разделены пробелами.

- **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.

  Если удалить этот параметр, будут отображаться все сообщения загрузки, а 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 выявление 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=en-US, de-DE, fr-FR, ...**

  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:

  Бельгийский: **be-BE**

  Чешский: **cz-CZ**

  Английский: **en-GB**

  Английский (США): **en-US**

  Французский: **fr-FR**

  Французский (Швейцария): **fr-CH**

  Немецкий: **de-DE**

  Немецкий (Швейцария): **de-CH**

  Итальянский: **it-IT**

  Польский: **pl-PL**

  Португальский: **pt-PT**

  Португальский (Бразилия): **pt-BR**

  Русский: **ru-RU**

  Сербский (кириллица): **sr-CR**

  Сербский (латиница): **sr-LT**

  Испанский: **es-ES**

  При работе на загрузочном носителе используйте CTRL + SHIFT для перехода по доступным раскладкам.

19.4.2.2 Сценарии на загрузочных носителях

Если нужно, чтобы на загрузочном носителе выполнялся определенный набор операций, укажите соответствующий сценарий при создании носителя в мастере создания загрузочных носителей. Таким образом, при каждой загрузке машины с данного носителя будет запускаться указанный сценарий, а интерфейс пользователя не будет отображаться.

Выберите один из предопределенных сценариев или создайте пользовательский сценарий в соответствии со стандартами создания сценариев.

Предопределенный сценарий

Bootable Media Builder предоставляет следующие предопределенные сценарии:

- Восстановление с облачного хранилища данных (**entire_pc_cloud**).
- Восстановление с сетевой папки (**entire_pc_share**).

Сценарии, расположенные в указанных ниже папках на машине, в которой установлен мастер создания загрузочных носителей:

- В ОС Windows: %**ProgramData%\Киберпротект\MediaBuilder\scripts**.
- В ОС Linux: **/var/lib/Киберпротект/MediaBuilder/scripts/**.

Восстановление из облачного хранилища

В Bootable Media Builder укажите следующие параметры сценария:

1. Имя файла резервной копии.
2. [Необязательно] Пароль, который сценарий будет использовать для доступа к зашифрованным резервным копиям.

Восстановление с сетевой папки

В Bootable Media Builder укажите следующие параметры сценария:

- Путь к сетевой папке.
- Имя пользователя и пароль для доступа в сетевую папку;
- Имя файла резервной копии. Порядок определения имени файла резервной копии
  a. В консоли службы Кибер Бэкап Облачный последовательно выберите пункты **Хранилище резервных копий** > **Хранилища**.
  b. Выберите сетевую папку (нажмите **Добавить хранилище**, если нужной папки нет в списке).
  c. Выберите резервную копию.
  d. Нажмите **Сведения**. Имя файла отобразиться в поле **Имя файла резервной копии**.
- [Необязательно] Пароль, который сценарий будет использовать для доступа к зашифрованным резервным копиям.

Пользовательские сценарии

Внимание
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. Спецификация JSON доступна на официальном сайте JSON.

Файлы сценария

Сценарий должен быть расположен в указанных ниже каталогах на машине, в которой установлен мастер создания загрузочных носителей:

- В ОС Windows: %**ProgramData%\Киберпротект\MediaBuilder\scripts**
- В ОС Linux: **/var/lib/Киберпротект/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. 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/<файл_сценария>.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

19.4.3 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).

19.4.4 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.
default	строка, если type является string, multiString, password или enum число, еслиtype 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.

19.4.5 Тип элемента управления

Имя	Описание
string	Текстовое поле высотой в одну строку и без ограничений ширины, используемое для введения или редактирования коротких строк.
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": «Это – описание автоматически запускаемого сценария",
    "variables": {
        "var_string": {
            "displayName": "VAR_STRING",
            "type": "string", "order": 1,
            "description": «Это – элемент управления 'string':", "default": "Hello, world!"
        },
        "var_multistring": {
            "displayName": "VAR_MULTISTRING",
            "type": "multiString", "order": 2,
            "description": «Это – элемент управления 'multiString':",
            "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
            "displayName": "VAR_NUMBER",
            "type": "number", "order": 3,
            "description": "Это – элемент управления 'number':", "default": 10
        },
        "var_spinner": {
            "displayName": "VAR_SPINNER",
            "type": "spinner", "order": 4,
            "description": "Это – элемент управления 'spinner':",
            "min": 1, "max": 10, "step": 1, "default": 5
        },
```

