КИБЕРПРОТЕКТ

КИБЕР
Бэкап Облачный

Версия 21.06

Руководство пользователя

Редакция: 12.02.2024

Заявление об авторских правах

Содержание

1 Поддерживаемые функции Кибер Бэкап Облачный по операционным системам 11

2 Требования к программному обеспечению 17

2.1 Поддерживаемые веб-браузеры 17

2.2 Поддерживаемые операционные системы и среды 17

2.2.1 Агент для Windows 17

2.2.2 Агент для SQL, агент для Active Directory, агент для Exchange (для резервного копирования базы данных и резервного копирования с поддержкой приложений) 18

2.2.3 Агент службы предотвращения утечки данных 18

2.2.4 Агент для Exchange (для резервного копирования почтового ящика) 18

2.2.5 Агент для Oracle 18

2.2.6 Агент для Linux 19

2.2.7 Агент для Mac 19

2.2.8 Агент для VMware (виртуальное устройство) 20

2.2.9 Агент для VMware (Windows) 20

2.2.10 Агент для Hyper-V 20

2.2.11 Агент для Virtuozzo 20

2.2.12 Агент для Virtuozzo Hybrid Infrastructure 20

2.2.13 Агент для Scale Computing HC3 20

2.2.14 Агент для oVirt 21

2.3 Поддерживаемые версии Microsoft SQL Server 21

2.4 Поддерживаемые версии Microsoft Exchange Server 21

2.5 Поддерживаемые версии Oracle Database 21

2.6 Поддерживаемые версии SAP HANA 21

2.7 Поддерживаемые платформы виртуализации 22

2.7.1 Ограничения 26

2.8 Совместимость с программами шифрования 27

2.8.1 Типичные правила установки 28

2.8.2 Способ использования Зона безопасности 28

2.8.3 Общее правило резервного копирования 28

2.8.4 Процедуры восстановления для конкретных программ 28

3 Поддержка файловых систем 29

3.0.1 Дедупликация данных 30

4 Активация учетной записи 32

4.1 Двухфакторная проверка подлинности 32

4.1.1 Что если... 33

5 Доступ к службе Кибер Бэкап Облачный **34**
6 Установка программного обеспечения **35**
6.1 Какой агент необходим? 35
6.2 Системные требования для агентов 37
6.3 Подготовка 38
6.3.1 Шаг 1 38
6.3.2 Шаг 2 38
6.3.3 Шаг 3 38
6.3.4 Шаг 4 38
6.3.5 Шаг 5 39
6.3.6 Шаг 6 40
6.4 Пакеты Linux 41
6.4.1 Установлены ли необходимые пакеты? 41
6.4.2 Установка пакетов из репозитория 42
6.4.3 Установка пакетов вручную 43
6.5 Настройки прокси-сервера 44
6.5.1 В Windows 44
6.5.2 В ОС Linux 45
6.5.3 В macOS 46
6.5.4 На загрузочном носителе 47
6.6 Установка агентов 48
6.6.1 В Windows 48
6.6.2 В ОС Linux 48
6.6.3 В macOS 50
6.6.4 Изменение учетной записи входа на машинах Windows 50
6.7 Автоматическое установка или автоматическое удаление 52
6.7.1 Автоматическое установка или автоматическое удаление в Windows 52
6.7.2 Автоматическое установка или автоматическое удаление в Linux 58
6.7.3 Автоматическая установка и удаление в macOS 64
6.8 Регистрация машин вручную 66
6.8.1 Пароли со специальными символами или пробелами 69
6.9 Автоматическое обнаружение машин 70
6.9.1 Принципы работы 70
6.9.2 Предварительные требования 71
6.9.3 Процесс обнаружения машины 71
6.9.4 Автоматическое и ручное обнаружение 73
6.9.5 Управление обнаруженными машинами 78

6.9.6 Устранение неисправностей ... 79
6.10 Развертывание агента для VMware (виртуальное устройство) ... 80
6.10.1 Перед началом ... 80
6.10.2 Развертывание шаблона OVF ... 81
6.10.3 Настройка виртуального устройства ... 82
6.11 Развертывание агента для Scale Computing HC3 (виртуальное устройство) ... 84
6.11.1 Перед началом ... 84
6.11.2 Развертывание шаблона QCOW2 ... 85
6.11.3 Настройка виртуального устройства ... 86
6.11.4 Агент для Scale Computing HC3: требуемые роли ... 87
6.12 Развертывание агента для Virtuozzo Hybrid Infrastructure (виртуальное устройство) ... 87
6.12.1 Перед началом ... 87
6.12.2 Настройка сетей в Virtuozzo Hybrid Infrastructure ... 89
6.12.3 Настройка учетных записей пользователей в Virtuozzo Hybrid Infrastructure ... 89
6.12.4 Развертывание шаблона QCOW2 ... 92
6.12.5 Настройка виртуального устройства ... 93
6.13 Развертывание агента для oVirt (виртуальное устройство) ... 95
6.13.1 Перед началом ... 95
6.13.2 Развертывание шаблона OVA ... 97
6.13.3 Настройка виртуального устройства ... 98
6.13.4 Агент для oVirt: требуемые роли и порты ... 99
6.14 Развертывание агентов с использованием групповой политики ... 100
6.14.1 Предварительные требования ... 100
6.14.2 Шаг 1. Формирование маркера регистрации ... 100
6.14.3 Шаг 2. Создание MST-преобразования и извлечение пакета установки ... 101
6.14.4 Шаг 3. Настройка объектов групповой политики ... 101
6.15 Обновление агентов ... 102
6.16 Удаление агентов ... 104
6.16.1 В Windows ... 104
6.16.2 В ОС Linux ... 105
6.16.3 В macOS ... 105
6.16.4 Удаление агента для VMware (виртуальное устройство) ... 105
6.16.5 Удаление машин с консоли службы ... 106
6.17 Настройки безопасности ... 106
6.17.1 Автоматические обновления компонентов ... 106
6.17.2 Обновление определений Кибер Бэкап согласно расписанию ... 108
6.17.3 Обновление определений киберзащиты по требованию ... 108

6.17.4 Хранилище кэша ... 108
6.17.5 Удаленное подключение ... 109
6.18 Изменение квоты службы машин ... 109
7 Консоль службы ... 111
8 Группы устройств ... 114
8.1 Встроенные группы ... 114
8.2 Пользовательские группы ... 114
8.3 Создание статической группы ... 115
8.4 Добавление устройств в статические группы ... 115
8.5 Создание динамической группы ... 116
8.5.1 Условия поиска ... 116
8.5.2 Операторы ... 122
8.6 Применение плана защиты к группе ... 123
9 Поддержка мультитенантности ... 124
10 План защиты и модули ... 125
10.1 Создание плана защиты ... 125
10.2 Разрешение конфликтов плана ... 125
10.2.1 Применение нескольких планов к устройству ... 126
10.2.2 Разрешение конфликтов плана ... 126
10.3 Операции с планами защиты ... 127
11 Резервное копирование и восстановление ... 129
11.1 Резервное копирование ... 129
11.2 План защиты: памятка ... 131
11.3 Выбор данных для резервного копирования ... 133
11.3.1 Выбор дисков и томов ... 133
11.3.2 Выбор файлов и папок ... 136
11.3.3 Выбор состояния системы ... 138
11.3.4 Выбор конфигурации ESXi ... 138
11.4 Выбор места назначения ... 139
11.4.1 Расширенный выбор расположений хранения ... 140
11.4.2 О программе Зона безопасности ... 141
11.5 Расписание ... 144
11.5.1 Схемы резервного копирования ... 144
11.5.2 Дополнительные параметры расписания ... 145
11.5.3 Планирование по событиям ... 147
11.5.4 Условия запуска ... 150
11.6 Правила хранения ... 157

11.6.1 Что еще нужно знать ... 158
11.7 Запуск резервного копирования вручную ... 158
11.8 Параметры резервного копирования по умолчанию ... 159
11.9 Параметры резервного копирования ... 159
11.9.1 Доступность параметров резервного копирования ... 159
11.9.2 Оповещения ... 162
11.9.3 Консолидация резервных копий ... 162
11.9.4 Имя файла резервной копии ... 163
11.9.5 Формат резервной копии ... 167
11.9.6 Проверка резервных копий ... 169
11.9.7 Функция Changed Block Tracking (CBT) ... 169
11.9.8 Способ резервного копирования кластера ... 170
11.9.9 Уровень сжатия ... 171
11.9.10 Обработка ошибок ... 172
11.9.11 Быстрое инкрементное/дифференциальное резервное копирование ... 173
11.9.12 Фильтры файлов ... 174
11.9.13 Моментальные снимки резервных копий на уровне файлов ... 175
11.9.14 Сокращение журнала ... 176
11.9.15 Создание моментальных снимков LVM ... 176
11.9.16 Точки подключения ... 177
11.9.17 Многотомные моментальные снимки ... 178
11.9.18 Производительность и окно резервного копирования ... 178
11.9.19 Команды до и после процедуры ... 182
11.9.20 Команды до и после захвата данных ... 184
11.9.21 Планирование ... 186
11.9.22 Посекторное резервное копирование ... 187
11.9.23 Разбиение ... 188
11.9.24 Действия при сбое задания ... 188
11.9.25 Условия запуска задания ... 188
11.9.26 Служба теневого копирования томов (VSS) ... 189
11.9.27 Служба теневого копирования томов (VSS) для виртуальных машин ... 190
11.9.28 Еженедельное резервное копирование ... 191
11.9.29 Журнал событий Windows ... 191
11.10 Восстановление ... 191
11.10.1 Восстановление: памятка ... 191
11.10.2 Восстановление машины ... 193
11.10.3 Подготовьте драйверы ... 201

11.10.4 Проверьте наличие доступа к драйверам в загрузочной среде ... 202
11.10.5 Автоматический поиск драйверов ... 202
11.10.6 Драйверы запоминающих устройств для обязательной установки ... 202
11.10.7 Восстановление файлов ... 204
11.10.8 Восстановление состояния системы ... 208
11.10.9 Восстановление конфигурации ESXi ... 209
11.10.10 Параметры восстановления ... 210
11.11 Операции с резервными копиями ... 218
11.11.1 Вкладка «Хранилище резервных копий» ... 218
11.11.2 Подключение томов из резервной копии ... 220
11.11.3 Удаление резервных копий ... 221
11.12 Защита приложений Microsoft ... 223
11.12.1 Защита Microsoft SQL Server и Microsoft Exchange Server ... 223
11.12.2 Защита контроллера домена ... 223
11.12.3 Восстановление приложений ... 223
11.12.4 Предварительные требования ... 224
11.12.5 Резервное копирование базы данных ... 226
11.12.6 Резервное копирование с поддержкой приложений ... 228
11.12.7 Резервная копия почтового ящика ... 230
11.12.8 Восстановление баз данных SQL ... 231
11.12.9 Восстановление баз данных Exchange ... 235
11.12.10 Восстановление почтовых ящиков Exchange и элементов почтового ящика ... 238
11.12.11 Изменение учетных данных для доступа к SQL Server или Exchange Server ... 244
11.13 Защита размещенных данных Exchange ... 245
11.13.1 Для каких элементов можно создавать резервные копии? ... 245
11.13.2 Какие элементы можно восстановить? ... 245
11.13.3 Выбор почтовых ящиков ... 245
11.13.4 Восстановление почтовых ящиков и элементов почтовых ящиков ... 246
11.14 Защита Oracle Database ... 249
11.15 Специальные операции с виртуальными машинами ... 249
11.15.1 Запуск виртуальной машины из резервной копии (мгновенное восстановление) ... 249
11.15.2 Работа в VMware vSphere ... 253
11.15.3 Резервное копирование кластеризованных машин Hyper-V ... 266
11.15.4 Ограничение общего количества виртуальных машин, для которых одновременно выполняется резервное копирование ... 267
11.15.5 Миграция машины ... 268
12 Инвентарь оборудования ... 271

12.1 Включение сканирования инвентаря оборудования ... 271
12.2 Ручной запуск сканирования инвентаря оборудования ... 272
12.3 Обзор инвентаря оборудования ... 273
12.4 Просмотр инвентаря одного устройства ... 275
13 Вкладка «Планы» ... 277
13.1 План защиты ... 277
13.2 План сканирования резервных копий ... 278
13.3 Планы резервного копирования для облачных приложений ... 279
14 Загрузочный носитель ... 280
14.1 Настраиваемый или готовый загрузочный носитель? ... 280
14.2 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE/WinRE? ... 280
14.2.1 На основе Linux ... 280
14.2.2 На основе WinPE/WinRE ... 280
14.3 Создание физического загрузочного носителя ... 281
14.4 Мастер создания загрузочных носителей ... 282
14.4.1 Для чего используется мастер создания загрузочных носителей? ... 282
14.4.2 32-разрядная или 64-разрядная версия? ... 282
14.4.3 Загрузочные носители на основе Linux ... 282
14.4.4 Объект высшего уровня ... 288
14.4.5 Объект переменной ... 288
14.4.6 Тип элемента управления ... 289
14.4.7 Загрузочный носитель на основе WinPE и WinRE ... 291
14.4.8 Регистрация загрузочного носителя ... 295
14.4.9 Сетевые настройки ... 296
14.5 Подключение машины, загруженной с загрузочного носителя ... 297
14.5.1 Локальное подключение ... 297
14.5.2 Настройка сети ... 297
14.6 Операции с загрузочным носителем ... 298
14.6.1 Настройка режима отображения ... 298
14.6.2 Восстановление ... 299
14.7 Восстановление при загрузке ... 299
15 Мониторинг ... 301
15.1 Статус защиты ... 302
15.1.1 Статус защиты ... 302
15.1.2 Обнаруженные машины ... 303
15.2 Сведения о сканировании резервной копии ... 303

15.3 Облачные приложения 304
15.4 Виджеты «Инвентаризация программного обеспечения» 304
15.5 Виджеты «Инвентарь оборудования» 305
16 Отчеты **307**
16.0.1 Добавление отчета 308
16.0.2 Изменение отчета 308
16.0.3 Планирование отчета 310
16.0.4 Экспорт и импорт структуры отчета 310
16.0.5 Скачивание отчета 310
16.0.6 Дамп данных отчета 310
17 Устранение неисправностей **312**
Глоссарий **313**
Указатель **317**

1 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 следующих операционных системах:

- Windows: Windows 7 с пакетом обновления 1 (SP1) и более поздних версий, Windows 2008 R2 с пакетом обновления 1 (SP1) и более поздних версий.

  Управление антивирусной программой "Защитник Windows" поддерживается в Windows 8.1 и более поздних версий.
- Linux: РЕД ОС 7.2, CentOS 6.10, 7.8+, CloudLinux 6.10, 7.8+, Ubuntu 16.04.7+, где знак «плюс» означает дополнительные версии этих дистрибутивов.

  Другие дистрибутивы Linux могут поддерживаться, но для них не выполнялось тестирование.
- macOS: 10.13.x и более поздних версий (поддерживается только функция "Антивирус и защита от вредоносных программ").

Примечание
Функция «Защита от вредоносных программ» для Linux и macOS поддерживается, только когда включена функция «Расширенная защита от вредоносных программ».

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 Virtuozzo Hybrid Infrastructure, агент Scale Computing, агент для oVirt), поддерживается только резервное копирование.

Функции Кибер Бэкап Облачный	Windows	Linux	macOS
Планы защиты по умолчанию			
Сотрудники, которые работают удаленно	Да	Нет	Нет
Офисные сотрудники (сторонняя антивирусная программа)	Да	Нет	Нет
Офисные сотрудники (антивирусная программа Кибер Бэкап)	Да	Нет	Нет
Непрерывная защита данных (CDP)			
CDP для файлов и папок	Да	Нет	Нет

CDP для измененных файлов посредством отслеживания приложений	Да	Нет	Нет
Автоматическое обнаружение и удаленная установка			
Обнаружение на основе сети	Да	Нет	Нет
Обнаружение на основе Active Directory	Да	Нет	Нет
Обнаружение на основе шаблонов (импорт машин из файла)	Да	Нет	Нет
Добавление устройств вручную	Да	Нет	Нет
Active Protection			
Обнаружение внедрений в процесс	Да	Нет	Нет
Автоматическое обнаружение затронутых файлов из локального кэша	Да	Да	Нет
Управление доверенным/блокированным процессом	Да	Нет	Нет
Исключения процессов/папок	Да	Да	Нет
Защита внешних дисков (жесткие диски (HDD), флэш-накопители, SD-карты)	Да	Нет	Нет
Защита сетевых папок	Да	Да	Нет
Защита на стороне сервера	Да	Нет	Нет
Защита Zoom, Cisco Webex, Citrix Workspace	Да	Нет	Нет
Антивирус и защита от вредоносных программ			
Полностью интегрированная функциональность Active Protection	Да	Нет	Нет
Защита от вредоносных программ в реальном времени	Да	Да, когда включена функция «Расширенная защита от вредоносных программ»	Да, когда включена функция «Расширенная защита от вредоносных программ»
Расширенная защита от вредоносных программ в реальном времени с локальным обнаружение на основе сигнатур	Да	Да	Да
Анализ статистики для переносимых	Да	Нет	Да*

исполняемых файлов			
Сканирование на вредоносные программы по требованию	Да	Да**	Да
Защита сетевых папок	Да	Да	Нет
Защита на стороне сервера	Да	Нет	Нет
Сканирование файлов архива	Да	Нет	Да
Сканирование съемных дисков	Да	Нет	Да
Сканирование только новых и измененных файлов	Да	Нет	Да
Исключения файлов/папок	Да	Да	Да***
Исключения процессов	Да	Нет	Нет
Модуль анализа поведения	Да	Нет	Нет
Предотвращение эксплойтов	Да	Нет	Нет
Карантин	Да	Да	Да
Автоматическая очистка карантина	Да	Нет	Да
Фильтрации URL-адресов (http/https)	Да	Нет	Нет
Корпоративный белый список	Да	Нет	Да
Управление антивирусной программой «Защитник Microsoft»	Да	Нет	Нет
Управление Microsoft Security Essentials	Да	Нет	Нет
Регистрация модуля "Антивирус и защита от вредоносных программ" и управление им через центр обеспечения безопасности Windows	Да	Нет	Нет
Оценка уязвимостей			
Оценка уязвимостей операционной системы и ее "родных" приложений	Да	Да****	Да
Оценка уязвимостей для сторонних приложений	Да	Нет	Да
Оценка уязвимостей для macOS	Нет	Нет	Да
Оценка уязвимостей для сторонних программ macOS	Нет	Нет	Да