```
        "var_enum": {
            "displayName": "VAR_ENUM",
            "type": "enum", "order": 5,
            "description": "Это – элемент управления 'enum':",
            "items": ["первый", "второй", "третий"], "default": "второй"
        },
        "var_password": {
            "displayName": "VAR_PASSWORD",
            "type": "password", "order": 6,
            "description": "Это – элемент управления 'password':", "default": "qwe"
        },
        "var_checkbox": {
            "displayName": "VAR_CHECKBOX",
            "type": "checkbox", "order": 7,
            "description": "Это – элемент управления 'checkbox'", "default": 1
        }
    }
}
```


19.4.6 Загрузочный носитель на основе WinPE и WinRE

Можно создать образы WinRE без какой-либо дополнительной подготовки или создать образы WinPE после установки пакета Windows AIK или комплекта средств для развертывания и оценки Windows (ADK).

19.4.6.1 Образы WinRE

Создание образов на основе WinRE поддерживается для следующих операционных систем:

- Windows 7 (64-разрядная версия)
- Windows 8, 8.1, 10 (64-разрядная версия)
- Windows Server 2012, 2016, 2019 (64-разрядная версия)

19.4.6.2 Образы WinPE

После установки пакета Windows AIK или комплекта средств для развертывания и оценки Windows (ADK), мастер создания загрузочных носителей поддерживает дистрибутивы WinPE, основанные

на любом из следующих ядер:

- Windows Vista (PE 2.0)
- Windows Vista SP1 и Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) с дополнением для Windows 7 SP1 (PE 3.1) или без него
- Windows 8 (PE 4.0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE для Windows 10)

Примечание
Для работы образов среды предустановки на основе WinPE 4 (и более поздних версий) требуется около 1 ГБ ОЗУ.

19.4.6.3 Создание загрузочного носителя на базе WinPE или WinRE

Мастер создания загрузочных носителей предоставляет два способа интеграции Кибер Бэкап Облачный с WinPE и WinRE:

- Создание ISO-файла с нуля с использованием подключаемого модуля Кибер Бэкап Облачный.
- Добавление подключаемого модуля Кибер Бэкап Облачный к WIM-файлу для использования в будущем (ручное создание ISO-образа, добавление других средств к образу и т. д.).

Порядок создания загрузочного носителя на базе WinPE или WinRE

1. На машине с установленным агентом Кибер Бэкап Облачный запустите мастер создания загрузочных носителей.

   Примечание
   На машинах с ОС Windows мастер создания загрузочных носителей расположен в папке C:\Program Files\Common Files\Acronis\MediaBuilder\.

2. В поле **Тип загрузочного носителя** выберите **Windows PE** или **Windows PE (64-разрядный)**. 64-разрядный носитель требуется для загрузки машины, которая использует интерфейс UEFI.
3. Выберите подтип загрузочного носителя: **WinRE** или **WinPE**.

   Для создания загрузочного носителя на основе WinRE не нужно устанавливать никаких дополнительных пакетов.

   Для создания носителя на основе WinPE (64-разрядного) необходимо скачать пакет Windows AIK или комплект средств для развертывания и оценки Windows (ADK).
4. [Необязательно] Выберите язык для загрузочного носителя.
5. [Необязательно] Выберите режим загрузки (BIOS или UEFI), который Windows будет использовать после восстановления.
6. Укажите сетевые параметры для сетевых адаптеров загруженной машины или оставьте в силе автоматическую настройку DHCP.

7. [Необязательно] Выберите способ регистрации загрузочного носителя в службе Кибер Бэкап Облачный при загрузке. Дополнительную информацию о настройках регистрации см. в разделе "Регистрация загрузочного носителя" (стр. 405).
8. [Необязательно] Укажите драйверы Windows, которые нужно добавить в загрузочный носитель.

   После загрузки Windows PE или Windows RE на машину эти драйверы помогут получить доступ к устройствам, на которых расположена резервная копия.

   Как добавить драйверы

   - Щелкните **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 или WinRE.
9. Выберите тип файла для создаваемого загрузочного носителя:
   - Образ ISO
   - образ WIM
10. Укажите полный путь к итоговому файлу образа, включая имя файла.
11. Проверьте настройки в итоговом окне и щелкните **Приступить**.

Порядок создания PE-образа (ISO-файла) из получившегося WIM-файла

- Замените в папке Windows PE файл boot.wim, используемый по умолчанию, созданным WIM-файлом. Например, введите:

  ```
  copy c:\RecoveryWIMMedia.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.

19.4.6.4 Подготовка WinPE 2.x и 3.x

Для создания или изменения образов PE 2.x или 3.x необходимо установить мастер создания загрузочных носителей на машину, на которую установлен пакет автоматической установки Windows (AIK). Если у вас нет машины с AIK, подготовьте ее следующим образом.

Как подготовить машину с AIK

1. Загрузите и установите пакет Windows AIK:
   - Набор средств автоматизированной установки (AIK) для Windows Server 2008 (PE 2.1)

   Системные требования для установки приведены по указанным выше ссылкам.
2. [Необязательно] Запишите WAIK на DVD или скопируйте на флэш-накопитель.
3. Установите платформу Microsoft .NET Framework из этого пакета.

4. Установите средство синтаксического анализа Microsoft Core XML (MSXML) 5.0 или 6.0 из этого набора.
5. Установите пакет Windows AIK из этого набора.
6. Установите мастер создания загрузочных носителей на этой же машине.

19.4.6.5 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 развертывания и оценки Windows (ADK). Если у вас нет машины с ADK, подготовьте ее следующим образом.

Как подготовить машину с ADK

1. Загрузите программу установки комплекта средств для развертывания и оценки (ADK):
   - Комплект средств для развертывания и оценки Windows (ADK) для Windows 10 (PE для Windows 10)

   Системные требования для установки приведены по указанным выше ссылкам.
2. Установите комплект ADK на машине.
3. Установите мастер создания загрузочных носителей на этой же машине.

19.4.7 Регистрация загрузочного носителя

Регистрация загрузочного носителя в службе Кибер Бэкап Облачный позволяет получить доступ к облачному хранилищу резервных копий. Регистрацию можно настроить при создании загрузочного носителя. Кроме того, можно зарегистрировать носитель после загрузки машины с его помощью или при выборе хранилища резервных копий.

Порядок предварительной настройки регистрации в службе Кибер Бэкап Облачный

1. В мастере создания загрузочных носителей перейдите в раздел **Регистрация загрузочного носителя**.
2. В поле **URL-адрес службы** укажите адрес службы Кибер Бэкап Облачный.
3. [Необязательно] В поле **Отображаемое имя** укажите имя загруженной машины.
4. Чтобы задать автоматическую регистрацию в службе Кибер Бэкап Облачный, установите флажок **Зарегистрировать загрузочный носитель автоматически**, а затем выберите уровень автоматической регистрации:
   - **Запрашивать маркер регистрации при загрузке**