Управление исправлениями			
Автоматическое утверждение исправлений	Да	Нет	Нет
Автоматическая установка исправлений	Да	Нет	Нет
Тестирование исправлений	Да	Нет	Нет
Ручная установка исправлений	Да	Нет	Нет
Планирование установки исправлений	Да	Нет	Нет
Надежная установка исправлений: перед установкой исправлений создается резервная копия машины (предусматривается в плане защиты)	Да	Нет	Нет
Отмена перезагрузки машины при выполняющемся резервном копировании	Да	Нет	Нет
Карта защиты данных			
Настраиваемое определение важных файлов	Да	Нет	Нет
Сканирование машин для поиска незащищенных файлов	Да	Нет	Нет
Обзор незащищенных хранилищ	Да	Нет	Нет
Возможность запустить действие защиты из виджета "Карта защиты данных" (действие **Защитить все файлы**)	Да	Нет	Нет
Работоспособность диска			
Мониторинг работоспособности дисков HDD и SSD на основе искусственного интеллекта	Да	Нет	Нет
Интеллектуальные планы защиты на основе оповещений Киберпротект Операционный Центр Кибер Бэкап (CPOC)			
Канал угроз	Да	Нет	Нет
Мастер исправления	Да	Нет	Нет
Сканирование резервной копии			
Сканирование резервных копий образов на вредоносные программы в рамках плана резервного копирования	Да	Нет	Нет

Сканирование резервных копий образов на вредоносные программы в облаке	Да	Нет	Нет
Сканирование шифрованных резервных копий на вредоносные программы	Да	Нет	Нет
Безопасное восстановление			
Сканирование на вредоносные программы с использованием модуля "Антивирус и защита от вредоносных программ" в процессе восстановления	Да	Нет	Нет
Безопасное восстановление для зашифрованных резервных копий	Да	Нет	Нет
Подключение к удаленному рабочему столу			
Подключение через клиент HTML5	Да	Нет	Нет
Подключение через собственный RDP-клиент Windows	Да	Нет	Нет
Удаленная помощь	Да	Нет	Нет
Параметры управления			
Сценарии апсейла для продвижения выпусков Кибер Бэкап Облачный	Да	Да	Да
Централизованная и удаленная веб-консоль управления	Да	Да	Да
Параметры защиты			
Удаленная очистка данных (только в Windows 10)	Да	Нет	Нет
Кибер Бэкап Монитор			
Приложение Кибер Бэкап Монитор	Да	Нет	Да
Статус защиты для Zoom	Да	Нет	Нет
Статус защиты для Cisco Webex	Да	Нет	Нет
Статус защиты для Citrix Workspace	Да	Нет	Нет
Инвентаризация программного обеспечения			
Сканирование инвентаря программы	Да	Нет	Да
Мониторинг инвентаризации программного обеспечения	Да	Нет	Да

Инвентарь оборудования			
Сканирование инвентаря оборудования	Да	Нет	Да
Мониторинг инвентаризации оборудования	Да	Нет	Да

* Статический анализ переносимых исполняемых файлов поддерживается только для запланированных заданий сканирования в macOS.

** Условия запуска не поддерживаются для сканирования по требованию в Linux.

*** Исключения файлов/папок поддерживаются только в том случае, когда указаны файлы и папки, которые не будут сканироваться в ходе защиты в реальном времени или в ходе планового сканирования в macOS.

**** Оценка уязвимостей зависит от доступности официальных советов по безопасности для специфического дистрибутива, например, https://lists.centos.org/pipermail/centos-announce/, https://lists.centos.org/pipermail/centos-cr-announce/ и других.

2 Требования к программному обеспечению

2.1 Поддерживаемые веб-браузеры

Веб-интерфейс сервиса резервного копирования поддерживает перечисленные ниже браузеры:

- Google Chrome 29 или более поздней версии
- Mozilla Firefox 23 или более поздней версии
- Opera 16 или более поздней версии
- Windows Internet Explorer 11 или более поздней версии
- Microsoft Edge 25 или более поздней версии
- В операционных системах macOS и iOS выполняется Safari 8 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.

2.2 Поддерживаемые операционные системы и среды

2.2.1 Агент для Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows Server 2003 SP1/2003 R2 и более поздних версий: выпуски Standard и Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2
- Windows Vista – все выпуски
- Windows Server 2008 – выпуски Standard, Enterprise, Datacenter, Foundation и Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – все выпуски
- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter, Foundation и Web
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – все выпуски
- Windows 8/8.1 – все выпуски (x86, x64), за исключением выпусков Windows RT
- Windows Server 2012/2012 R2 – все выпуски
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10: выпуски Home, Pro, Education, Enterprise, IoT Enterprise и LTSC (прежнее название LTSB)

- Windows Server 2016 – все варианты установки, кроме Nano Server
- Windows Server 2019: все варианты установки, кроме Nano Server

2.2.2 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.

2.2.3 Агент службы предотвращения утечки данных

- Microsoft Windows 7 с пакетом обновления 1 (SP1) и более поздних версий
- Microsoft Windows Server 2008 R2 и более поздних версий

2.2.4 Агент для Exchange (для резервного копирования почтового ящика)

- Windows Server 2008 – выпуски Standard, Enterprise, Datacenter, Foundation и Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 – все выпуски
- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter, Foundation и Web
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – все выпуски
- Windows 8/8.1 – все выпуски (x86, x64), за исключением выпусков Windows RT
- Windows Server 2012/2012 R2 – все выпуски
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – выпуски Home, Pro, Education и Enterprise
- Windows Server 2016 – все варианты установки, кроме Nano Server
- Windows Server 2019: все варианты установки, кроме Nano Server

2.2.5 Агент для Oracle

- Windows Server 2008 R2 – выпуски Standard, Enterprise, Datacenter и Web (x86, x64)
- Windows Server 2012 R2 – выпуски Standard, Enterprise, Datacenter и Web (x86, x64)
- Linux: все ядра и дистрибутивы, которые поддерживаются агентом для Linux (перечислены ниже)

2.2.6 Агент для Linux

Linux с версией ядра от 2.6.9 до 5.7 и glibc версии 2.3.4 или более поздней, включая следующие дистрибутивы x86 и x86_64:

- РЕД ОС 7.3.1
- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7. 7.8, 7.9, 8.0*, 8.1*, 8.2*, 8.3*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10 и 11
- SUSE Linux Enterprise Server 12 – поддерживается в файловых системах, за исключением Btrfs
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.0, 8.1, 8.2, 8.3
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.8, 8.0, 8.1, 8.2, 8.3 – Unbreakable Enterprise Kernel и Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.2, 8.3
- ClearOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7
- ALT Linux 7.0

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.

2.2.7 Агент для Mac

Поддерживаются процессоры x64.

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11

2.2.8 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

2.2.9 Агент для VMware (Windows)

Этот агент предоставляется в виде приложения Windows для работы в любой из перечисленных выше операционных систем для агента для Windows, за следующими исключениями:

- 32-разрядные операционные системы не поддерживаются;
- Windows XP, Windows Server 2003/2003 R2 и Windows Small Business Server 2003/2003 R2 не поддерживаются.

2.2.10 Агент для Hyper-V

- Windows Server 2008 (только x64) с ролью Hyper-V, включая режим установки Server Core
- Windows Server 2008 R2 с ролью Hyper-V, включая режим установки Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 с ролью Hyper-V, включая режим установки Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (только x64) с Hyper-V
- Windows 10 – выпуски Pro, Education и Enterprise с Hyper-V
- Windows Server 2016 с ролью Hyper-V – все варианты установки, кроме Nano Server
- Microsoft Hyper-V Server 2016
- Windows Server 2019 с ролью Hyper-V – все варианты установки, кроме Nano Server
- Microsoft Hyper-V Server 2019

2.2.11 Агент для Virtuozzo

- Virtuozzo 6.0.10, 6.0.11, 6.0.12, 7.0.13, 7.0.14
- Virtuozzo Hybrid Server 7.5

2.2.12 Агент для Virtuozzo Hybrid Infrastructure

Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5

2.2.13 Агент для Scale Computing HC3

Scale Computing Hypercore 8.8, 8.9, 9.0

2.2.14 Агент для oVirt

Red Hat Virtualization 4.2, 4.3, 4.4

2.3 Поддерживаемые версии Microsoft SQL Server

- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.4 Поддерживаемые версии Microsoft Exchange Server

- **Microsoft Exchange Server 2019**: все выпуски.
- **Microsoft Exchange Server 2016** – все выпуски.
- **Microsoft Exchange Server 2013** – все выпуски, накопительный пакет обновления 1 (CU1) или более поздней версии.
- **Microsoft Exchange Server 2010** – все выпуски, все пакеты обновления. Резервное копирование почтового ящика и фрагментарное восстановление из резервных копий базы данных поддерживается начиная с пакета обновления 1 (SP1).
- **Microsoft Exchange Server 2007** – все выпуски, все пакеты обновления. Резервное копирование почтового ящика и фрагментарное восстановление из резервных копий базы данных не поддерживается.

2.5 Поддерживаемые версии Oracle Database

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

Поддерживаются только конфигурации с одним экземпляром.

2.6 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.

2.7 Поддерживаемые платформы виртуализации

В следующей таблице представлена сводная информация о разных поддерживаемых платформах виртуализации.

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
VMware		
Версии VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0 **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 2008 (x64) с Hyper-V Windows Server 2008 R2 с Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 с Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) с Hyper-V 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		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
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		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		+
Red Hat Virtualization (под управлением oVirt) 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		+
Virtuozzo		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Только виртуальные машины. Контейнеры не поддерживаются.
Virtuozzo 7.0.13, 7.0.14	Только контейнеры ploop. Виртуальные машины не поддерживаются.	Только виртуальные машины. Контейнеры не поддерживаются.
Virtuozzo Hybrid Server 7.5	+	Только виртуальные машины. Контейнеры не поддерживаются.
Virtuozzo Hybrid Infrastructure		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+

* 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.

2.7.1 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, миграция V2P и миграция V2V с Virtuozzo. Создание резервной копии и загрузочного носителя для восстановления с помощью агента для Linux.
  - Запуск виртуальной машины с резервной копии, созданной агентом для Linux.

- **Зашифрованные виртуальные машины** (эта функциональная возможность представлена в VMware vSphere 6.5)
  - Резервное копирование зашифрованных виртуальных машин выполняется в незашифрованном состоянии. Если шифрование является критически важным, включите шифрование резервных копий при создании плана защиты.
  - Восстановленные виртуальные машины всегда являются незашифрованными. По окончании восстановления шифрование можно включить вручную.
  - 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**
  - Виртуальные машины VMware: (впервые реализовано в VMware vSphere 6.5) **Безопасная загрузка** отключается после восстановления виртуальной машины как новой виртуальной машины. По окончании восстановления можно вручную включить этот параметр. Это ограничение действует для VMware.
  - Виртуальные машины Hyper-V: Для всех виртуальных машин GEN2 безопасная загрузка отключается после восстановления виртуальной машины как на новую, так и на имеющуюся виртуальную машину.
- **Резервное копирование конфигурации ESXi** не поддерживается для VMware vSphere 7.0.

2.8 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 Зона 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.

2.8.1 Типичные правила установки

Настоятельно рекомендуется установить программу шифрования перед установкой агентов защиты.

2.8.2 Способ использования Зона безопасности

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

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

2.8.3 Общее правило резервного копирования

Позволяет выполнить резервное копирование на уровне дисков операционной системы.

2.8.4 Процедуры восстановления для конкретных программ

2.8.4.1 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.

2.8.4.2 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 по ссылке https://support.microsoft.com/kb/2622803

3 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="3">Поддержка</th><th rowspan="2">Ограничения</th></tr>
<tr><th>Агенты</th><th>Загрузочные носители для Windows и Linux</th><th>Загрузочный носитель для Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Все агенты</td><td>+</td><td>+</td><td rowspan="4">Без ограничений</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td rowspan="2">Агент для Mac</td><td>-</td><td>+</td></tr>
<tr><td>APFS</td><td>-</td><td>+</td><td>• Поддерживается, начиная с macOS High Sierra 10.13.
• При восстановлении на машину, отличную от исходной, или на «голое железо» конфигурацию диска необходимо заново создать вручную.</td></tr>
<tr><td>JFS</td><td rowspan="2">Агент для Linux</td><td>+</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><td>-</td></tr>
</table>

ReiserFS4		+	-	• Файлы невозможно исключить из резервной копии диска • Невозможно включить быстрое инкрементное/дифференциальное резервное копирование • Невозможно изменить размер томов при выполнении восстановления
ReFS	Все агенты	+	+	
XFS		+	+	
Linux SWAP	Агент для Linux	+	-	Без ограничений
exFAT	Все агенты	+ Если резервная *копия хранится в* файловой системе exFAT, загрузочный носитель невозможно использовать для восстановления.	+	• Поддерживается только резервное копирование дисков/томов • Файлы невозможно исключить из резервной копии • Отдельные файлы невозможно восстановить из резервной копии

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.

3.0.1 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 Cyber Backup.

4 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.

4.1 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.

4.1.1 Что если...

4.1.1.1 ...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.

4.1.1.2 ...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.

5 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 выпусковКибер 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**.

6 Установка программного обеспечения

6.1 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 и агента для Virtuozzo 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	
Физические машины под управлением macOS	Агент для Mac	
Приложения		
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 Scale Computing HC3	Агент для Scale Computing HC3 (виртуальное устройство)	На хосте Scale Computing HC3.
Виртуальные машины Red Hat Virtualization (с управлением oVirt)	Агент для oVirt (виртуальное устройство)	На хосте Red Hat Virtualization.
Виртуальные машины и контейнеры Virtuozzo***	Агент для Virtuozzo	На хосте Virtuozzo.
Виртуальные машины на хосте Citrix XenServer		
Red Hat Virtualization (RHV/RHEV)		
Виртуальные машины на основе ядра (KVM)		
Виртуальные машины Oracle		
Виртуальные машины Nutanix AHV		
Мобильные устройства		
Мобильные устройства с Android	Мобильное приложение для Android	На мобильное устройство, резервную копию которого нужно создать.
Мобильные устройства с iOS	Мобильное приложение для iOS	

*В ходе установке агент для Exchange проверяет достаточность свободного пространства 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».

***Для Virtuozzo 7 поддерживаются только контейнеры ploop. Виртуальные машины не поддерживаются.

****Виртуальная машина считается виртуальной, если ее резервная копия была создана с использованием внешнего агента. Если агент установлен в гостевой системе, то операции резервного копирования и восстановления выполняются точно так же, как и на виртуальной машине. Тем не менее машина считается виртуальной, если заданы квоты на количество машин.

6.2 Системные требования для агентов

Агент	Для установки необходимо место на диске
Агент для Windows	1,2 ГБ
Агент для Linux	2 ГБ
Агент для Mac	900 МБ
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 Virtuozzo и агент для Linux	1 ГБ
Агент для Virtuozzo Hybrid Infrastructure	700 МБ
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.

6.3 Подготовка

6.3.1 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?

6.3.2 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. 37).

6.3.3 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**. Доступны 32-разрядный и 64-разрядный пакеты. 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.

Установка в ОС Linux и macOS 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.

6.3.4 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 https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

6.3.5 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).

6.3.5.1 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.

6.3.5.2 Порты, требуемые для компонента "Загрузчик"

Компонента "Загрузчик" отвечает за доставку обновлений на компьютер и их распространение на другие экземпляры "Загрузчик". Он может выполняться в режиме агента. В этом случае соответствующий компьютер становится агентом загрузчика. Агент "Загрузчик" скачивает обновления из Интернета и серверов, становясь источником распространения обновлений на другие компьютеры. Для работы компонента "Загрузчик" требуется указанные ниже порты:

- **6888**: используется протоколом BitTorrent для обновлений между одноранговыми узлами.
- **6771**: используется локальным портом обнаружения однорангового узла. Также принимает участие в обновлениях между одноранговыми узлами.
- **18018**: используется для обмена данными между средствами обновлений, которые работают в разных режимах: Средство обновления и агент с ролью "Средство обновления".
- **18019**: локальный порт, который используется для обмена данными между средством обновления и агентом Кибер Бэкап.

6.3.6 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.

6.3.6.1 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

6.4 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.

6.4.1 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.

6.4.2 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.

6.4.3 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
  ```

6.4.3.1 Пример: Установка пакетов вручную в Fedora 14

Для установки необходимых пакетов в Fedora 14 на 32-разрядной машине выполните следующие шаги.

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

   ```
   cat /proc/version
   ```

   Выходные данные этой команды включают следующее:

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

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

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

3. Получите пакет **make** для Fedora 14:

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

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

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

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

6.5 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.

6.5.1 В 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
```

6.5.2 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
    ```

6.5.3 В macOS

Параметры прокси-сервера можно указать во время установки или заранее, как описано в процедуре ниже. С помощью той же процедуры эти параметры можно изменить после установки.

Указание параметров прокси-сервера в macOS

1. Создайте файл **/Library/Application Support/Acronis/Registry/Global.config** и откройте его в текстовом редакторе, например Text Edit.

2. Скопируйте и вставьте в этот файл следующие строки:

```
<?xml version="1.0" ?>
<registry name="Global">
  <key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"proxy.company.com"</value>
    <value name="Port" type="Tdword">"443"</value>
    <value name="Login" type="TString">"proxy_login"</value>
    <value name="Password" type="TString">"proxy_password"</value>
  </key>
</registry>
```

3. Замените proxy.company.com именем хоста или IP-адресом прокси-сервера, а 443 – номером порта в десятичном формате.
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 файл.
6. Если агент защиты еще не установлен, то можно установить его сейчас.
7. Откройте файл **/Library/Application Support/Acronis/Agent/etc/aakore.yaml** в текстовом редакторе.
8. Найдите раздел **env** или создайте его и добавьте туда следующие строки:

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

9. Вместо proxy_login и proxy_password укажите учетные данные прокси-сервера, а вместо proxy_address:port – адрес и номер порта прокси-сервера.
10. Откройте **Приложения** > **Утилиты** > **Терминал**
11. Перезапустите службу aakore, выполнив следующие команды:

```
sudo launchctl stop aakore
sudo launchctl start aakore
```

12. Перезапустите агент, выполнив следующие команды:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

6.5.4 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.

6.6 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 пункте Поддерживаемые функции Кибер Бэкап Облачный по операционным системам.

6.6.1 В Windows

1. Убедитесь в том, что машина подключена к Интернету.
2. Войдите как администратор и запустите программу установки.
3. [Необязательно] Щелкните **Настройка параметров установки** и внесите нужные изменения (при необходимости):
   - Чтобы изменить устанавливаемые компоненты (например, отключить установку Кибер Бэкап Монитор, программы командной строки)
   - Изменение метода регистрации машины в службе Кибер Бэкап Облачный. Можно изменить параметр **Использовать консоль службы** (по умолчанию) на **Использовать учетные данные** или **Использовать маркер регистрации**.
   - Изменение пути установки.
   - Изменение учетной записи, с которой будет запускаться служба агента. Дополнительную информацию см. в разделе "Изменение учетной записи входа на машинах Windows".
   - Проверка или изменение имени хоста или IP-адреса, порта и учетных данных прокси-сервера. Если прокси-сервер включен в Windows, он определяется и используется автоматически.
4. Нажмите **Установить**.
5. [Только при установке агента для VMware] Укажите адрес и учетные 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 учетную запись пользователя, под которой будет работать служба агента, и нажмите кнопку **Готово**. В целях безопасности программа установки не может автоматически создавать учетные 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.

6.6.2 В ОС Linux

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

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. Установите флажки для агентов, которые необходимо установить. Доступны следующие агенты:
   - **Агент для Linux**
   - **Агент для Virtuozzo**
   - **Агент для Oracle**

   Для агента для Oracle и агента для Virtuozzo требуется установленный агент для Linux (64-разрядная версия).
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.**

6.6.3 В macOS

1. Убедитесь в том, что машина подключена к Интернету.
2. Дважды щелкните DMG-файл установки.
3. Дождитесь, пока операционная система подключит образ установочного диска.
4. Дважды щелкните **Установить**.
5. Если в сети включен прокси-сервер, в строке меню щелкните **Агент защиты**, затем — **Настройки прокси-сервера** и укажите имя хоста или IP-адрес, порт и учетные данные прокси-сервера.
6. При необходимости введите учетные данные администратора.
7. Нажмите кнопку **Продолжить**.
8. Подождите, пока появится экран регистрации.

   Если вы используете macOS версии Mojave 10.14.x или более поздней, предоставьте полный доступ к агенту защиты, чтобы активировать операции резервного копирования.

6.6.4 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.

6.7 Автоматическое установка или автоматическое удаление

6.7.1 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.

6.7.1.1 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 "Развертывание агентов с использованием групповой политики".
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**.

6.7.1.2 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
```

6.7.1.3 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.

6.7.1.4 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 по ссылке https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

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		32-разрядная/64-разрядная	Компоненты Core для агентов
BackupAndRecoveryAgent	MmsMspComponents	32-разрядная/64-	Агент для Windows

		разрядная	
ArxAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для SQL
ARADAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент для Oracle
AcronisESXSupport	MmsMspComponents	64-разрядная версия	Агент для VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32-разрядная/64-разрядная	Агент для Hyper-V
CommandLineTool		32-разрядная/64-разрядная	Программа командной строки
TrayMonitor	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Cyber Protection Monitor
DLPAgentFeature	BackupAndRecoveryAgent	32-разрядная/64-разрядная	Агент службы предотвращения утечки данных
BackupAndRecoveryBootableComponents;		32-разрядная/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, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW.
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 "Развертывание агентов с использованием групповой политики".

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
```

6.7.2 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 .i686 или .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.

6.7.2.1 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
AgentForPCS	Агент для Virtuozzo
OracleAgentFeature	Агент для Oracle

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

Для агента для Oracle и агента для Virtuozzo 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, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW.
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 "Развертывание агентов с использованием групповой политики".

  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.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
  ```

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

  ```
  ./Cyber_Protection_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.

  ```
  ./Cyber_Protection_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 Virtuozzo, агента для Oracle с настройками конфигурации в отдельном текстовом файле.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
  ```

- Установка агента для Linux, агента для Virtuozzo, агента для Oracle и удаление всех их

журналов, задач и настроек конфигурации.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

6.7.3 Автоматическая установка и удаление в macOS

В этом разделе описан порядок установки, регистрации и удаления агента Кибер Бэкап Облачный в автоматическом режиме на машинах под управлением macOS с использованием командной строки.

Порядок скачивания установочного файла (.dmg)

1. В консоли службы последовательно выберите пункты **Устройства**> **Все устройства**.
2. Щелкните **Добавить**, а затем – **Mac**.

Установка агента для Mac

1. Создайте временный каталог для подключения файла установки (.dmg).

   ```
   mkdir <dmg_root>
   ```

   <dmg_root> – имя по вашему усмотрению.
2. Подключите файл .dmg.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   <dmg_file> – это имя файла установки. Например, **Cyber_Protection_Agent_for_MAC_x64.dmg**.
3. Запустите установщик.

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. Отсоедините файл установки (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

6.7.3.1 Примеры

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/Cyber_Protection_Agent_for_MAC_x64.dmg -mountpoint mydirectory
  ```

  ```
  sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
  ```

  ```
  hdiutil detach mydirectory
  ```

Порядок регистрации агента для Mac
  ```

Выполните одно из следующих действий:

- Зарегистрируйте агент для определенной учетной записи, указав имя пользователя и пароль.

  ```
  sudo /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a <адрес службы Кибер Бэкап Облачный> -t cloud -u <имя пользователя> -p <пароль> -o register
  ```

  В этой формуле:

  <адрес службы Кибер Бэкап Облачный> – адрес, который используется **для входа в** службу Кибер Бэкап Облачный. Пример:

  <имя пользователя> и <пароль> – учетные данные учетной записи, которую нужно использовать для регистрации агента. Для этого нельзя использовать учетную запись администратора партнера.

- Зарегистрируйте агент, используя маркер регистрации.

  ```
  sudo /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a <адрес службы Кибер Бэкап Облачный> -t cloud -o register --token <маркер>
  ```

  Маркер регистрации – это последовательность из 12 символов, разделенных дефисами на три части. Его можно создать в консоли службы, как указано в разделе "Развертывание агентов с использованием групповой политики".

  При использовании маркера регистрации необходимо указать точный адрес центра обработки данных. Это URL-адрес, который отображается **после входа в** службу Кибер Бэкап Облачный. Пример:

6.7.3.2 Примеры

Регистрация с использованием имени пользователя и пароля.

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a https://cloud.company.com -t cloud -u johndoe -p johnspassword -o register
  ```

Регистрация с использованием маркера.

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -a https://eu2-cloud company.com -t cloud o -register --token D91D-DC46-4F0B
  ```

Внимание
Если используется macOS 10.14 или более поздней версии, предоставьте агенту защиты полный доступ к диску. Для этого последовательно выберите пункты **Программы** > **Утилиты**, а затем запустите **Кибер Бэкап Agent Assistant**. Следуйте инструкциям в окне приложения.

Порядок удаления агента для Mac

Выполните следующую команду:

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\ Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

Чтобы удалить все журналы, задачи и настройки конфигурации при удалении, выполните следующую команду:

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\ Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

6.8 Регистрация машин вручную

Помимо регистрации машины в службе Кибер Бэкап Облачный при установке агента, можно также зарегистрировать ее в интерфейсе командной строки. Это может понадобиться, например, когда агент установлен, но при этом не удалось выполнить автоматическую регистрацию, или необходимо зарегистрировать существующую машину под новой учетной записью.

Порядок регистрации машины

Чтобы зарегистрировать машину с использованием имени пользователя и пароля, выполните указанную ниже команду.

В ОС Windows

Команда для регистрации машины в текущей учетной записи:

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

Шаблон команды для регистрации машины в другой учетной записи:

```
"%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
```

В ОС Linux

Команда для регистрации машины в текущей учетной записи:

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

Шаблон команды для регистрации машины в другой учетной записи:

```
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
```

В macOS

Команда для регистрации машины в текущей учетной записи:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --update
```

Шаблон команды для регистрации машины в другой учетной записи:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <адрес службы> -u <имя пользователя> -p <пароль>
```

Пример команды:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

Примечание

Введите имя пользователя и пароль для учетной записи, под которой агент будет зарегистрирован. Для этого нельзя использовать учетную запись администратора партнера. Адрес службы – это URL-адрес для **входа в** службу Кибер Бэкап Облачный. Например, https://cloud.company.com:

Как вариант, можно зарегистрировать машину, используя маркер регистрации. Для этого выполните указанную ниже команду.

В ОС Windows

Шаблон команды:

```
"%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
```

В ОС Linux

Шаблон команды:

```
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
```

В macOS

Шаблон команды:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a <адрес службы> --token <маркер>
```

Пример команды:

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

Примечание

При использовании маркера регистрации необходимо указать 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 для этого https://cloud.company.com.

Маркер регистрации – это последовательность из 12 символов, разделенных дефисами на три части. Дополнительную информацию о создании маркера регистрации см. в разделе "Развертывание агентов с использованием групповой политики".

Отмена регистрации машины

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
```

В macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

6.8.1 Пароли со специальными символами или пробелами

Если пароль содержит специальные символы или пробелы, заключите его в кавычки при вводе в командной строке.

Например, в Windows выполните указанную ниже команду.

Шаблон команды:

```
"%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 "johns password"
```

Если не удалось устранить ошибку:

- Зашифруйте пароль в формат base64 на портале https://www.base64encode.org/.
- В командной строке укажите зашифрованный пароль, используя параметры "-b" или "--base64".

Например, в Windows выполните указанную ниже команду.

Шаблон команды:

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

Пример команды:

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud -a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

6.9 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.

6.9.1 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.

6.9.2 Предварительные требования

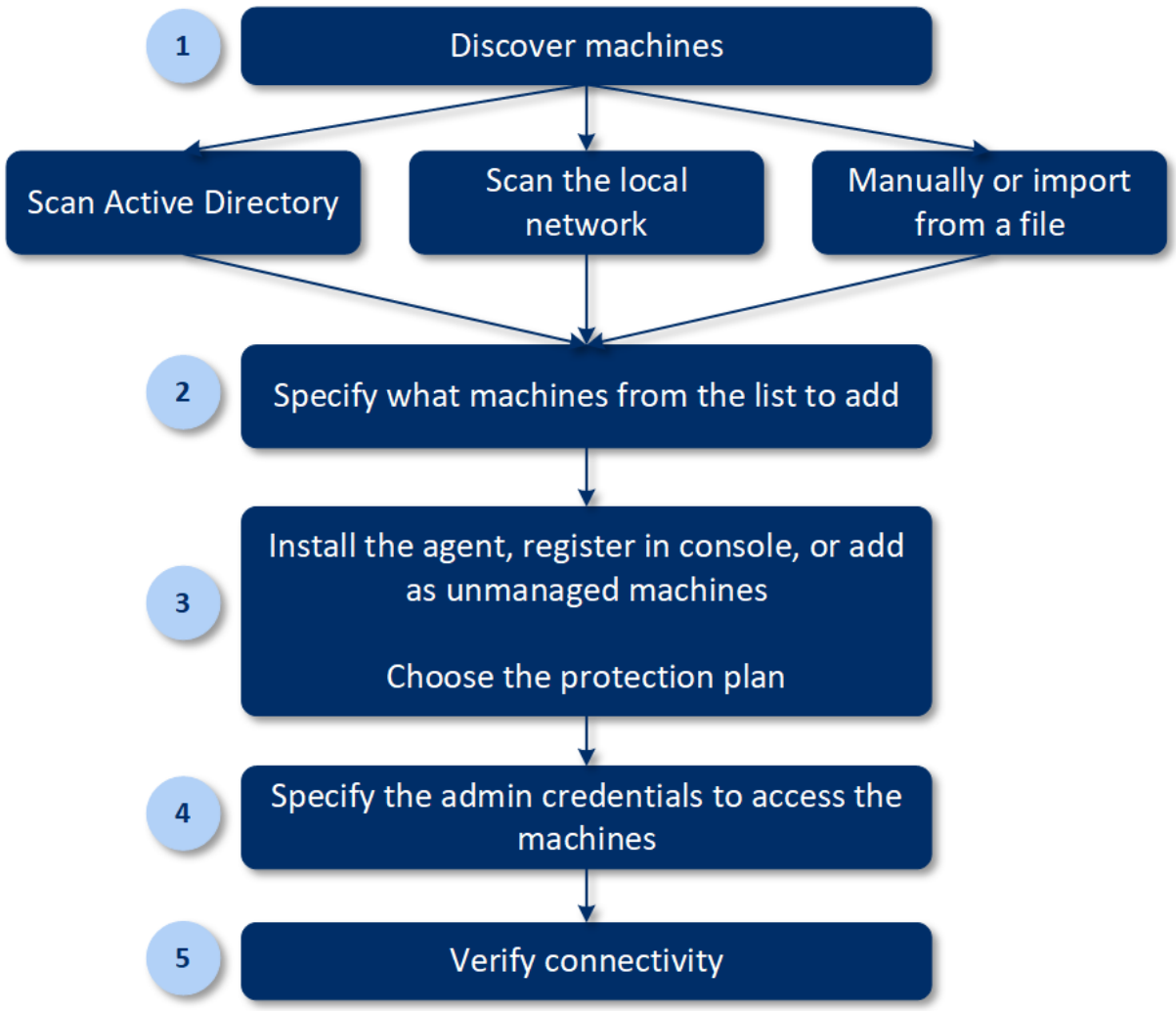
Прежде чем запустить обнаружение машин, необходимо установить агент защиты хотя бы на одной машине в локальной сети, чтобы использовать его как агент обнаружения.

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.

6.9.3 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.

6.9.4 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 для обнаружения машин.
6. Выберите метод обнаружения:
   - **Поиск в Active Directory**. Убедитесь, что машина с агентом обнаружения входит в домен Active Directory.
   - **Сканировать локальную сеть**. Если выбранному агенту обнаружения не удалось найти никаких машин, выберите другой агент обнаружения.
   - **Укажите вручную или импортируйте из файла**. Вручную определите машины для добавления или импортируйте их из текстового файла.
7. [Если выбран метод обнаружения Active Directory] Выберите метод поиска машин:
   - **В списке организационной единицы**. Выбор группы машин для добавления.
   - **По запросу диалекта LDAP**. Запрос диалект LDAP для выбора машин. **База поиска** определяет места поиска, а **Фильтр** позволяет указать критерий выбора машины.
8. [Если выбран метод обнаружения Active Directory или локальной сети] Используйте список для выбора машин, которые необходимо добавить.

[Если выбран ручной метод обнаружения] Укажите IP-адреса машины или имена хостов либо импортируйте список машины из текстового файла. Файл должен содержать IP-адреса/имена хостов, по одному на строку. Ниже приводим пример файла:

```
156.85.34.10
156.85.53.32
156.85.53.12
EN-L00000100
EN-L00000101
```

После добавления адресов машины вручную или их импорте из файла агент попытается выполнить команду ping в отношении добавленных машин и определить их доступность.

9. Выберите 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.

     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 их 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**).

6.9.4.1 Подготовка машины для удаленной установки

1. Для успешной установки на удаленной машине под управлением ОС Windows XP параметр **Панель управления > Свойства папки > Вид > Использовать мастер общего доступа** должен быть *отключен* на этой машине.
2. 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".
3. 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)".
4. Общий доступ к файлам и принтерам на удаленной машине должен быть *включен*. Получение доступа к этому параметру
   - На машине под управлением Windows 2003 Server: выберите **Панель управления > Брандмауэр Windows > Исключения > Общий доступ к файлам и принтерам**.
   - На машине под управлением Windows Vista, Windows Server 2008, Windows 7 или более поздних версий: выберите **Панель управления > Брандмауэр Windows > Центр управления сетями и общим доступом > Изменить дополнительные параметры общего доступа**.
5. 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.

6.9.4.2 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 Microsoft по следующей ссылке: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

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

6.9.4.3 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.

6.9.5 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.

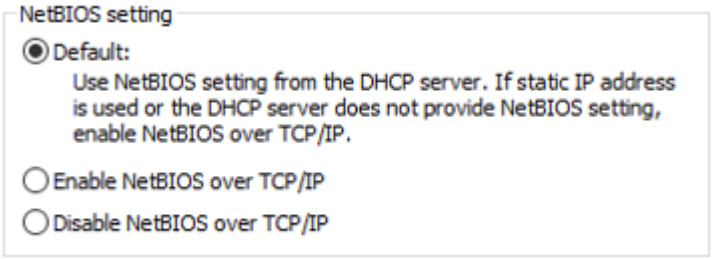
Те машины, на которых установлен агент защиты, отображаются в разделе **Устройства** > **Машины с агентами**.