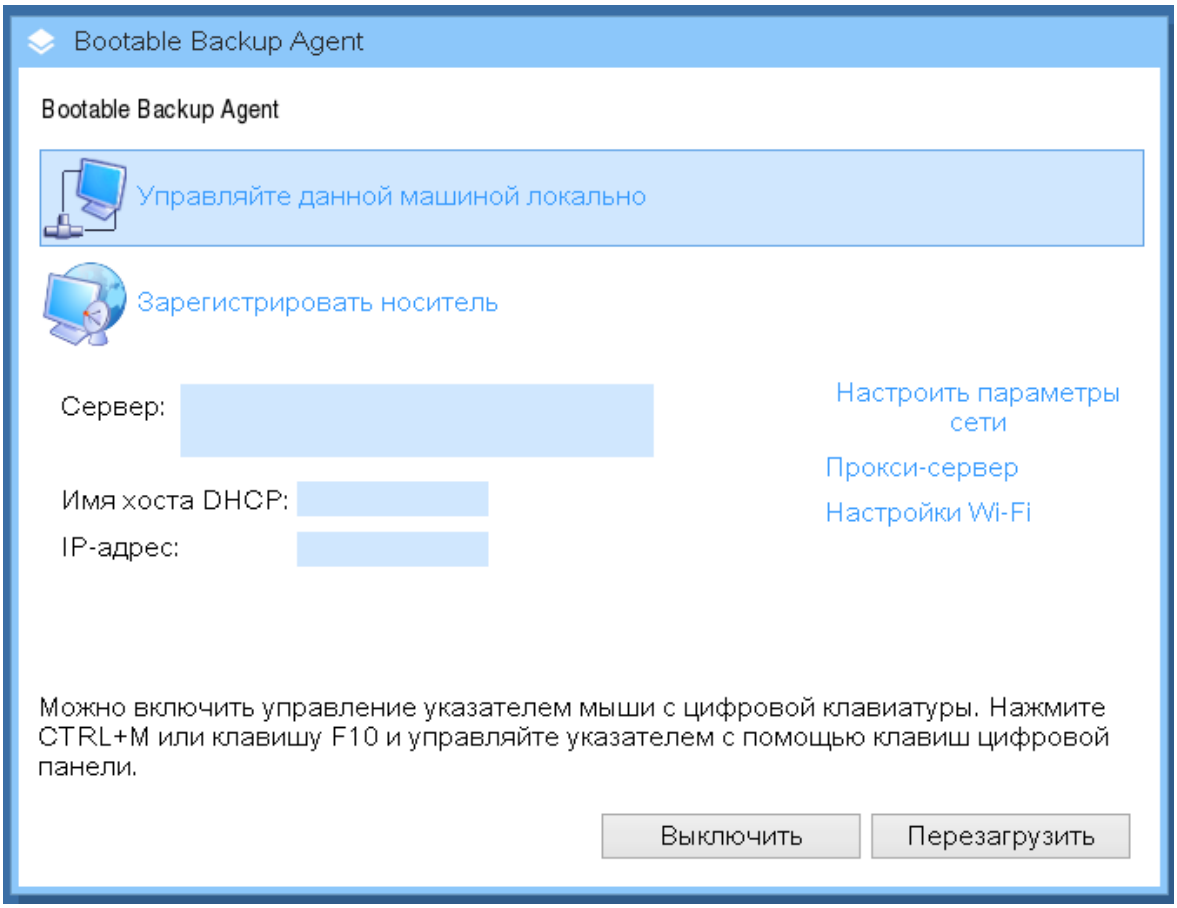
     При каждой загрузке машины с этого загрузочного носителя необходимо указывать маркер регистрации.
   - **Использовать следующий маркер**

     При загрузке с этого носителя машина будет регистрироваться автоматически.

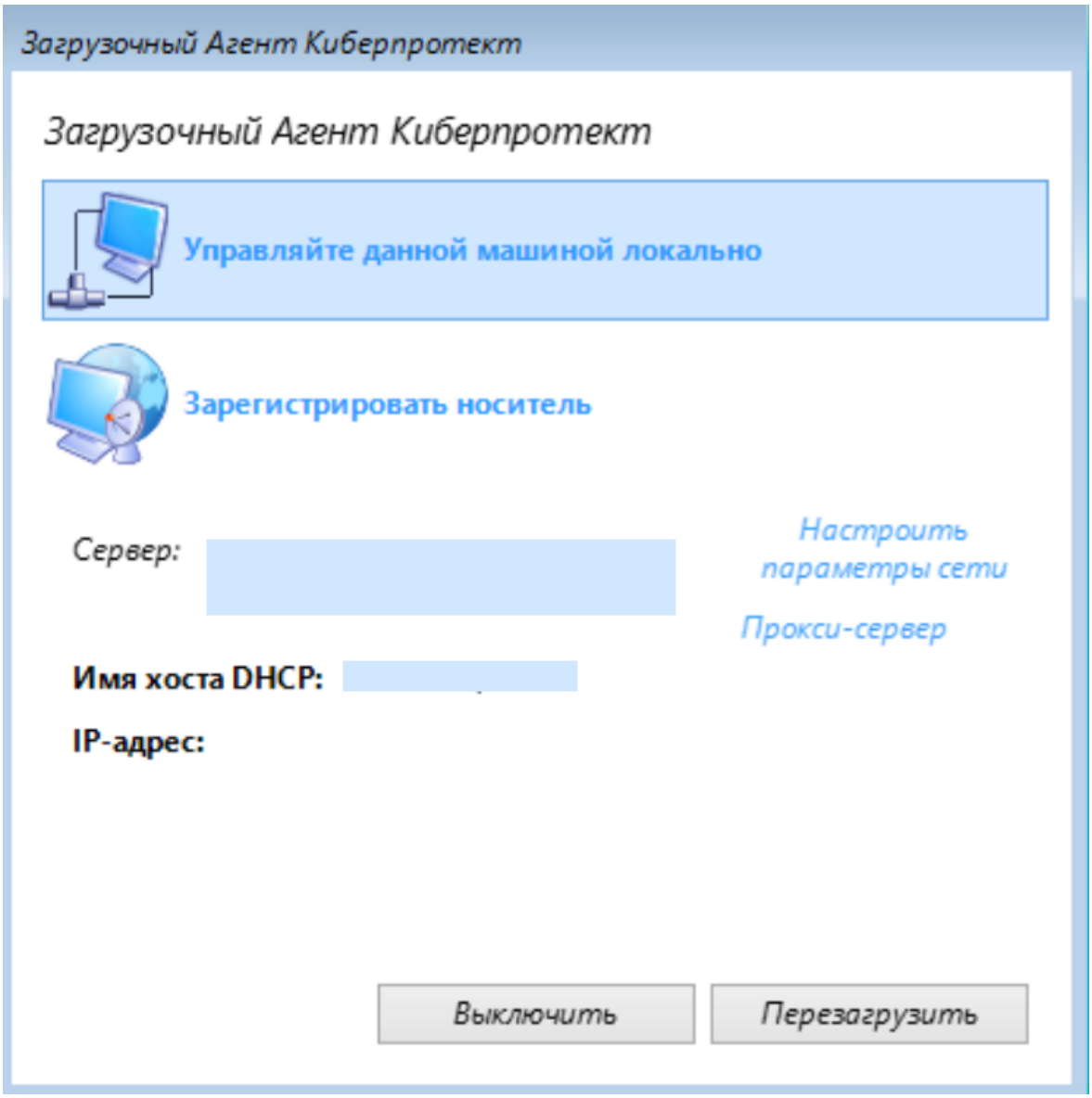
Порядок регистрации загрузочного носителя после загрузки машины с него

1. Загрузите машину с загрузочного носителя.
2. В окне запуска щелкните **Зарегистрировать носитель**.