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

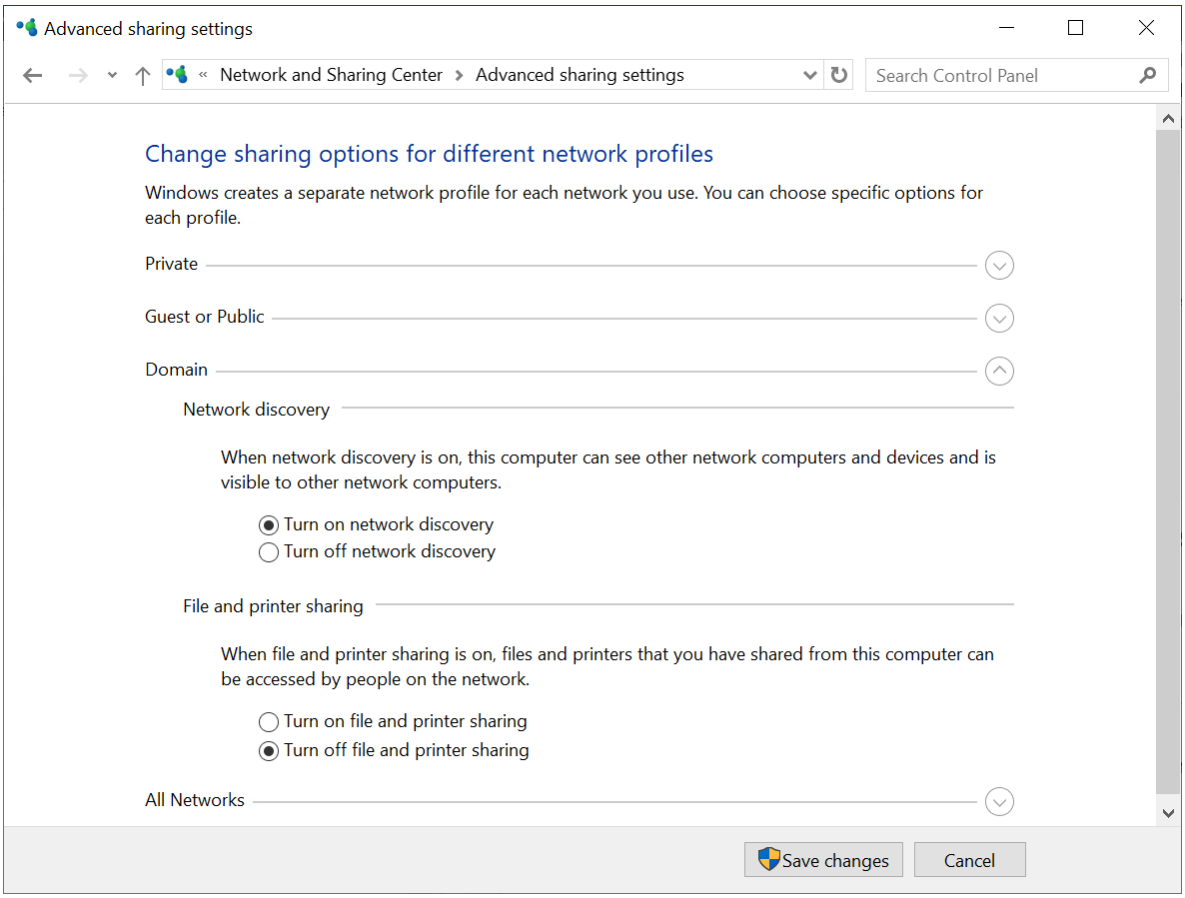
6.9.6 Устранение неисправностей

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.

6.10 Развертывание агента для VMware (виртуальное устройство)

6.10.1 Перед началом

6.10.1.1 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.

6.10.1.2 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».

6.10.1.3 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**.

6.10.2 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.

6.10.3 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.

6.11 Развертывание агента для Scale Computing HC3 (виртуальное устройство)

6.11.1 Перед началом

Этот программно-аппаратный комплекс представляет собой предварительно настроенную виртуальную машину, которая развертывается в кластере Scale Computing HC3. В ее состав входит агент защиты, который позволяет вам администрировать киберзащиту для всех виртуальных машин в кластере.

6.11.1.1 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 в свойствах виртуальной машины в веб-интерфейсе Scale Computing HC3. 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 9 ГБ.

6.11.1.2 Сколько агентов необходимо?

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

Если в кластере несколько агентов, виртуальные машины автоматически равномерно 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, вы понимаете, что для необходимой пропускной способности требуется больше агентов, и развертываете в кластере дополнительное виртуальное устройство. Сервер управления назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится. Если агент удаляется с сервера управления, то машины, назначенные этому агенту, распределяются между оставшимися агентами. Однако этого не происходит, если агент повреждается или вручную удаляется из кластера Scale Computing HC3. 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 **Scale Computing**.
2. Щелкните значок шестерни в верхнем правом углу таблицы и в области **Система** установите флажок **Агент**.
3. Имя агента отобразится в появившемся столбце.

6.11.2 Развертывание шаблона QCOW2

1. Войдите в учетную запись Кибер Бэкап Облачный.
2. Щелкните **Устройства** > **Все устройства** > **Добавить** > **Scale Computing HC3**.
   ZIP-архив загрузится на машину.
3. Распакуйте ZIP-архив и сохраните файлы .qcow2 и .xml в папке с именем **ScaleAppliance**.
4. Передайте папку **ScaleAppliance** в сетевую папку и убедитесь, что кластер Scale Computing HC3 имеет к ней доступ.
5. Войдите в кластер Scale Computing HC3 как администратор с ролью **Создание/изменение ВМ**. Дополнительную информацию о ролях, которые необходимы для выполнения операций с виртуальными машинами Scale Computing HC3, см. в разделе "Агент для Scale Computing HC3: требуемые роли" (стр. 87).
6. В веб-интерфейсе Scale Computing HC3 импортируйте шаблон виртуальной машины из папки **ScaleAppliance**.
   a. Щелкните шаблон **Import HC3 VM** (Импорт ВМ HC3).
   b. В окне **Import HC3 VM** (Импорт ВМ HC3) укажите следующую информацию:
      - Имя новой виртуальной машины.
      - Сетевая папка, в которой расположена папка **ScaleAppliance**.
      - Имя пользователя и пароль для доступа к сетевой папке.
      - [Необязательно] Тег домена для новой виртуальной машины.
      - Путь к папке **ScaleAppliance** в сетевой папке.
   c. Щелкните **Импорт**.

По окончании развертывания необходимо настроить виртуальное устройство. Инструкции о том, как это сделать, см. в разделе "Настройка виртуального устройства" (стр. 86)

Примечание
Если в кластере 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) в веб-интерфейсе Scale Computing HC3.

6.11.3 Настройка виртуального устройства

После развертывания виртуального устройства необходимо настроить его таким образом, чтобы у него был доступ как к кластеру Scale Computing HC3, для которого оно будет обеспечивать защиту, так и к службе Кибер Бэкап Облачный.

Для настройки виртуального приложения

1. Войдите в учетную запись Scale Computing HC3.
2. Выберите виртуальную машину с программно-аппаратным комплексом 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 **Scale Computing** щелкните **Изменить** и укажите адрес кластера Scale Computing HC3 и учетные данные для доступа к нему:
   a. В поле **Имя/IP-адрес сервера** введите DNS-имя или IP-адрес кластера.
   b. В полях **Имя пользователя** и **Пароль** введите учетные данные для ученой записи администратора Scale Computing HC3.
      Убедитесь, что учтеная запись имеет роли, необходимые для операций с виртуальными машинами Scale Computing HC3. Дополнительную информацию об этих ролях см. в разделе "Агент для Scale Computing HC3: требуемые роли" (стр. 87).
   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.

Порядок защиты виртуальных машин в кластере Scale Computing HC3

1. Войдите в учетную запись Кибер Бэкап Облачный.
2. Откройте **Устройства** > **Scale Computing HC3**> <ваш кластер> или найдите машины в разделе **Устройства** > **Все устройства**.
3. Выберите нужные машины и примените к ним план защиты.

6.11.4 Агент для Scale Computing HC3: требуемые роли

В этом разделе описаны роли, необходимые для операций с виртуальными машинами Scale Computing HC3.

Операция	Роль
Резервное копирование виртуальной машины	Резервное копирование Создание/изменение ВМ
Восстановление на существующую виртуальную машину	Резервное копирование Создание/изменение ВМ Управление электропитанием ВМ Удаление ВМ Настройки кластера
Восстановление на новую виртуальную машину	Резервное копирование Создание/изменение ВМ Управление электропитанием ВМ Удаление ВМ Настройки кластера

6.12 Развертывание агента для Virtuozzo Hybrid Infrastructure (виртуальное устройство)

6.12.1 Перед началом

Этот программно-аппаратный комплекс представляет собой предварительно настроенную виртуальную машину, которая развертывается в Virtuozzo Hybrid Infrastructure. В ее состав входит агент защиты, который позволяет вам администрировать киберзащиту для всех виртуальных машин в кластере Virtuozzo Hybrid Infrastructure.

Примечание
Чтобы процессы резервного копирования с включенным параметром **Служба теневого копирования томов (VSS) для виртуальных машин** выполнялись правильно и захватывали данные в согласованном с приложениями состоянием, убедитесь, что на защищенных виртуальных машинах установлен и обновлен пакет инструментов Virtuozzo Guest Tools.

6.12.1.1 Системные требования для агента

При развертывании виртуального устройства можно выбрать одну из нескольких предварительно настроенных комбинаций виртуальных ЦП и ОЗУ (варианты). Кроме того, можно создать собственные варианты.

Для большинства операций оптимальной и достаточной является комбинация из 2 виртуальных ЦП и 4 ГБ ОЗУ (так называемый средний вариант). 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 ГБ.

6.12.1.2 Сколько агентов необходимо?

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

Если в кластере несколько агентов, виртуальные машины автоматически равномерно 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, вы понимаете, что для необходимой пропускной способности требуется больше агентов, и развертываете в кластере дополнительное виртуальное устройство. Сервер управления назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится. Если агент удаляется с сервера управления, то машины, назначенные этому агенту, распределяются между оставшимися агентами. Однако этого не происходит, если агент повреждается или вручную удаляется с узла Virtuozzo Hybrid Infrastructure. Перераспределение начнется только после удаления такого агента из веб-интерфейса Кибер Бэкап Облачный.

Порядок получения информации об агенте, управляющем конкретной машиной

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

6.12.1.3 Ограничения

- Программно-аппаратный комплекс Virtuozzo Hybrid Infrastructure невозможно развернуть удаленно.
- Резервное копирование виртуальных машин с поддержкой приложений не поддерживается.

6.12.2 Настройка сетей в Virtuozzo Hybrid Infrastructure

Перед развертыванием и настройкой виртуального устройства необходимо настроить сети в Virtuozzo Hybrid Infrastructure.

Требования к сети для агента для Virtuozzo Hybrid Infrastructure (виртуальное устройство)

- Для виртуального устройства требуются 2 сетевых адаптера.
- Виртуальное устройство должно быть подключено к сетям Virtuozzo с указанными ниже типами сетевого трафика:
  - Compute API (API вычислительной инфраструктуры)
  - Резервное копирование ВМ
  - ABGW Public (ABGW в общедоступной сети)
  - VM Public (ВМ в общедоступной сети)

Дополнительную информацию о настройке сетей см. в разделе Requirements for the compute cluster (Требования к вычислительному кластеру) документации Virtuozzo.

6.12.3 Настройка учетных записей пользователей в Virtuozzo Hybrid Infrastructure

Для настройки виртуального устройства понадобится учетная запись пользователя Virtuozzo Hybrid Infrastructure. Учетная запись должна иметь роль **Администратор** в домене **По умолчанию**. Дополнительную информацию о пользователях см. в разделе Managing domain users (Управление пользователями домена) в документации к Virtuozzo Hybrid Infrastructure. Убедитесь, что этой учетной записи предоставлен доступ ко всем проектам в домене **По умолчанию**.

Порядок предоставления доступа ко всем проектам в домене "По умолчанию"

1. Создайте файл среды для системного администратора. Для этого выполните указанный ниже сценарий в кластере Virtuozzo Hybrid Infrastructure, используя интерфейс командной строки OpenStack. Дополнительную информацию о подключении к этому интерфейсу см. в разделе Connecting to OpenStack command-line interface (Подключение к интерфейсу командной строки OpenStack) в документации к Virtuozzo Hybrid Infrastructure.

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

2. Используйте файл среды для авторизации последующих команд OpenStack:

```
. /etc/kolla/admin-openrc.sh
```

3. Выполните следующие команды:

```
openstack --insecure user set --project admin --project-domain Default --domain Default
<username>
openstack --insecure role add --domain Default --user <username> --user-domain Default
compute --inherited
```

<имя_пользователя> – это учетная запись Virtuozzo Hybrid Infrastructure с ролью **Администратор** в домене **По умолчанию**. Виртуальное устройство будет использовать эту учетную запись для резервного копирования и восстановления виртуальных машин в любом дочернем проекте в домене **По умолчанию**.

6.12.3.1 Пример

```
su - vstoradmin
kolla-ansible post-deploy
exit
. /etc/kolla/admin-openrc.sh
openstack --insecure user set --project admin --project-domain Default --domain Default johndoe
openstack --insecure role add --domain Default --user johndoe --user-domain Default compute --
inherited
```

Для управления резервными копиями виртуальных машин в другом домене (не **По умолчанию**), выполните также следующую команду.

Порядок предоставления доступа ко всем проектам в другом домене

```
openstack --insecure role add --domain <domain name> --inherited --user <username> --user-
domain Default admin
```

<имя домена> – это домен для проектов, в котором учетная запись <имя_пользователя> будет иметь доступ.

6.12.3.2 Пример

```
openstack --insecure role add --domain MyNewDomain --inherited --user johndoe --user-domain
Default admin
```

После предоставления доступа к проектам проверьте, что роли назначены учетной записи.

Порядок проверки назначенных ролей

```
openstack --insecure role assignment list --user <username> --names
```

<username> — это учетная запись Virtuozzo Hybrid Infrastructure.

6.12.3.3 Пример

```
openstack --insecure role assignment list --user johndoe --names -c Role -c User -c Project -c
Domain
+--------------+-----------------+---------+-------------+
| Role         | User            | Project | Domain      |
+--------------+-----------------+---------+-------------+
| admin        | johndoe@Default |         | MyNewDomain |
| compute      | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
| domain_admin | johndoe@Default |         | Default     |
+--------------+-----------------+---------+-------------+
```

В этом примере параметры -c Role, -c User, -c Project и -c Domain используются для сокращения вывода команды, чтобы он поместился на странице.

Чтобы узнать, какие действующие роли назначены учетной записи во всех проектах, выполните следующую команду.

Порядок проверки действующих ролей во всех проектах

```
openstack --insecure role assignment list --user <username> --names --effective
```

<username> — это учетная запись Virtuozzo Hybrid Infrastructure.

6.12.3.4 Пример

```
openstack --insecure role assignment list --user johndoe --names --effective  -c Role -c User -c
Project -c Domain
+--------------+-----------------+-----------------+---------+
| Role         | User            | Project         | Domain  |
+--------------+-----------------+-----------------+---------+
| domain_admin | johndoe@Default |                 | Default |
| compute      | johndoe@Default | admin@Default   |         |
| compute      | johndoe@Default | service@Default |         |
| domain_admin | johndoe@Default | admin@Default   |         |
| domain_admin | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | service@Default |         |
| member       | johndoe@Default | service@Default |         |
| reader       | johndoe@Default | service@Default |         |
| project_user | johndoe@Default | admin@Default   |         |
| member       | johndoe@Default | admin@Default   |         |
| reader       | johndoe@Default | admin@Default   |         |
| project_user | johndoe@Default |                 | Default |
| member       | johndoe@Default |                 | Default |
```

```
| reader     | johndoe@Default |              | Default |
+------------+-----------------+--------------+---------+
```

В этом примере параметры -c Role, -c User, -c Project и -c Domain используются для сокращения вывода команды, чтобы он поместился на странице.

6.12.4 Развертывание шаблона QCOW2

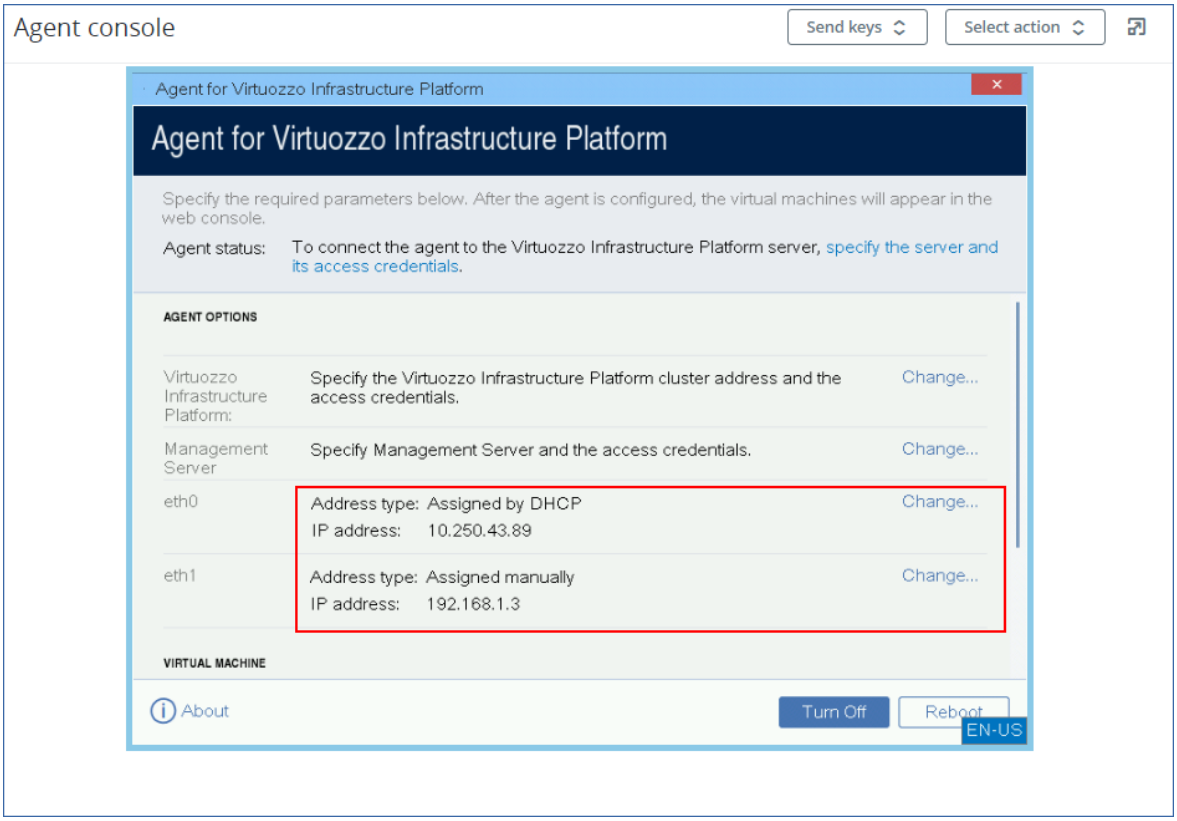
1. Войдите в учетную запись Кибер Бэкап Облачный.
2. Последовательно выберите пункты **Устройства** > **Все устройства** > **Добавить** > **Virtuozzo Hybrid Infrastructure**.
   ZIP-архив загрузится на машину.
3. Распакуйте ZIP-архив. Он содержит файл образа .qcow2.
4. Войдите в учетную запись Virtuozzo Hybrid Infrastructure.
5. Добавьте файл образа .qcow2 в вычислительный кластер Virtuozzo Hybrid Infrastructure следующим образом:
   - На вкладке **Compute** (Вычислительная среда) > **Виртуальные машины** > **Образы** щелкните **Добавить образ**.
   - В окне **Добавить образ** щелкните **Обзор**, а затем выберите файл .qcow2.
   - Укажите имя образа, выберите тип **Generic Linux OS** (Универсальная ОС Linux), а затем щелкните **Добавить**.
6. На вкладке **Compute** (Вычислительная среда) > **Виртуальные машины** > **Виртуальные машины** щелкните **Создать виртуальную машину**. Откроется окно, в котором необходимо будет указать следующие параметры:
   - Имя новой виртуальной машины.
   - В поле **Deploy from** (Развернуть из) выберите **Образ**.
   - В окне **Образы** выберите файл образа .qcow2 программно-аппаратного комплекса, а затем щелкните **Готово**.
   - В окне **Тома** не нужно добавлять никакие тома. Будет достаточно тома, который автоматически добавлен для системного диска.
   - В окне **Вариант** выберите нужную комбинацию виртуальных процессоров ЦП и объема ОЗУ, а затем щелкните **Готово**. Как правило, достаточно 2 виртуальных ЦП и 4 ГБ ОЗУ.
   - В окне **Сетевые интерфейсы** щелкните **Добавить** выберите виртуальную сеть типа *общедоступная*, а затем щелкните **Добавить**. Она появится в списке **Сетевые интерфейсы**. Если в вашей установке несколько физических сетей (и соответственно несколько общедоступных виртуальных сетей), повторите это действие и выберите необходимые виртуальные сети.
7. Нажмите кнопку **Готово**.
8. В окне **Создать виртуальную машину** щелкните **Развернуть**, чтобы создать и загрузить виртуальную машину.

6.12.5 Настройка виртуального устройства

После развертывания виртуального устройства необходимо настроить его таким образом, чтобы у него был доступ как к кластеру Virtuozzo Hybrid Infrastructure, для которого оно будет обеспечивать защиту, так и к облачной службе Кибер Бэкап Облачный.

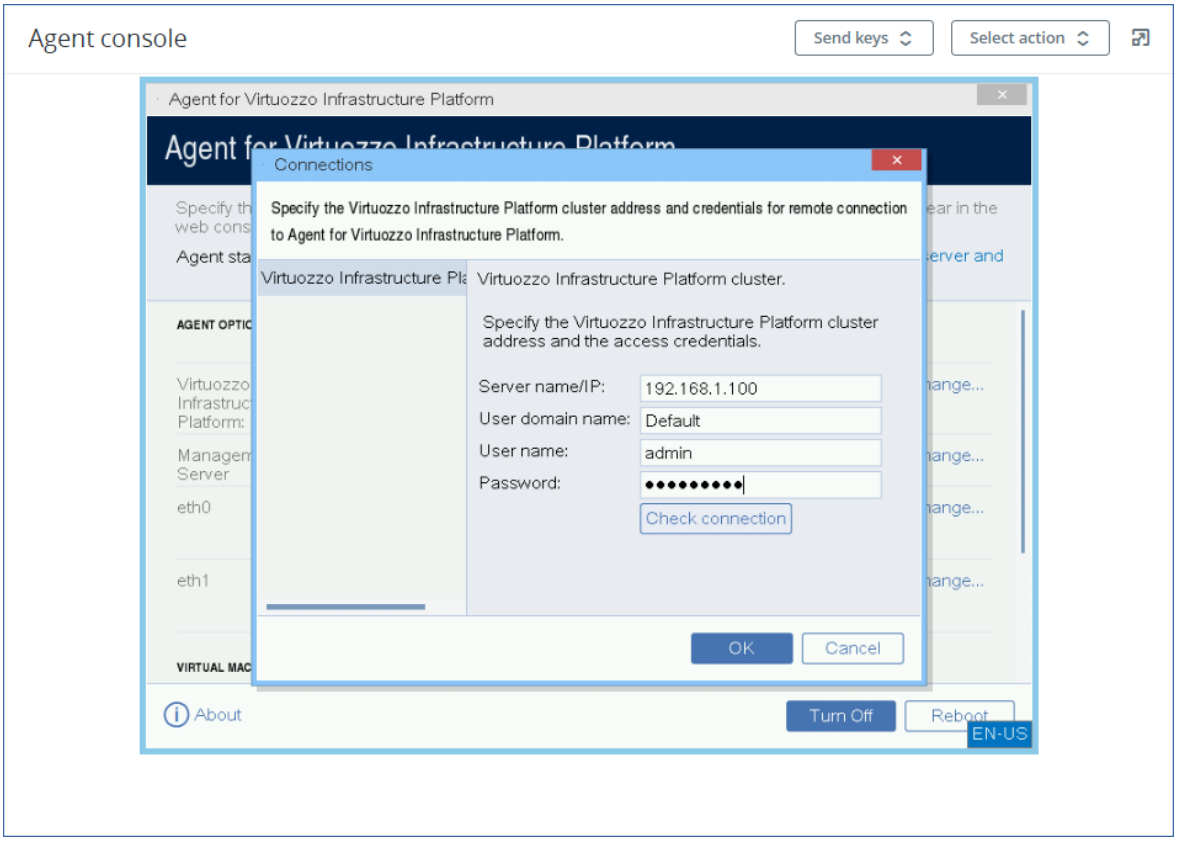
Для настройки виртуального приложения

1. Войдите в учетную запись Virtuozzo Hybrid Infrastructure.
2. На вкладке **Compute** (Вычислительная среда) > **Виртуальные машины** > **Виртуальные машины** выберите созданную виртуальную машину. После этого щелкните **Консоль**.
3. Настройте сетевые интерфейсы программно-аппаратного комплекса. Для настройки может быть доступен один интерфейс или несколько интерфейсов – это зависит от количества виртуальных сетей, которые использует программно-аппаратный комплекс. Убедитесь, что автоматически назначенные адреса DHCP (если есть) действительны в сетях, которые использует ваша виртуальная машина, или назначьте их вручную.

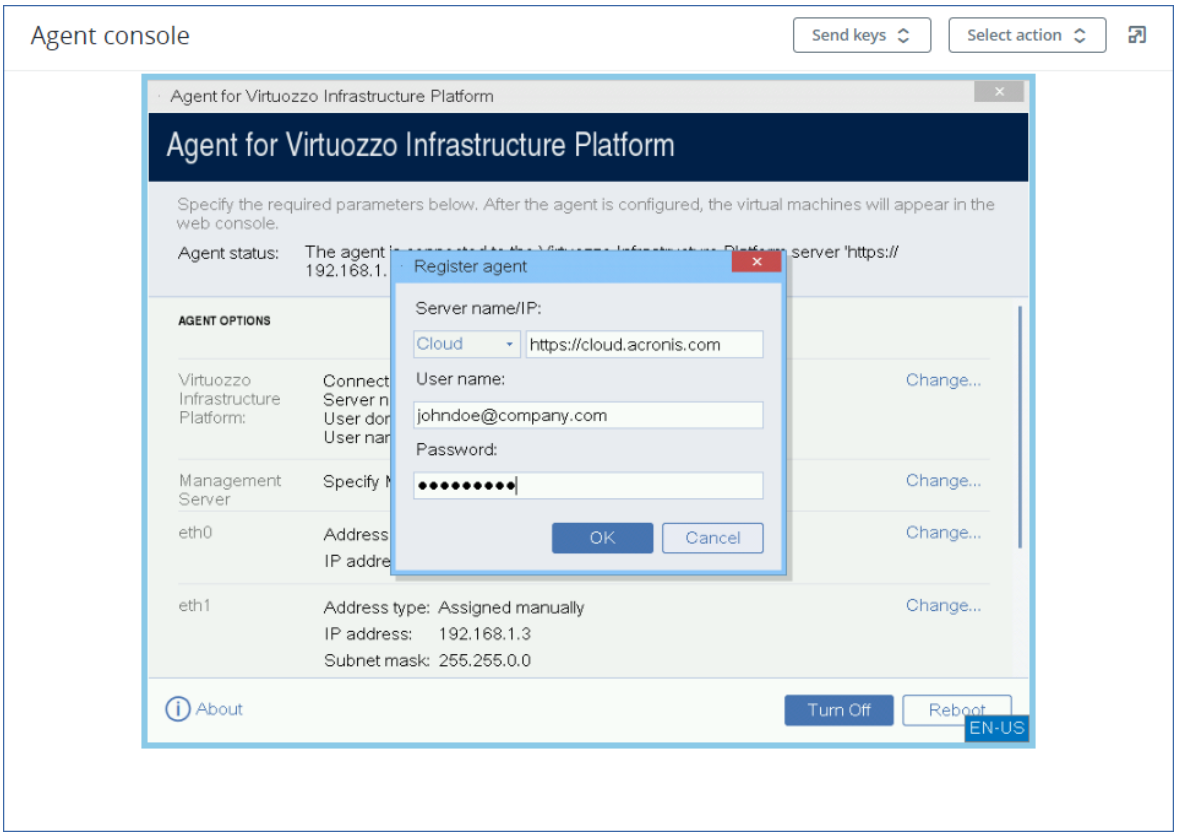


4. Укажите адрес кластера и учетные данные Virtuozzo:
   - DNS-имя или IP-адрес кластера Virtuozzo Hybrid Infrastructure. Это адрес узла управления данного кластера. По умолчанию автоматически устанавливается порт 5000. Если нужно использовать другой порт, укажите его вручную.
   - В поле **Имя домена пользователя** укажите домен в Virtuozzo Hybrid Infrastructure. Например, **По умолчанию**.
     В имени домена учитывается регистр символов.

- В полях **Имя пользователя** и **Пароль** введите учетные данные для ученой записи Virtuozzo Hybrid Infrastructure с ролью **Администратор** в указанном домене. Дополнительную информацию о пользователях, ролях и доменах см. в разделе Настройка учетных записей пользователей в Virtuozzo Hybrid Infrastructure.



5. Укажите адрес сервера управления Кибер Бэкап Облачный и учетные данные для доступа к нему.



Порядок защиты виртуальных машин в кластере Virtuozzo Hybrid Infrastructure

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

6.13 Развертывание агента для oVirt (виртуальное устройство)

6.13.1 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.

6.13.1.1 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.

6.13.1.2 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.

6.13.1.3 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)

6.13.2 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. 99).
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. 98)

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 acronis_virtual_appliance.

6.13.3 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. 99).
   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.

6.13.4 Агент для oVirt: требуемые роли и порты

6.13.4.1 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

6.13.4.2 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.

6.14 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.

6.14.1 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.

6.14.2 Шаг 1. Формирование маркера регистрации

Маркер регистрации передает ваше удостоверение в программу установки, не сохраняя имя входа и пароль для консоли службы. Это позволяет зарегистрировать любое количество машин в учетной записи. Чтобы обеспечить более высокий уровень безопасности, маркер имеет ограниченный срок действия.

Формирование маркера регистрации

1. Войдите в консоль службы с учетными данными той учетной записи, для которой необходимо назначить машины.
2. Щелкните **Все устройства** > **Добавить**.
3. Прокрутите вниз до поля **Маркер регистрации** и нажмите кнопку **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 щелкните **Создать**.

4. Укажите срок действия маркера и нажмите кнопку **Создать маркер**.
5. Скопируйте маркер или запишите его. Сохраните маркер, если он понадобится в будущем.

   Для просмотра уже сформированных маркеров и управления ими можно щелкнуть **Управление активными маркерами**. Имейте в виду, что из соображений безопасности в этой таблице не отображаются полные значения маркеров.

6.14.3 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.

6.14.4 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**.

6.15 Обновление агентов

Виртуальные устройства указанных ниже версий необходимо обновить только через консоль службы:

- Агент для VMware (виртуальное устройство): версия 12.5.23094 и более поздние
- Агент для Virtuozzo Hybrid Infrastructure (виртуальное устройство): версия 12.5.23094 и более поздние

Агенты указанных ниже версий также можно обновить через консоль службы:

- Агент для Windows, агент для VMware (Windows), агент для Hyper-V: 11.9.191 и более поздние версии

- Агент для Linux – 11.9.179 и более поздние версии
- Другие агенты: можно обновить любую версию

Чтобы найти версию агента, выберите машину и нажмите кнопку **Сведения**.

Чтобы обновить агент более ранней версии, загрузите и установите новую версию вручную. Чтобы найти ссылки загрузки, последовательно выберите пункты **Все устройства** > **Добавить**.

6.15.0.1 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 https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

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.

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.

Обновление определений киберзащиты на машине

1. Щелкните **Настройки** > **Агенты**.
2. Выберите машину, на которой необходимо обновить определения киберзащиты, и щелкните **Обновить определения**. Машина должна быть включена.

Порядок назначения роли "Средство обновления" агенту

1. Щелкните **Настройки** > **Агенты**.
2. Выберите машину, которой необходимо назначить Средство обновления, щелкните **Подробнее**, выберите раздел **Определения киберзащиты** и включите параметр **Используйте этот агент для скачивания и распространения исправлений и обновлений**.

Порядок удаления кэшированных данных на агенте

1. Щелкните **Настройки** > **Агенты**.
2. Выберите машину, на которой необходимо очистить кэшированные данные (устаревшие файлы обновления и данные управления исправлениями), и щелкните **Очистить кэш**.

6.16 Удаление агентов

6.16.1 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**.

6.16.2 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.

6.16.3 В macOS

1. Дважды щелкните DMG-файл установки.
2. Дождитесь, пока операционная система подключит образ установочного диска.
3. В данном образе дважды щелкните **Удалить**.
4. При необходимости введите учетные данные администратора.
5. Подтвердите операцию.

6.16.4 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.

6.16.5 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 удаление 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**.

6.17 Настройки безопасности

Для настройки общих параметров защиты для Кибер Бэкап Облачный выберите **Настройки**> **Защита** в консоли службы.

6.17.1 Автоматические обновления компонентов

По умолчанию все агенты могут подключаться к Интернету и скачивать обновления.

Администратор может минимизировать сетевой трафик. Для этого нужно выбрать один или несколько агентов в среде и назначить им роль ъ«Средство обновления». Такие выделенные агенты смогут подключаться к Интернету и скачивать обновления. Все остальные агенты смогут подключаться к выделенным агентам, которым назначена роль ъ«Средство обновления»,

используя технологию одноранговых подключений, для последующего скачивания с них обновлений.

Агенты без роли «Средство обновления» смогут подключиться к Интернету, если в среде нет агента с ролью «Средство обновления», или в течение пяти минут невозможно установить подключение к выделенному агенту с ролью «Средство обновления».

Перед назначением агенту роли «Средство обновления» убедитесь, что компьютер, на котором выполняется агент, имеет достаточно ресурсов, высокоскоростное подключение к Интернету и достаточно места на диске.

Порядок подготовки машины для роли «Средство обновления»

1. На машине агента, на которой нужно включить роль «Средство обновления», примените следующие правила:
   - Входящие порты «updater_incoming_tcp_ports»: разрешите подключение к портам TCP 18018 и 6888 для всех профилей брандмауэра (общедоступный, частный и домен).
   - Входящие порты «updater_incoming_udp_ports»: разрешите подключение к порту UDP 6888 для всех профилей брандмауэра (общедоступный, частный и домен).
2. Перезапустите службу Agent Core.
3. Перезапустить службу брандмауэра.

Если эти правила не применены, и брандмауэр включен, одноранговые агенты скачают обновления с облака.

Порядок назначения роли "Средство обновления" агенту защиты

1. В консоли службы последовательно выберите пункты **Настройки** > **Агенты**.
2. Выберите машину, которой необходимо назначить роль "Средство обновления".
3. Щелкните **Сведения** и включите параметр **Используйте этот агент для скачивания и распространения исправлений и обновлений**.

Ниже описан принцип работы обновления с однорангового хоста.

1. Агент с ролью "Средство обновления" проверяет согласно расписанию файл индекса, предоставленный поставщиком услуги для обновления основных компонентов.
2. Агент с ролью "Средство обновления" начинает скачивать и распространять обновления на все агенты.

Роль «Средство обновления» можно назначить нескольким агентам в среде. Таким образом, если агент с ролью «Средство обновления» станет недоступным, другие агенты с этой ролью могут стать источником обновлений определения.

6.17.2 Обновление определений Кибер Бэкап согласно расписанию

На вкладке **Расписание** можно задать расписание автоматического обновления определений Кибер Бэкап для следующих компонентов:

- Защита от вредоносных программ
- Оценка уязвимостей
- Управление исправлениями

Чтобы изменить параметры обновлений определения, выберите пункты **Настройки** > **Защита** > **Обновление определений защиты** > **Расписание**.

Тип расписания:

- **Ежедневно**: выберите дни недели для обновления определений.

  Запускать в: выберите время для обновления определений.
- **Каждый час**: задайте более детализированное ежечасное расписание для обновления определений.

  Запускать каждые: укажите периодичность запуска обновлений.

  С ... **До**: укажите определенный диапазон времени, в пределах которого будет выполняться автоматическое обновление определений.

6.17.3 Обновление определений киберзащиты по требованию

Порядок обновления определений киберзащиты для определенной машины по требованию

1. В консоли службы последовательно выберите пункты **Настройки** > **Агенты**.
2. Выберите машины, на которых необходимо обновить определения киберзащиты, и щелкните **Обновить определения**.

6.17.4 Хранилище кэша

Расположение кэшированных данных:

- На машинах Windows: C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache
- На машинах Linux: /opt/acronis/var/atp-downloader/Cache
- На машинах macOS: /Library/Application Support/Acronis/Agent/var/atp-downloader/Cache

Чтобы изменить параметры хранения кэша, выберите пункты **Настройки** > **Защита** > **Обновление определений защиты** > **Хранилище кэша**.