   Окно запуска для загрузочного носителя на основе Linux:



   Окно запуска для загрузочного носителя на основе WinPE:



3. По умолчанию поле **Сервер** предзаполнено, при необходимости скорректируйте адрес службы Кибер Бэкап Облачный.
4. В поле **Маркер регистрации** введите маркер регистрации.
5. Щелкните **Зарегистрироваться**.

Порядок регистрации в облачном хранилище после загрузки машины с загрузочного носителя

1. Загрузите машину с загрузочного носителя.
2. В окне запуска нажмите **Управляйте данной машиной локально**.
3. В окне консоли нажмите **Обзор хранилищ**, в открывшемся окне выберите **Облачное хранилище**.
4. Возможны следующие варианты регистрации:
   - При использовании имени и пароля пользователя нажмите кнопку **Вход**. В открывшемся окне введите учетные данные и нажмите кнопку подтверждения. Регистрация выполнена.

- При использовании кода регистрации нажмите кнопку **Использовать код регистрации** и продолжите выполнение сценария.

5. В открывшемся окне будет предзаполнен адрес службы Кибер Бэкап Облачный, нажмите кнопку подтверждения.

   В открывшемся окне отобразится сформированный регистрационный код.
6. В веб-консоли Кибер Бэкап Облачный перейдите в раздел **Устройства** > **Добавить** > **Регистрация по коду**.
7. Нажмите кнопку **Зарегистрировать**.
8. В открывшемся окне введите регистрационный код, нажмите **Проверить код** и подтвердите регистрацию устройства.

Отобразится сообщение об успешной регистрации, регистрация выполнена.

19.4.8 Сетевые настройки

При создании загрузочного носителя можно предварительно настроить сетевые подключения, которые будут использоваться загрузочным агентом. Указанные ниже параметры можно настроить предварительно:

- 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.

Кроме того, можно задать сетевые параметры вручную при запуске загрузочного агента на машине.

19.4.8.1 Предварительная настройка нескольких сетевых подключений

Можно предварительно настроить параметры TCP/IP максимум для 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 и сохраняются 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. Содержимое этого списка 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.

19.5 Подключение машины, загруженной с загрузочного носителя

19.5.1 Локальное подключение

Для непосредственной работы на машине, загружаемой с носителя, щелкните **Локальное управление этой машиной** в окне загрузки.

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.

19.5.2 Настройка сети

Чтобы изменить сетевые параметры для текущего сеанса, в окне запуска щелкните **Настройка сети**. Появится окно **Сетевые параметры**, в котором можно задать сетевые параметры для каждого сетевого адаптера (NIC) машины.

Изменения, внесенные во время сеанса, будут утрачены после перезагрузки машины.

19.5.2.1 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. Щелкните **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, щелкните соответствующую сеть VLAN и нажмите кнопку **Удалить VLAN**.

Регистрация готового загрузочного носителя

Регистрация загрузочного носителя в службе Кибер Бэкап Облачный позволяет получить доступ к облачному хранилищу резервных копий. Способы регистрации готовых носителей совпадают со способами регистрации носителей, созданных после загрузки машины (см. раздел "Регистрация загрузочного носителя" (стр. 405)).

19.6 Операции с загрузочным носителем

Операции с загрузочным носителем подобны операциям резервного копирования и восстановления, которые выполняются при запущенной операционной системе. Отличия заключаются в следующем:

- 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
  Рекомендуется назначить уникальные имена томам.

- Загрузочный носитель с представлением томов по типу Linux отображает локальные диски и тома как отключенные (sda1, sda2...).

- Задания невозможно запланировать в расписании. Если требуется повторить операцию, настройте ее с нуля.
- Время существования журнала ограничено текущим сеансом. Весь журнал или отфильтрованные записи журнала можно сохранить в файл.

19.6.1 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**.

19.6.2 Восстановление

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Локальное управление этой машиной**.
3. Нажмите кнопку **Восстановить**.
4. В разделе **Объект восстановления** щелкните **Выбрать данные**.
5. Выберите файл резервной копии, на основе которой необходимо выполнить восстановление.
6. В левой нижней панели выберите файлы и тома (или файлы и папки), которые необходимо восстановить, и нажмите кнопку **OK**.
7. Настройте правила перезаписи.
8. Настройте исключения восстановления.
9. Настройте параметры восстановления.
10. Проверьте правильность настроек и нажмите кнопку **OK**.

19.7 Восстановление при загрузке

Восстановление при загрузке – это загрузочный компонент, который расположен на системном диске Windows или в разделе /boot в Linux. Восстановление при загрузке позволяет запустить восстановление без использования отдельного загрузочного носителя.

Восстановление при загрузке – особенно полезен для мобильных пользователей. В случае сбоя перезагрузите машину, дождитесь появления запроса **Press F11 for Киберпротект Восстановление при загрузке** и нажмите клавишу F11. Программа запустится, и можно будет

выполнить восстановление. На машинах с установленным загрузчиком GRUB пользователь не нажимает клавишу F11 при загрузке, а выбирает Восстановление при загрузке в меню загрузки.

Для использования Восстановление при загрузке сначала его необходимо активировать. Это позволяет активировать подсказку при загрузке **Press F11 for Киберпротект Восстановление при загрузке** (или добавить пункт **Восстановление при загрузке** в меню GRUB, если используется загрузчик GRUB).

Примечание
Для активации Восстановление при загрузке необходимо как минимум 100 МБ свободного дискового пространства на системном диске Windows или разделе /boot в Linux.

За исключением случая, когда используется загрузчик GRUB и он установлен в основную загрузочную запись (MBR), активация Восстановление при загрузке перезаписывает основную загрузочную запись (MBR) своим собственным загрузочным кодом. Таким образом, при использовании загрузчиков сторонних разработчиков может потребоваться их повторное активирование.