В разделе **Устаревшие файлы обновления и данные управления исправлениями** укажите период времени, по истечении которого необходимо удалить кэшированные данные.

Максимальный размер хранилища кэша (ГБ) для агентов:

- **Роль "Средство обновления"**: определите размер хранилища для кэша на машинах с ролью "Средство обновления".
- **Другие роли**: определите размер хранилища для кэша на других машинах.

6.17.5 Удаленное подключение

Щелкните **Подключение к удаленному рабочему столу**, чтобы включить удаленное подключение к машинам через клиент RDP или клиент HTML5. Если оно отключено, параметры **Подключиться через клиент RDP** / **Подключиться через клиент HTML5** будут скрыты в консоли службы, и пользователи не смогут подключиться к машинам удаленно. Этот параметр влияет на всех пользователей вашей организации.

Щелкните **Предоставить общий доступ к подключению к удаленному рабочему столу**, чтобы включить общий доступ к удаленному подключению для пользователей. После этого при выборе машины в меню справа появится параметр **Предоставить общий доступ к удаленному подключению**. Вы сможете сгенерировать ссылку, чтобы предоставить ее пользователям для доступа к удаленной машине.

6.18 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**.

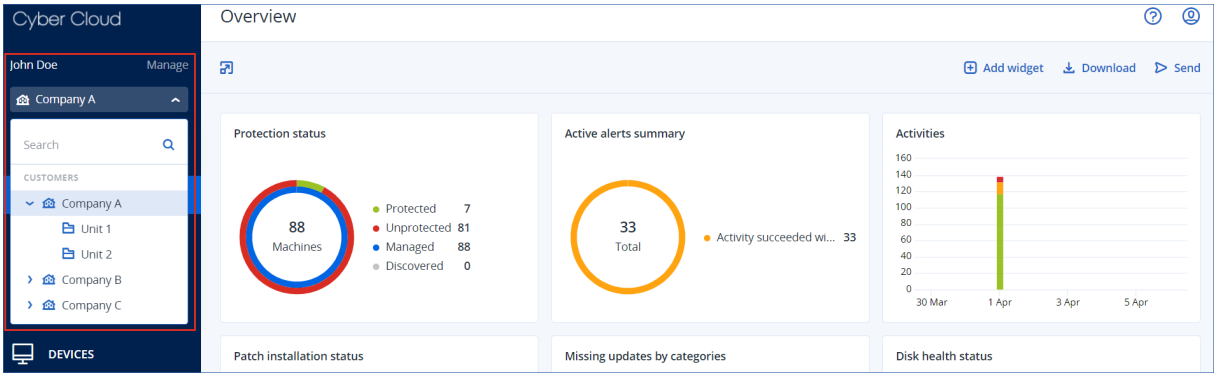
7 Консоль службы

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.

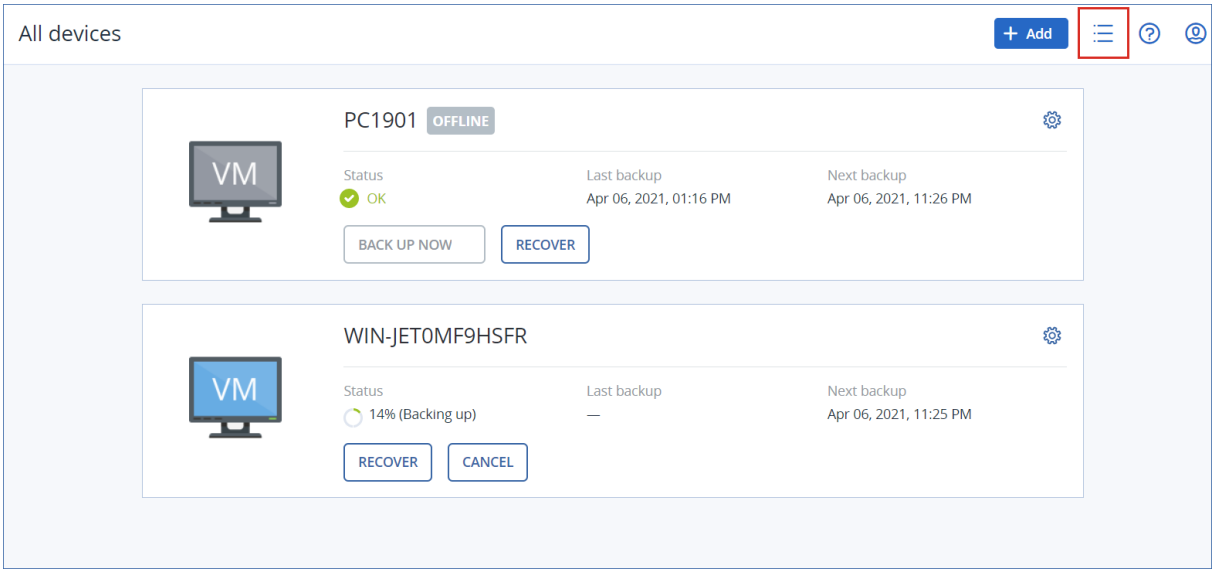
В консоли службы можно получить доступ к дополнительным службам или функциям Кибер Бэкап Облачный, таким как "File Sync & Share", "Антивирус и защита от вредоносных программ", "Управление исправлениями", ъ"Управление устройствами" и "Оценка уязвимостей". Их тип и номер зависят от лицензии Кибер Бэкап 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**.

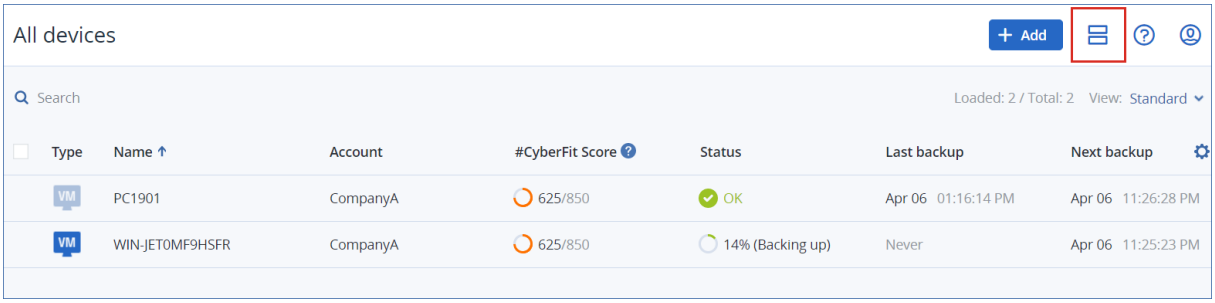


Раздел **Устройства** доступен в простом и табличном представлении. Для переключения между ними используется значок в правом верхнем углу.

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.

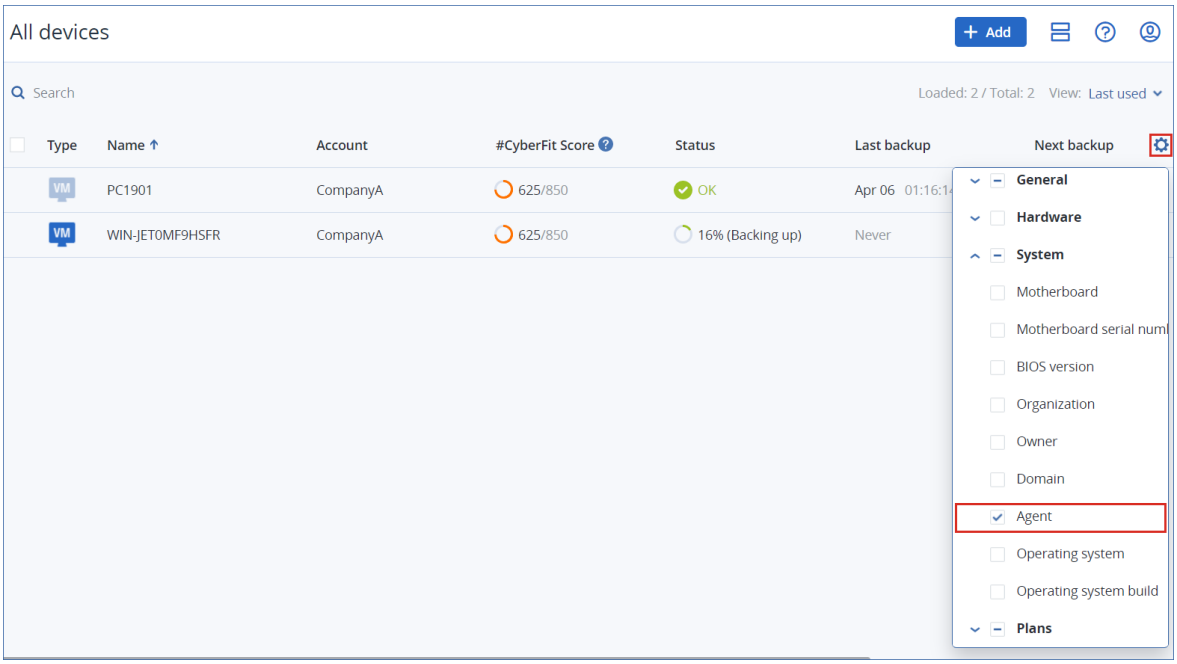
Резервные копии хостов ESXi и виртуальных машин на указанных ниже платформах виртуализации могут создаваться агентом, который не установлен на них, т. е. в режиме без агента:

- Hyper-V
- VMware
- Virtuozzo Hybrid Infrastructure
- Scale Computing
- 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, агент для Virtuozzo Hybrid Infrastructure, агент для Scale Computing 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. 104).

8 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.

8.1 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.

8.2 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.

8.3 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.

8.4 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 группой, 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**.

8.5 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**.

8.5.1 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' • 'macosx'	osType IN ('linux', 'macosx')	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

8.5.2 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'

8.6 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".

9 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 списке исправлений, карантине, канале угроз, оповещениях и действиях, доступны для просмотра только текущему клиенту и его субклиентам. Данные, относящиеся к родительского клиенту, не отображаются.

10 План защиты и модули

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

- Резервная копия: позволяет создавать резервную копию источников данных в локальном или облачном хранилище данных.

Используйте план защиты для защиты источников данных Создавая гибкие планы для разных потребностей бизнеса, различные модули можно включить и отключить, задать их настройки.

10.1 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.
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**.

10.2 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.

10.2.1 Применение нескольких планов к устройству

К одному устройству можно применить несколько планов защиты. В результате получится комбинация разных планов защиты, назначенных одному устройству. Например, можно применить план, в котором включен только модуль "Антивирус и защита от вредоносных программ", и еще один план, который содержит только модуль резервного копирования. 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.

10.2.2 Разрешение конфликтов плана

10.2.2.1 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.

10.2.2.2 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.

10.2.2.3 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.

10.3 Операции с планами защиты

10.3.0.1 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.

11 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.

11.1 Резервное копирование

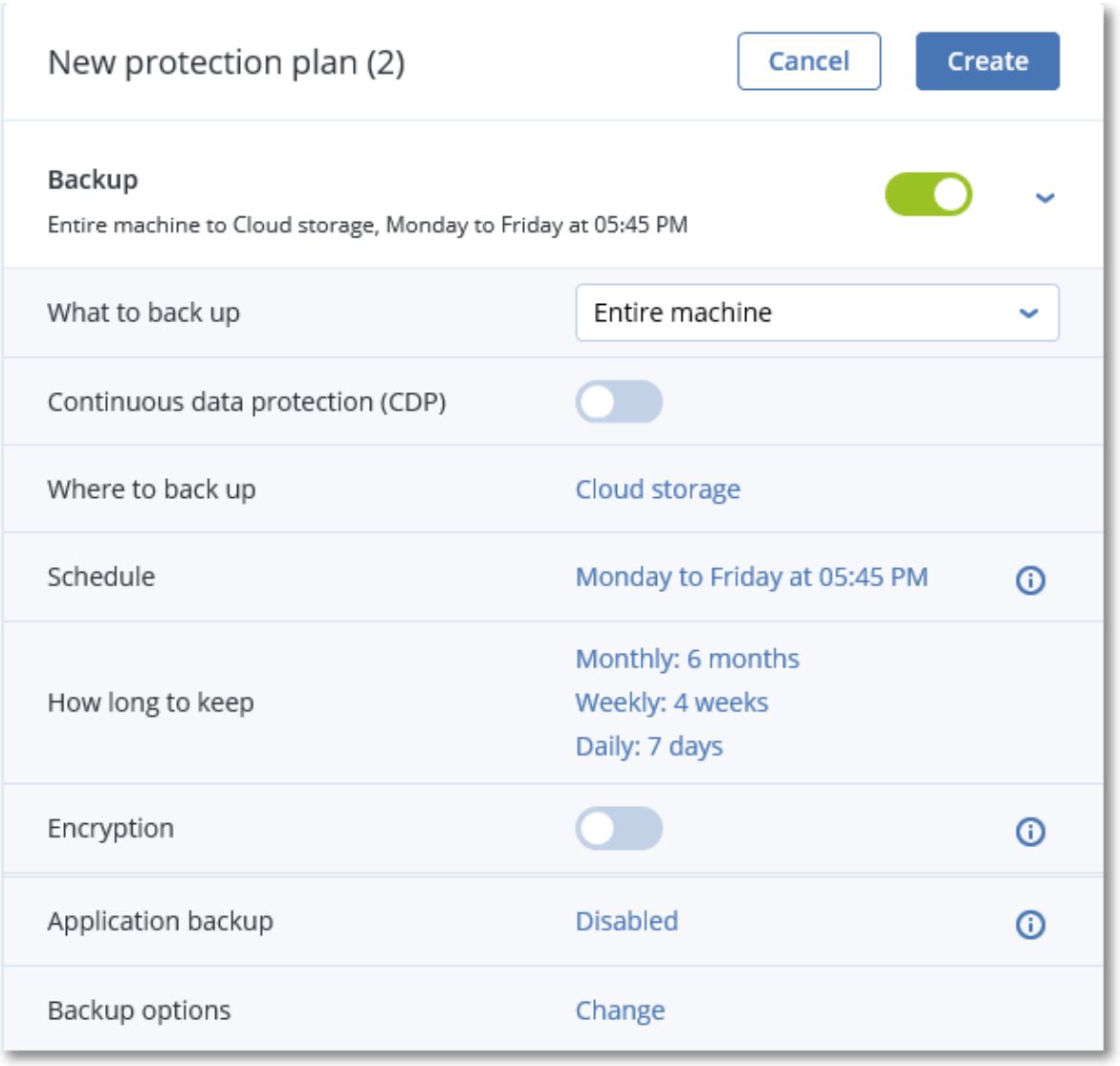
План защиты с включенным модулем "Резервное копирование" – это набор правил, определяющий способ защиты указанных данных на конкретной машине.

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.

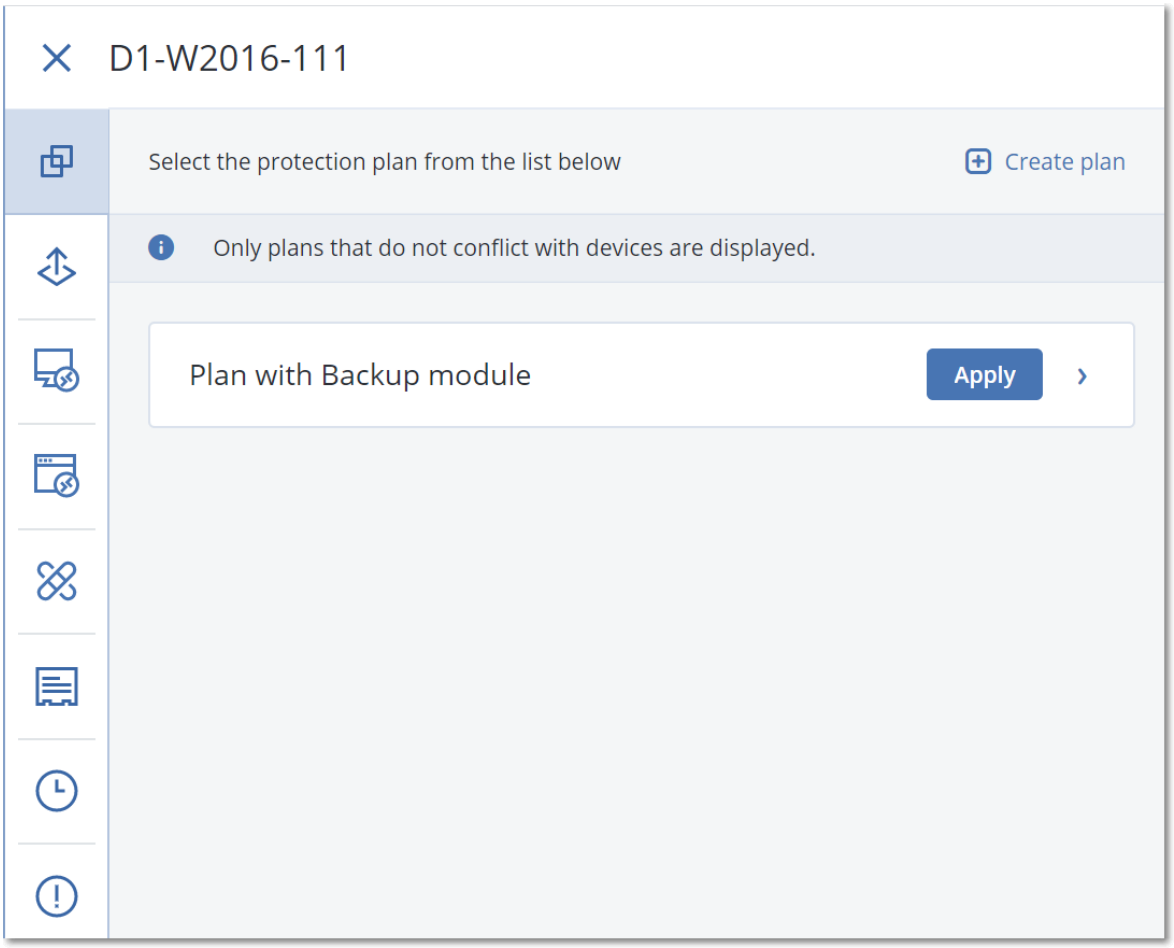


4. [Необязательно] Для изменения имени плана защиты щелкните имя по умолчанию.
5. [Необязательно] Чтобы изменить параметры модуля "Резервное копирование", щелкните соответствующую настройку панели плана защиты.
6. [Необязательно] Чтобы изменить параметры резервного копирования, щелкните **Изменить** 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**.

11.2 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[1])	Непосредственный выбор Правила политики Фильтры файлов	Локальная папка Сетевая папка NFS*	Всегда инкрементное (один файл) Всегда полное Еженедельно полное,	По возрасту резервной копии (одно правило на набор

[1]Компьютер, резервное копирование которого выполняется с помощью агента, установленного в операционной системе.

		Зона безопасности**	ежедневно инкрементное	
Диски/тома (виртуальные машины[1])	Правила политики Фильтры файлов	Локальная папка Сетевая папка NFS*	Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) Всегда инкрементное (один файл)*** Настраиваемый вариант (П-Д-И)	резервных копий) По количеству резервных копий По общему размеру резервных копий**** Хранить бессрочно
Файлы (только физические машины[2])	Непосредственный выбор Правила политики Фильтры файлов	Облако Локальная папка Сетевая папка NFS* Зона безопасности**	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*		
Состояние системы Базы данных SQL Базы данных Exchange	Непосредственный выбор	Облако Локальная папка Сетевая папка	Всегда полное Еженедельно полное, ежедневно инкрементное Настраиваемый вариант (П-И)	

* Резервное копирование в общие папки NFS недоступно в Windows.

** Невозможно создать Зону безопасности на компьютере Mac.

*** 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.

[1]Виртуальная машина, резервное копирование которой выполняется на уровне гипервизора сторонним агентом, например агентом для VMware или агентом для Hyper-V. Виртуальная машина, которая содержит агент, воспринимается службой резервного копирования как физическая.
[2]Компьютер, резервное копирование которого выполняется с помощью агента, установленного в операционной системе.

11.3 Выбор данных для резервного копирования

11.3.1 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.

11.3.1.1 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**.

11.3.1.2 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, Linux и macOS

- [All Volumes] позволяет выбрать все тома машин с Windows и все подключенные тома машин с Linux или macOS.

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
```

Правила для macOS

- [Disk 1] позволяет выбрать первый диск машины, включая все тома на нем. Чтобы выбрать другой диск, введите соответствующий номер.

11.3.1.3 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, файлы и папки, указанные 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.

Mac

Резервная копия диска или тома содержит все файлы и папки выбранного диска или тома или тома, а также описание способа размещения тома.

Исключены следующие элементы

- Метаданные системы, такие как журнал файловой системы и индекс Spotlight
- Корзина
- Резервное копирование Time Machine

Резервное копирование дисков и томов в ОС Mac выполняется на уровне файла. Восстановление резервных копий дисков и томов на «голое железо» (восстановление исходного состояния системы) возможно, но режим посекторного резервного копирования будет недоступен.

11.3.2 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.

11.3.2.1 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**.

11.3.2.2 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.

Правила выбора для macOS

- Полный путь к файлу или каталогу.
- Шаблоны
  - [All Profiles Folder] позволяет выбрать каталог **/Users**. В этой папке по умолчанию размещены все профили пользователя.

Примеры:

- Чтобы создать резервную копию файла **file.txt** на рабочем столе, укажите **/Users/<username>/Desktop/file.txt**, где <username> — ваше имя пользователя.
- Чтобы создать резервные копии домашних каталогов всех пользователей, укажите **/Users**.
- Чтобы создать резервную копию каталога, в котором установлены приложения, укажите **/Applications**.

11.3.3 Выбор состояния системы

Резервную копию состояния системы можно создавать на машинах с Windows Vista и ОС более поздних версий.

Для этого в области **Элементы для резервного копирования** выберите вариант **Состояние системы**.

В резервную копию состояния системы включаются файлы перечисленных ниже компонентов.

- Конфигурация планировщика задач
- Хранилище метаданных VSS
- Конфигурация счетчика производительности
- Служба MSSearch
- Фоновая интеллектуальная служба передачи (BITS)
- Реестр
- Инструментарий управления Windows (WMI)
- База данных регистрации классов служб компонентов

11.3.4 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.

11.4 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 или macOS)

  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 «Информация о разделе Зона безопасности».

11.4.1 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**.

11.4.2 О программе Зона безопасности

Зона безопасности – это безопасный раздел на диске машины, для которой создана резервная копия. В этом разделе могут храниться диски или файлы этой машины.

Если на диске произойдет физический сбой, резервные копии в разделе Зона безопасности могут быть утрачены. Поэтому Зона безопасности не должен быть единственным хранилищем резервных копий. В корпоративных средах Зона безопасности можно представить как вспомогательное хранилище резервных копий, когда обычное хранилище временно недоступно или подключено через медленный или загруженный канал.

11.4.2.1 Почему нужно использовать раздел Зона безопасности?

Зона безопасности:

- обеспечивает восстановление того же диска, на котором находится резервная копия этого диска;
- обеспечивает экономный и удобный метод защиты данных при неправильной работе программного обеспечения, вирусной атаке или ошибках, вызванных человеческим фактором;
- устраняет необходимость в отдельном носителе или сетевом подключении для резервного копирования или восстановления данных; Это особенно полезно для пользователей, которые меняют место расположения.
- Может служить первичным назначением при использовании репликации резервных копий.

11.4.2.2 Ограничения

- Зона безопасности невозможно организовать на компьютере Mac.
- Зона безопасности – это раздел на базовом диске. Его 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 раздел Зона безопасности. Это не влияет на процедуру резервного копирования и его скорость.
- Зона безопасности не поддерживает формат одного файла резервной копии[1]. При изменении назначения на раздел Зона безопасности в плане защиты, который имеет схему резервного копирования **Всегда инкрементное (один файл)**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

[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.

11.4.2.3 Преобразование диска в результате создания раздела Зона безопасности

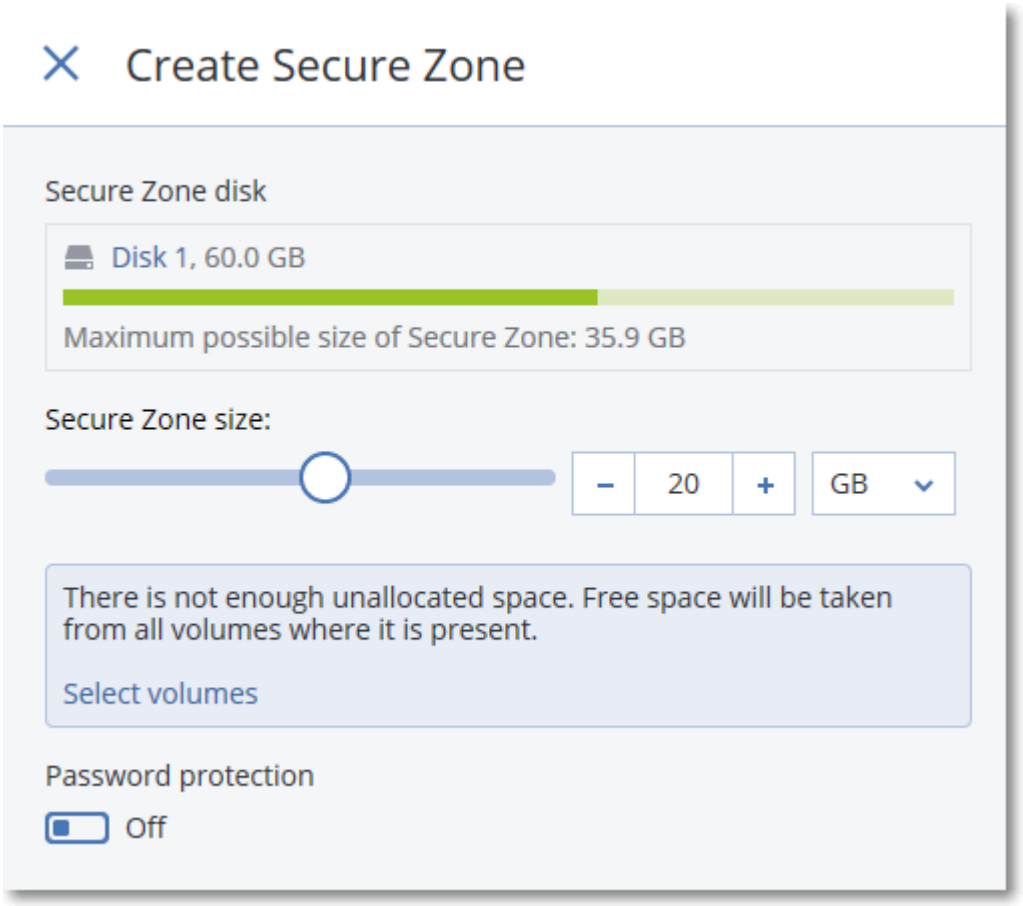
- Зона безопасности всегда создается в конце жесткого диска.
- Если в конце диска нераспределенного пространства нет или недостаточно, но существует нераспределенное пространство между томами, то эти тома будут перемещены, чтобы добавить больше нераспределенного пространства в конец диска.
- Если все незанятое пространство собрано, но его не хватает, то программа заберет свободное пространство из томов по выбору, пропорционально уменьшив их размер.
- Тем не менее на томе должно быть свободное пространство для работы операционной системы и приложений, например для создания временных файлов. Программа не будет уменьшать размер тома, на котором свободное пространство меньше или равно 25 % общего объема тома. Только если все тома на диске будут иметь 25 % или меньше свободного пространства, программа продолжит пропорциональное уменьшение томов.

Как следует из приведенных выше соображений, не рекомендуется указывать максимальный возможный размер раздела Зона безопасности. Следствием этого будет отсутствие свободного пространства на любом томе, что может привести к нестабильной работе операционной системы или приложений либо даже к невозможности их запуска.

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

11.4.2.4 Порядок создания Зона безопасности

1. Выберите машину, на которой необходимо создать раздел Зона безопасности.
2. Щелкните **Сведения** > **Создать Зона безопасности** .
3. В разделе **Диск Зона безопасности** щелкните **Выбрать**, выберите жесткий диск (если их несколько), на котором нужно создать зону.
   Программа рассчитает максимальный возможный размер раздела Зона безопасности.
4. Введите размер Зона безопасности или перетащите ползунок, чтобы выбрать любой размер в диапазоне между минимальным и максимальным.
   Минимальный размер зоны 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.

   Для доступа к резервным копиям, расположенным в разделе Зона безопасности, необходимо будет указать пароль. 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 раздел Зона безопасности.

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

11.4.2.5 Порядок удаления Зона 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 раздел Зона безопасности будет удален вместе со всеми содержащимися в нем резервными копиями.

11.5 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, запанирован к запуску в 21:00, то процесс резервного копирования на каждой машине начнется в 21:00 по местному времени данной машины.

11.5.1 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

[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.

создаваться несколько полных резервных копий, что приведет к существенным затратам времени и высокому объему сетевого трафика.

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, Exchange и состояния системы.

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».

11.5.2 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.

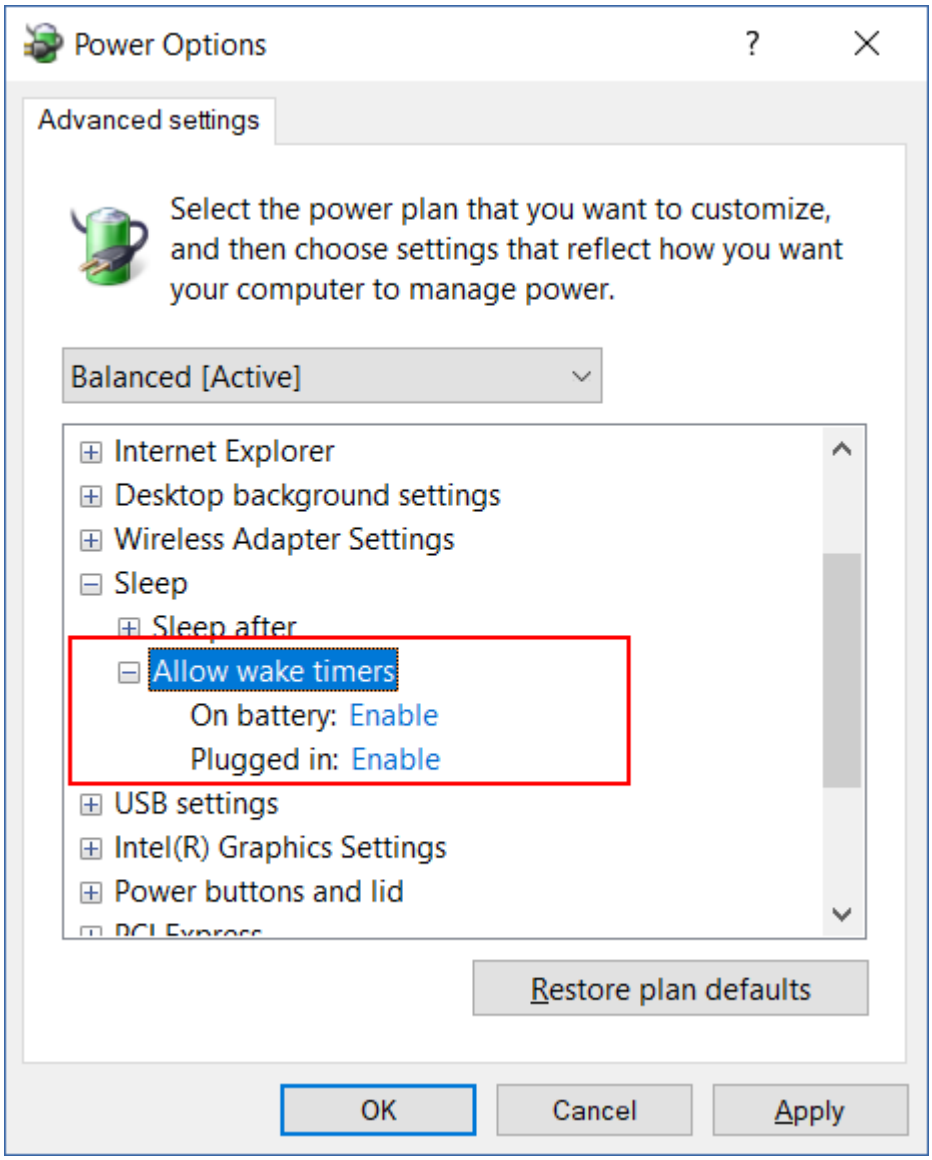
  В настройках модуля "Резервное копирование" в плане защиты последовательно выберите пункты **Параметры резервного копирования** > **Планирование**. Установите флажок **Распределять время запуска резервного копирования по доступному времени**, затем укажите максимальную задержку. Продолжительность задержки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

11.5.3 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, Linux и macOS.

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, macOS	Windows	Windows	Windows, Linux, macOS	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

11.5.3.1 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 аварийное полное резервное копирование данных будет запускаться автоматически, как только ОС Windows обнаружит вероятность отказа жесткого диска.

Для обзора событий и просмотра свойств событий используйте встраиваемое **Средство просмотра событий**, доступное в консоли **Управление компьютером**. Журнал **Безопасность** может быть открыт только из-под учетной записи, которая входит в группу **«Администраторы»**.

Свойства событий

Имя журнала

Указывает имя журнала. Выберите имя стандартного журнала (**Приложение**, **Безопасность** или **Система**) из списка или введите имя журнала. Пример: **Microsoft Office Sessions**

Источник события

Указывает источник события. Как правило, это программа или компонент системы, который вызвал событие. Пример: **диск**.

Любой источник событий с указанной строкой запустит запланированное резервное копирование. Этот параметр не является регистрозависимым. Таким образом, если указана строка **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**.

11.5.4 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, Linux и macOS.

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, macOS	Windows, Linux	Windows, Linux	Windows	Windows
Пользователи завершили сеанс	Windows	-	-	-	-
В интервале времени	Windows, Linux, macOS	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	-	-	-	-

11.5.4.1 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.

11.5.4.2 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.

11.5.4.3 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.

11.5.4.4 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.

11.5.4.5 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.

11.5.4.6 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. по ссылке https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

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.

11.5.4.7 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.

11.5.4.8 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 находится в указанном диапазоне, резервное копирование запустится немедленно.

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

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

11.6 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.

11.6.1 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.

  Это поведение можно изменить, используя опцию резервного копирования «Консолидация резервной копии».
- 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".

11.7 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.

11.8 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**.

11.9 Параметры резервного копирования

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

11.9.1 Доступность параметров резервного копирования

Набор доступных параметров резервного копирования зависит от следующих факторов:

- Среда, в которой работает агент (Windows, Linux, macOS).
- 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	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Virtuozzo	Windows
Оповещения	+	+	+	+	+	+	+	+	+	+
Консолидация резервных копий	+	+	+	+	+	+	+	+	+	-
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	+	-	-	+	-	-	+	+	-	+

11.9.2 Оповещения

11.9.2.1 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.

11.9.3 Консолидация резервных копий

Этот параметр определяет, нужно ли консолидировать резервные копии при очистке или при полном удалении цепочек резервных копий.

Значение по умолчанию: **Отключено**.

Консолидация – это процесс объединения двух и более последовательных резервных копий в одну резервную копию.

Если этот параметр включен, то резервная копия, которая должна быть удалена при очистке, консолидируется со следующей зависимой резервной копией (инкрементная или дифференциальная).

В противном случае данная резервная копия сохраняется до тех пор, пока все зависимые резервные копии не станут предметом для удаления. Это поможет избежать потенциально долгой консолидации, но требует дополнительного пространства для хранения резервных копий, удаление которых откладывается. Возраст или количество резервных копий могут превысить значения, заданные в правилах хранения.

Внимание
Необходимо учитывать, что консолидация – это просто один из методов удаления, но не альтернатива удалению. Итоговая резервная копия не будет содержать данные, которые присутствовали в удаленной резервной копии и отсутствовали в оставшейся инкрементной или дифференциальной резервной копии.

Этот параметр *не действует* в любом из следующих случаев:

- Местом назначения резервной копии является облачное хранилище данных.
- Используется схема резервного копирования **Всегда инкрементное (один файл)**.
- Используется формат резервной копии **Версии 12**.

Резервные копии, сохраненные в облачном хранилище данных, а также резервные копии в виде одного файла (форматы версий 11 и 12) всегда консолидированы, поскольку их внутренняя структура позволяет ускорить и упростить консолидацию.

Однако если используется формат версии 12 и при этом есть несколько цепочек резервных копий (каждая цепочка хранится в отдельном файле), консолидация работает только для последней цепочки. Все цепочки, за исключением первой, удаляются. Первая цепочка сжимается до минимально необходимого размера для хранения метаданных (~12 КБ). Эти метаданные требуются, чтобы обеспечить согласованность данных при одновременном выполнении операций чтения и записи. Сразу же после применения правила хранения резервные копии, входящие в эти цепочки, исчезают из графического интерфейса пользователя, хотя физически они существуют до удаления всей цепочки.

Во всех остальных случаях резервные копии, удаление которых отложено, помечаются значком корзины () в графическом пользовательском интерфейсе. Если удалить такую резервную копию, щелкнув значок X, будет выполнена консолидация.

11.9.4 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.

11.9.4.1 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**.

11.9.4.2 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**.

11.9.4.3 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**).

11.9.4.4 Имя файла резервной копии по умолчанию

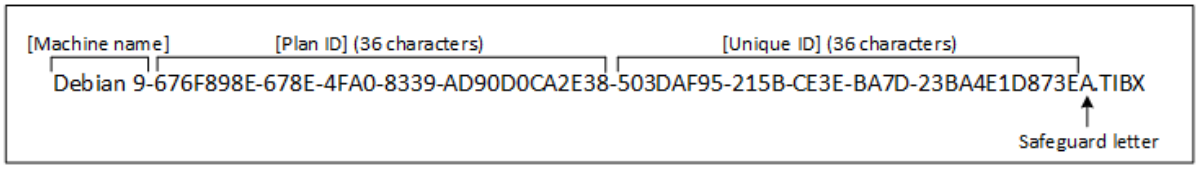
По умолчанию для имени файла резервной копии всей физической или виртуальной машины, дисков/томов, файлов/папок, баз данных Microsoft SQL Server и Microsoft Exchange, а также конфигурации ESXi используется следующий формат: [ИмяМашины]-[ИД плана]-[Уникальный ИД]A.

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.



11.9.4.5 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
...
```