В ОС Linux при использовании загрузчика, отличного от GRUB (например, LILO), возможна его установка в загрузочную запись корневого (или загрузочного) раздела Linux вместо MBR до активации Восстановление при загрузке. В противном случае измените конфигурацию этого загрузчика вручную после активации.

Порядок активации Восстановление при загрузке на машине с агентом для Windows или агентом для Linux

1. В консоли службы Кибер Бэкап Облачный выберите машину, на которой нужно активировать Восстановление при загрузке.
2. Нажмите **Сведения**.
3. Включите переключатель **Восстановление при загрузке** .
4. Дождитесь, пока программа активирует Восстановление при загрузке.

Порядок активации Восстановление при загрузке на машине без агента

1. Загрузите машину с загрузочного носителя.
2. Щелкните **Инструменты** > **Активировать Восстановление при загрузке**.
3. Дождитесь, пока программа активирует Восстановление при загрузке.

Чтобы деактивировать Восстановление при загрузке, повторите процедуру активации и выберите соответствующие обратные действия. Деактивация отключает подсказку **Press F11 for Киберпротект Восстановление при загрузке** (или пункт меню в GRUB).

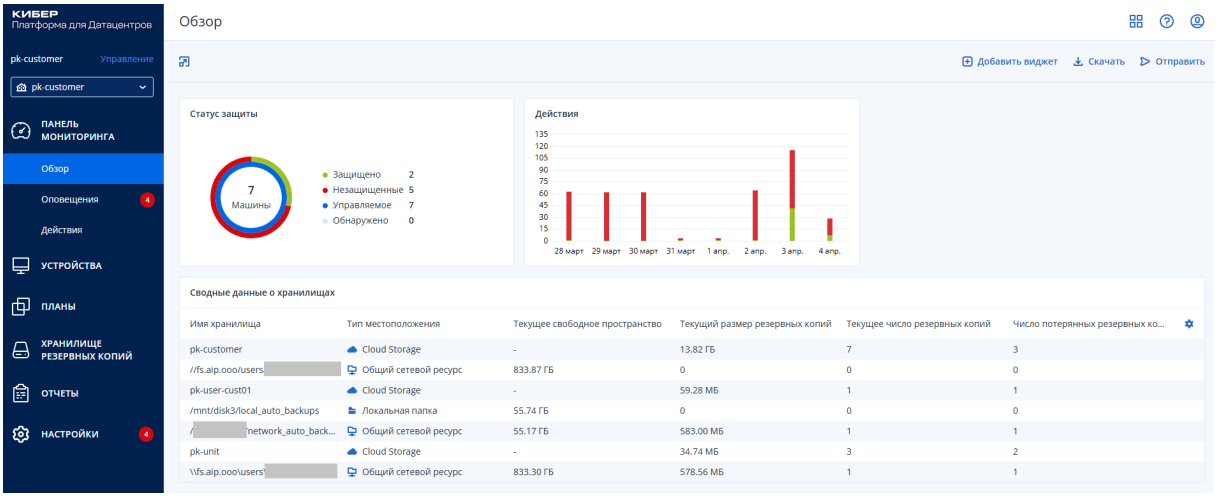
20 Мониторинг

На панели мониторинга **Обзор** есть несколько настраиваемых виджетов, которые позволяют выполнить обзор операций, относящихся к службе Кибер Бэкап Облачный. Виджеты для других служб будут доступны в следующих выпусках.

Виджеты обновляются каждые пять минут. У виджетов есть активные элементы, на которые можно нажать для анализа возникших неполадок, их диагностики и устранения. Вы можете загрузить текущее состояние панели мониторинга или отправить его по электронной почте в файле формата .pdf и (или) .xlsx.

Вы можете выбирать из целого ряда виджетов, представленных в виде таблиц, круговых диаграмм, линейчатых диаграмм, списков и карт дерева. Можно добавить несколько виджетов одного типа с разными фильтрами.

Кнопки **Скачать** и **Отправить** в разделе **Панель мониторинга** > **Обзор** недоступны в выпусках Standard службы Кибер Бэкап Облачный.



Порядок изменения расположения виджетов на панели мониторинга

Перетащите виджеты, щелкнув их имена.

Порядок изменения виджета

Щелкните значок карандаша рядом с именем виджета. Изменение виджета позволяет переименовать его, изменить диапазон времени, задать фильтры и сгруппировать строки.

Порядок добавления виджета

Щелкните **Добавить виджет** и выполните одно из следующих действий:

- Щелкните виджет, который необходимо добавить. Виджет будет добавлен с настройками по умолчанию.
- Чтобы изменить виджет перед его добавлением, щелкните Настроить, когда виджет выбран. После изменения виджета щелкните **Готово**.

Порядок удаления виджета

Щелкните значок X рядом с именем виджета.

На панели мониторинга **Действия** отображается список событий за последние 90 дней.

Можно выполнить поиск по следующим критериям:

- Имя устройства
- Пользователь, который запустил действие (например, резервное копирование).

Кроме того, можно отфильтровать действия по следующим свойствам:

- Состояние (например, «Успешно», «Сбой», «Выполняется» и т. д.).
- Состояние (например, «План защиты», «Применение плана», «Удаление резервных копий» и т. д.).
- Интервал времени (например, последние действия или указанный период времени).

20.1 Статус защиты

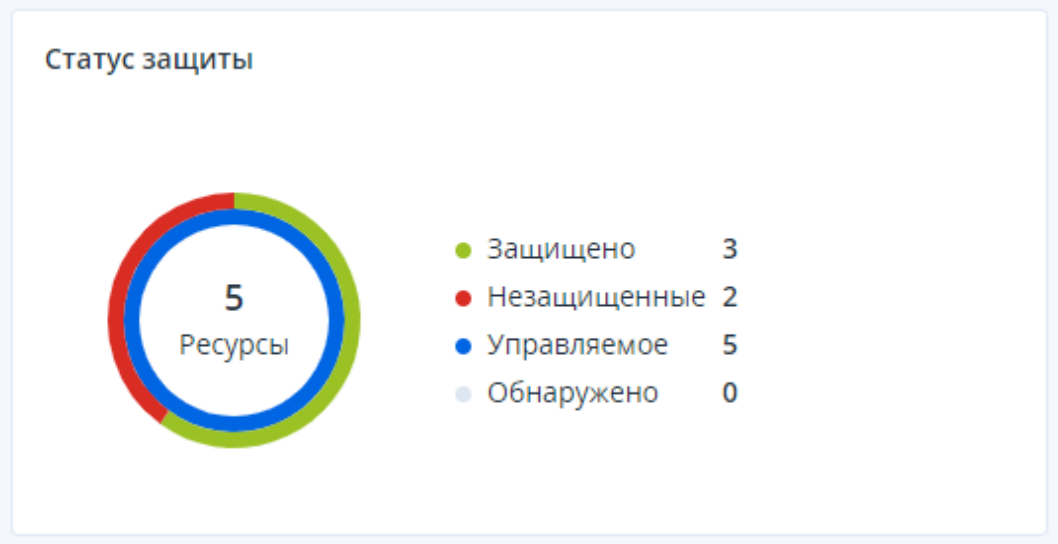
20.1.1 Статус защиты

В этом виджете показано текущее состояние защиты для всех машин.

Машина может быть в одном из следующих состояний:

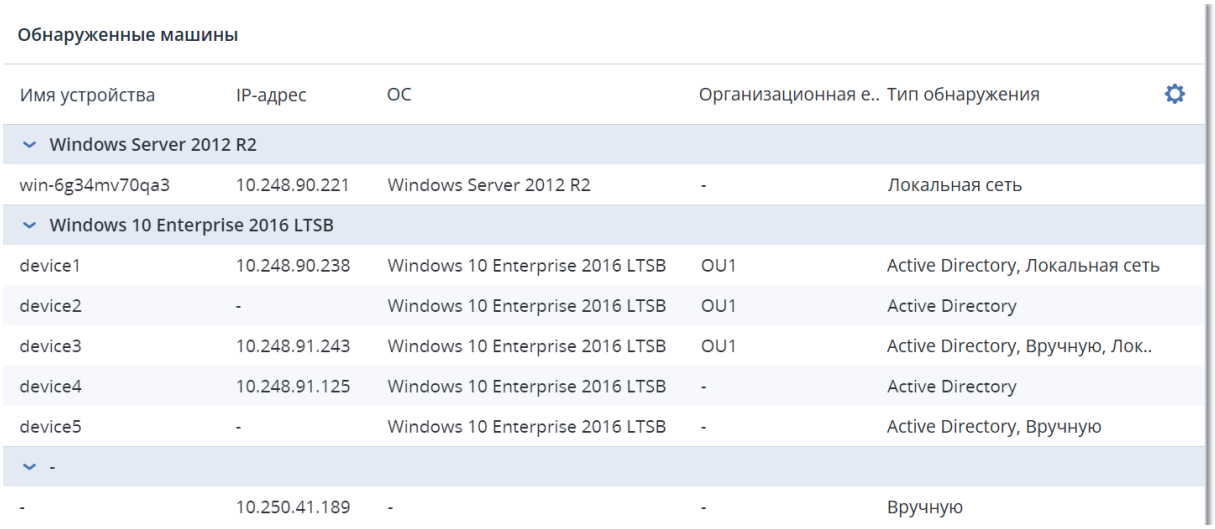
- **Защищенные**: машины, для которых применен план защиты.
- **Незащищенные**: машины, для которых не применен план защиты. Под ними подразумеваются как обнаруженные, так и управляемые машины без примененного плана защиты.
- **Управляемое**: машины с установленным агентом защиты.
- **Обнаружено**: машины без установленного агента защиты.

Если щелкнуть состояние машины, для получения более подробной информации откроется список машин, которые имеют данное состояние.



20.1.2 Обнаруженные машины

В этом виджете показан список машин, обнаруженных за указанный период времени.



Обнаруженные машины

Имя устройства	IP-адрес	ОС	Организационная е..	Тип обнаружения
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Локальная сеть
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Локальная сеть
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Вручную, Лок..
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Вручную
-				
-	10.250.41.189	-	-	Вручную

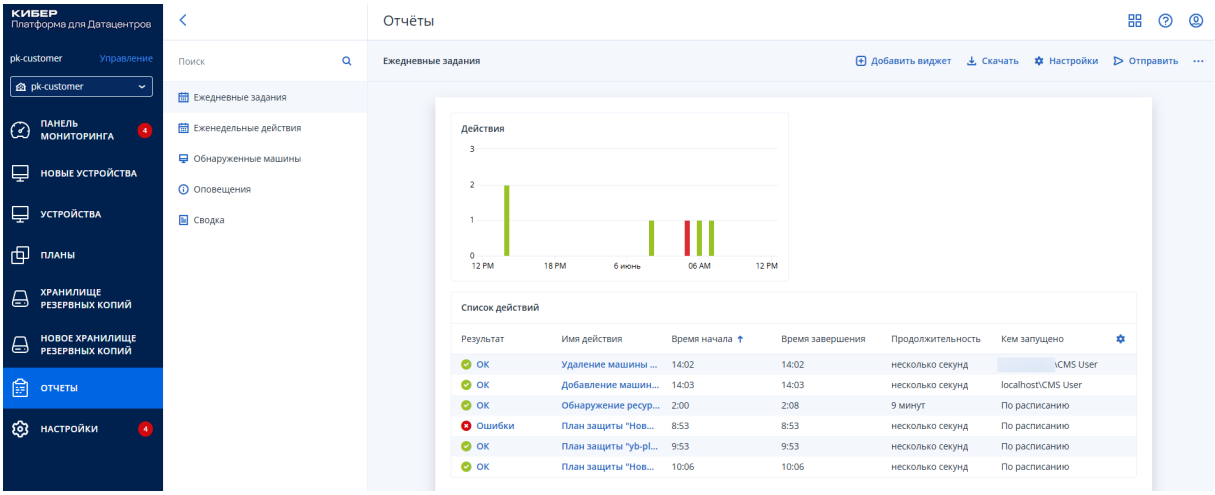
21 Отчеты

Примечание

Эта функциональность доступна только в выпусках Advanced службы Кибер Бэкап Облачный.

Отчет об операциях может включать в себя любой набор виджетов панели мониторинга. Во всех виджетах отображается сводная информация для всей компании. Во всех виджетах показаны параметры для одного диапазона времени. Этот диапазон можно изменить в настройках отчета.

Вы можете использовать отчеты по умолчанию или создать пользовательский отчет.



Набор отчетов по умолчанию зависит от используемого выпуска службы Кибер Бэкап Облачный. Ниже перечислены отчеты по умолчанию

Имя отчета	Описание
Оповещения	Показывает оповещения, выполненные за указанный период времени.
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Обнаруженные машины	Показывает все найденные машины в сети организации.
Сводные данные	Показывает сводную информацию об устройствах, защищенных за указанный период времени.
Еженедельные действия	Показывает сводную информацию о действиях, выполненных за указанный период времени.

Для просмотра отчета щелкните его имя.

Чтобы получить доступ к операциям в отчете, щелкните значок многоточия в строке отчета. Такие же операции доступны из отчета.

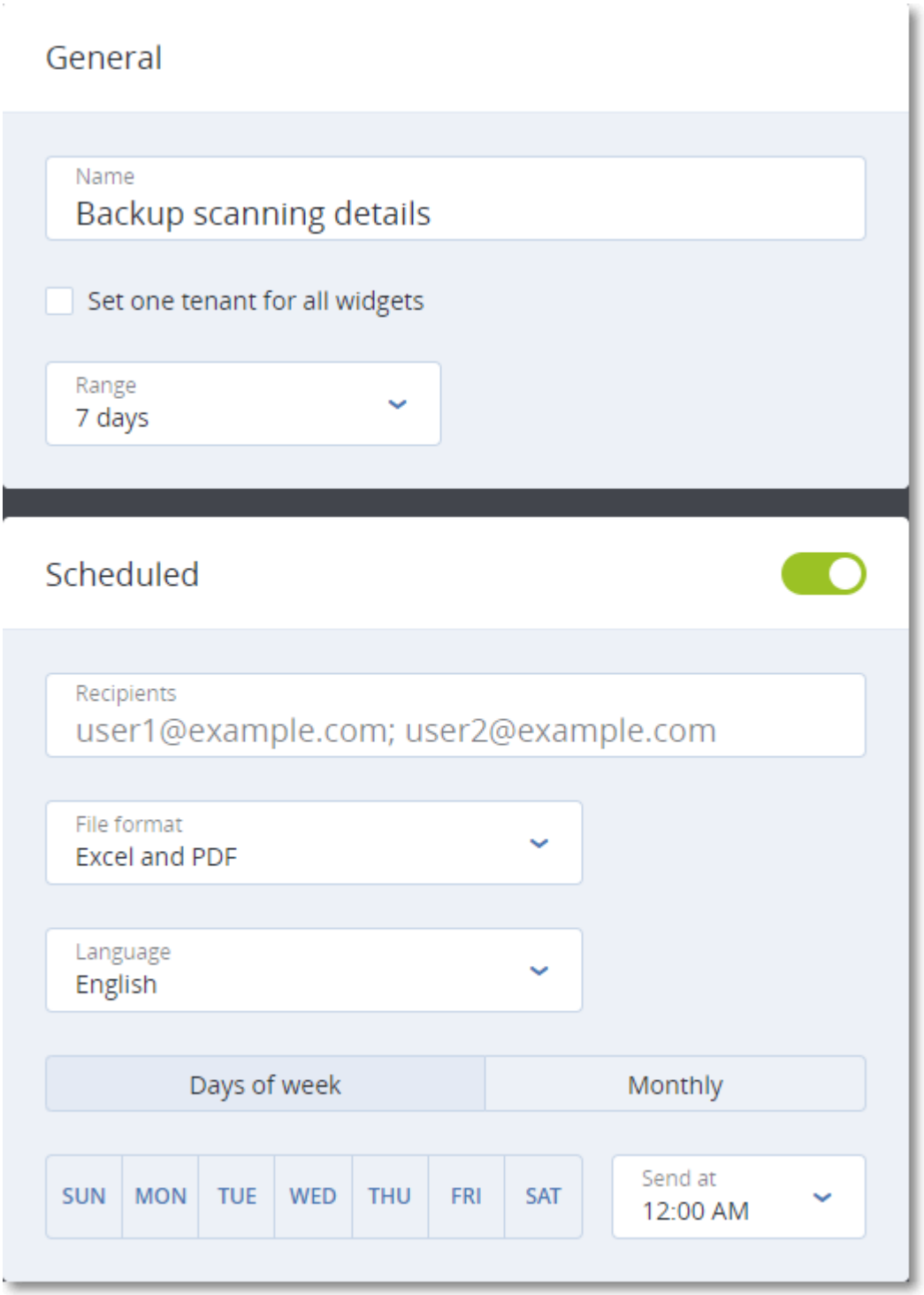
21.0.1 Добавление отчета

1. Щелкните **Добавить отчет**.
2. Выполните одно из следующих действий:
   - Чтобы добавить предопределенный отчет, щелкните его имя.
   - Чтобы добавить настраиваемый отчет, щелкните **Настраиваемый**, выберите имя отчета (по умолчанию назначаются имена типа **Custom(1)**) и добавьте виджеты в отчет.
3. [Необязательно] Для изменения положения виджетов перетащите их.
4. [Необязательно] Измените отчет, как описано ниже.

21.0.2 Изменение отчета

Чтобы изменить отчет, щелкните его имя и выберите пункт **Настройки**. При изменении отчета можно выполнить следующие действия:

- Переименовать отчет.
- Изменить диапазон времени для всех виджетов, включенных в отчет.
- Запланировать отправку отчета по электронной почте в формате PDF и (или) XLSX.



21.0.3 Планирование отчета

1. Щелкните имя отчета и выберите пункт **Настройки**.
2. Включите переключатель **Запланировано**.
3. Укажите адреса электронной почты получателей.
4. Выберите формат отчета: .pdf, .xlsx или и то, и другое.

5. Выберите дни и время отправки отчета.
6. Щелкните **Сохранить** в верхнем правом углу.

Примечание
В файл .pdf можно экспортировать не более 1000 элементов, а в файл .xlsx – не более 10000.

21.0.4 Экспорт и импорт структуры отчета

Структуру отчета (набор виджетов и настройки отчета) можно экспортировать и импортировать в файл .json.

Чтобы экспортировать структуру отчета, щелкните имя отчета, щелкните значок многоточия в правом верхнем углу и выберите пункт **Экспорт**.

Для импорта структуры отчета щёлкните **Добавить отчет** и выберите пункт **Импорт**.

21.0.5 Скачивание отчета

Чтобы скачать отчет, щелкните **Скачать** и выберите необходимые форматы:

- Excel и PDF
- Excel
- PDF

21.0.6 Дамп данных отчета

Дамп данных отчета в файле .csv можно отправить по электронной почте. Дамп содержит все данные отчета (без фильтрации) за определенный промежуток времени. Метки времени в CSV-отчетах указаны в формате UTC, а в отчетах Excel и PDF – в часовом поясе текущей системы.

ПО динамически генерирует дамп данных. При указании большого промежутка времени данное действие может долго выполняться.

Дамп данных отчета

1. Щелкните имя отчета.
2. Щелкните значок многоточия в правом верхнем углу, а затем щелкните **Данные дампа**.
3. Укажите адреса электронной почты получателей.
4. В **Диапазон времени** укажите диапазон времени.
5. Щелкните **Отправить**.

Примечание
В файл .csv можно экспортировать не более 150 000 элементов.

22 Устранение неисправностей

В этом разделе объясняется, как сохранить журнал агента в ZIP-файл. Этот файл поможет сотрудникам технической поддержки определить проблему в случае неудачного резервного копирования по неясной причине.

Получение журналов

1. Выберите машину, для которой нужно сохранить журналы.
2. Нажмите кнопку **Действия**.
3. Нажмите кнопку **Сбор сведений о системе**.
4. При появлении соответствующего запроса в веб-браузере укажите место сохранения файла.

Глоссарий

А

Агент защиты

Агент защиты – это агент, который устанавливается на машинах для защиты данных.

Агент службы предотвращения утечки данных

Клиентский компонент системы предотвращения утечки данных, который защищает хост- компьютер от несанкционированного использования, передачи и хранения конфиденциальных, защищенных или важных данных, применяя комбинацию методов контекстного анализа и анализа содержимого, а также политики предотвращения утечки данных с централизованным управлением. Cyber Protection предоставляет полнофункциональный агент службы предотвращения утечки данных. Однако функциональность агента на защищенном компьютере ограничена набором функций предотвращения утечки данных, доступных для лицензирования в Cyber Protection, и зависит от плана защиты, примененного к данному компьютеру.

В

Возврат из реплики

Перенос рабочей нагрузки с резервного сервера (например, с реплики виртуальной машины или сервера восстановления в облаке) на рабочий сервер.

Д

Дифференциальное резервное копирование

В дифференциальной резервной копии хранятся только те данные, которые отличаются от содержимого последней версии полной резервной копии. Для восстановления данных из нее необходим доступ к дифференциальной резервной копии.

И

Инкрементная резервная копия

Резервная копия, в которой хранятся изменения, произведенные в данных относительно самой поздней резервной копии. Для восстановления данных из нее необходим доступ к другим резервным копиям.

М

Модуль

Модуль – это часть плана защиты с определенными функциями защиты данных, например, модуль резервного копирования, модуль "Антивирус и защита от вредоносных программ" и т. д.

Н

Набор резервных копий

Группа резервных копий, к которым можно применить отдельное правило хранения. Для настраиваемой схемы резервного копирования наборы резервных копий соответствуют методам резервного копирования (полный, дифференциальный и инкрементный). Во всех других случаях используются ежемесячный, ежедневный,

еженедельный и почасовой наборы резервного копирования. Ежемесячная резервная копия — это первая копия, которая создается после начала месяца. Еженедельная резервная копия создается в день недели, который задан с помощью параметра Еженедельная резервная копия (щелкните значок шестеренки и последовательно выберите пункты Параметры резервного копирования > Еженедельная резервная копия). Если еженедельная копия является первой с начала месяца, она считается ежемесячной. В этом случае еженедельная резервная копия создается в назначенный день на следующей неделе. Ежедневная резервная копия — это первая копия, которая создается после начала дня, если только она не является ежемесячной или еженедельной. Почасовая резервная копия — это первая копия, которая создается после начала часа, если только она не является ежемесячной, еженедельной или ежедневной

П

Переход к реплике

Перенос рабочей нагрузки с рабочего сервера на резервный сервер (например, в реплику виртуальной машины или на сервер восстановления в облаке).

План защиты

План защиты — это план, объединяющий в себе модули защиты данных, включая следующие: «Резервное копирование», «Active Protection (Активная защита)».

Полная резервная копия

Самостоятельная резервная копия, содержащая все необходимые данные. Для восстановления данных из нее не нужен доступ к какой-либо другой резервной копии.

С

Служба предотвращения утечки данных

Система интегрированных технологий и организационных мер, которые позволяют выявить и предотвратить случайное или преднамеренное раскрытие конфиденциальных, защищенных или важных данных (или доступ к ним) со стороны неуполномоченных на то лиц в или вне организации, а также передачу таких данных в ненадежные среды.

Ф

Финализация

Операция, которая переводит временную виртуальную машину, запущенную из резервной копии, в статус постоянной. С физической точки зрения это означает восстановление всех дисков виртуальной машины вместе с изменениями, внесенными при работе машины, в хранилище данных, в котором хранятся эти изменения.

Формат резервной копии в виде одного файла

Формат резервных копий, в котором первоначальная полная и последующие инкрементные резервные копии сохраняются в одном TIBX-файле. Преимуществом этого формата является скорость инкрементного метода; при этом он лишен основного недостатка — сложностей, связанных с удалением устаревших копий. Программа помечает блоки, которые используются такими копиями, как свободные, и записывает на их место новые резервные копии. В

результате очистка выполняется очень быстро и с минимальным потреблением ресурсов. Формат резервной копии в виде одного файла недоступен при резервном копировании в хранилища, которые не поддерживают операции произвольного чтения и записи.

Указатель

Е

Ж

З

И

К

Л

М

Н

Р

С

Т

У

Ф

Х

Ч

Ш

Э