11.9.4.6 Использование переменных

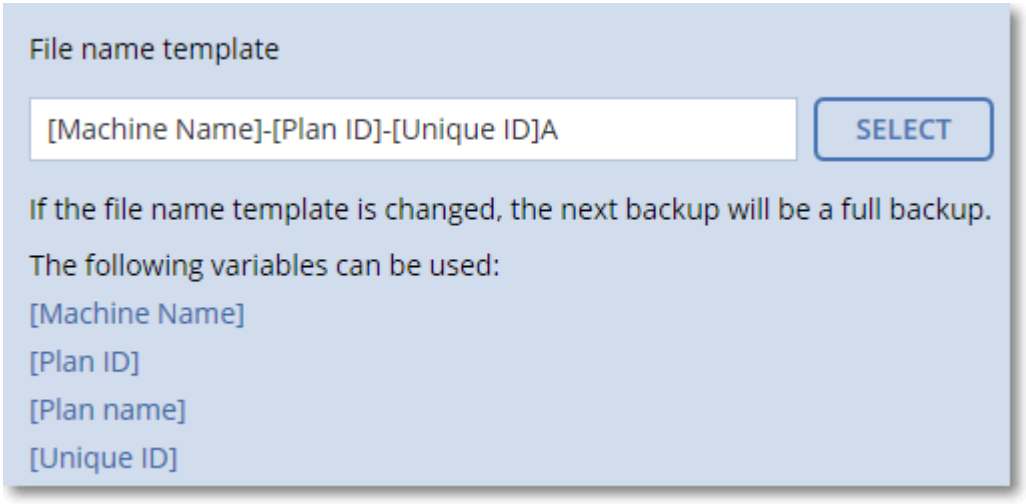
Кроме переменных, используемых по умолчанию, можно использовать следующие переменные:

- 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].

11.9.4.7 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.

11.9.5 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.

11.9.5.1 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.	

11.9.5.2 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 не вы не удалите их вручную.

11.9.5.3 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.

11.9.6 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.

11.9.7 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.

11.9.8 Способ резервного копирования кластера

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

Эти параметры относится к резервной копии баз данных Microsoft SQL Server и Microsoft Exchange Server.

Эти параметры действует только в том случае, если для резервного копирования выбран сам кластер (группа обеспечения доступности Microsoft SQL Server Always On (AAG) или группа обеспечения доступности баз данных Microsoft Exchange Server (DAG)), а не отдельные содержащиеся в нем узлы или базы данных. Если вы выберете отдельные элементы, содержащиеся в кластере, резервные копии не будут поддерживать кластеры и будут созданы резервные копии только выбранных копий элементов.

11.9.8.1 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.

11.9.8.2 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. раздел«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.

11.9.9 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.

11.9.10 Обработка ошибок

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

11.9.10.1 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.

11.9.10.2 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.

11.9.10.3 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.

11.9.10.4 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).

11.9.11 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.

11.9.12 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.

11.9.12.1 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 или macOS).
  Как в Windows, так и в Linux/macOS, 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**

11.9.12.2 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.

11.9.12.3 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.

11.9.13 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.

11.9.14 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.

11.9.15 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.

11.9.16 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**.

11.9.17 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.

11.9.18 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.

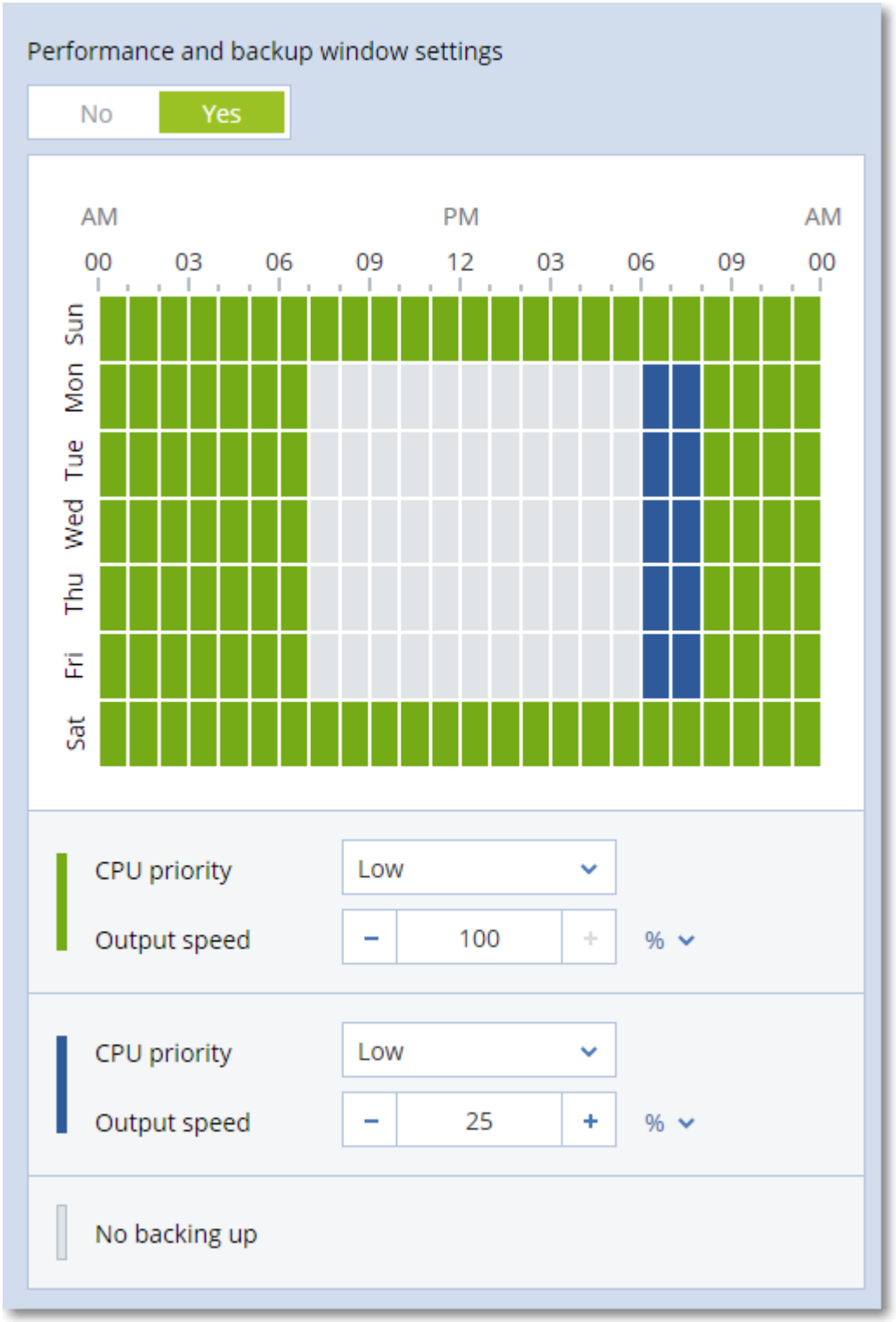
Даже если запланированные резервные копии заблокированы, резервное копирование можно запустить вручную. Для него будут использоваться параметры производительности последнего часа, когда процессы резервного копирования были разрешены.

11.9.18.1 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.



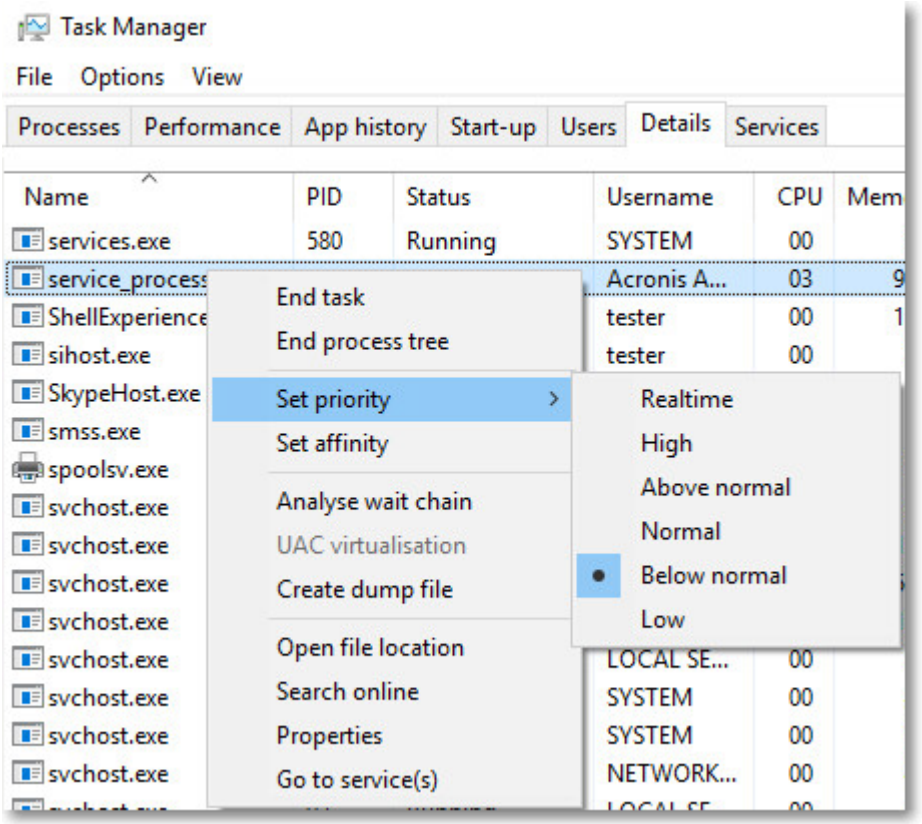
11.9.18.2 Приоритет ЦП

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.



11.9.18.3 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).

11.9.19 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).

11.9.19.1 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).
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	Установить	Снять	Установить	Снять

команды*				
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
```

11.9.19.2 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**.

11.9.20 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.

11.9.20.1 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).
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
```

11.9.20.2 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 копирование только после успешного выполнения команды.	Продолжить резервное копирование после команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Продолжить резервное копирование одновременно с выполнением команды и независимо от результатов выполнения команды.

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

11.9.21 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.

11.9.22 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.

11.9.23 Разбиение

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.

11.9.24 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**.

11.9.25 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.**

11.9.25.1 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.

11.9.25.2 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.

11.9.26 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 программный поставщик 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.

11.9.26.1 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.

11.9.27 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, Virtuozzo Guest Tools 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.

Примечание
Этот параметр не влияет на виртуальные машины Scale Computing HC3. Для них заморозка зависит от того, установлены ли инструменты масштабирования на виртуальной машине.

11.9.28 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**.

11.9.29 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**.

11.10 Восстановление

11.10.1 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
Физическая машина (Mac)	Использование загрузочного носителя
Виртуальная машина (VMware, Hyper-V, Red Hat Virtualization (oVirt) или Scale Computing HC3)	Использование веб-интерфейса Использование загрузочного носителя
Виртуальная машина или контейнер (Virtuozzo, Virtuozzo Hybrid Server или Virtuozzo Hybrid Infrastructure)	Использование веб-интерфейса
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
Состояние системы	Использование веб-интерфейса
Базы данных SQL	Использование веб-интерфейса
Базы данных Exchange	Использование веб-интерфейса
Почтовые ящики Exchange	Использование веб-интерфейса

Примечание для пользователей Mac

- Начиная с 10.11 El Capitan, отдельные системные файлы, папки и процессы помечены для защиты расширенным атрибутом файла com.apple.rootless. Эта функция называется System Integrity Protection (SIP). Среди защищенных файлов – предустановленные приложения и большинство папок в каталогах /system, /bin, /sbin, /usr.

  Защищенные файлы и папки невозможно перезаписать при восстановлении в операционной системе. Чтобы перезаписать защищенные файлы, выполните восстановление с загрузочного носителя.
- Начиная с macOS Sierra 10.12, файлы, которые используются редко, можно переместить в iCloud с использованием функции сохранения в облаке (Store in Cloud). В файловой системе остаются небольшие следы этих файлов. Вместо оригинальных файлов создается резервная копия этих следов.

При восстановлении следа в исходное расположение он синхронизируется с iCloud, после чего становится доступен оригинальный файл. При восстановлении следа в другое расположение синхронизировать его невозможно, поэтому оригинальный файл будет недоступен.

11.10.2 Восстановление машины

11.10.2.1 Физическая машина

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

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

- Машина с macOS
- Машина с клиентом в режиме «Улучшенная безопасность»
- любую операционную систему на «голое железо» либо на отключенной машине.
- Структура логических томов (тома созданы диспетчером логических томов в ОС Linux). Носитель позволяет автоматически воссоздать структуру логических томов.

Для восстановления операционной системы потребуется перезагрузка. Вы можете перезапустить машину автоматически или присвоить ей статус **Требуется вмешательство**. Восстановленная операционная система автоматически запускается.

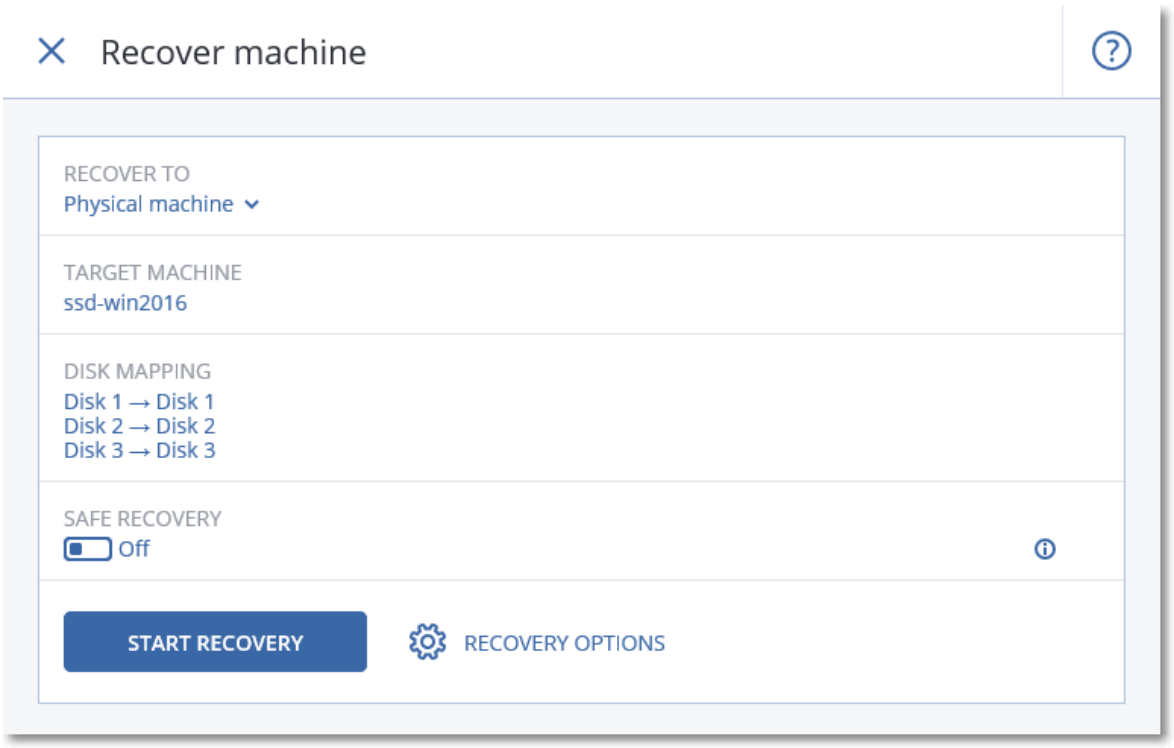
Восстановление физической машины

1. Выберите машину, для которой есть резервная копия.
2. 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**.

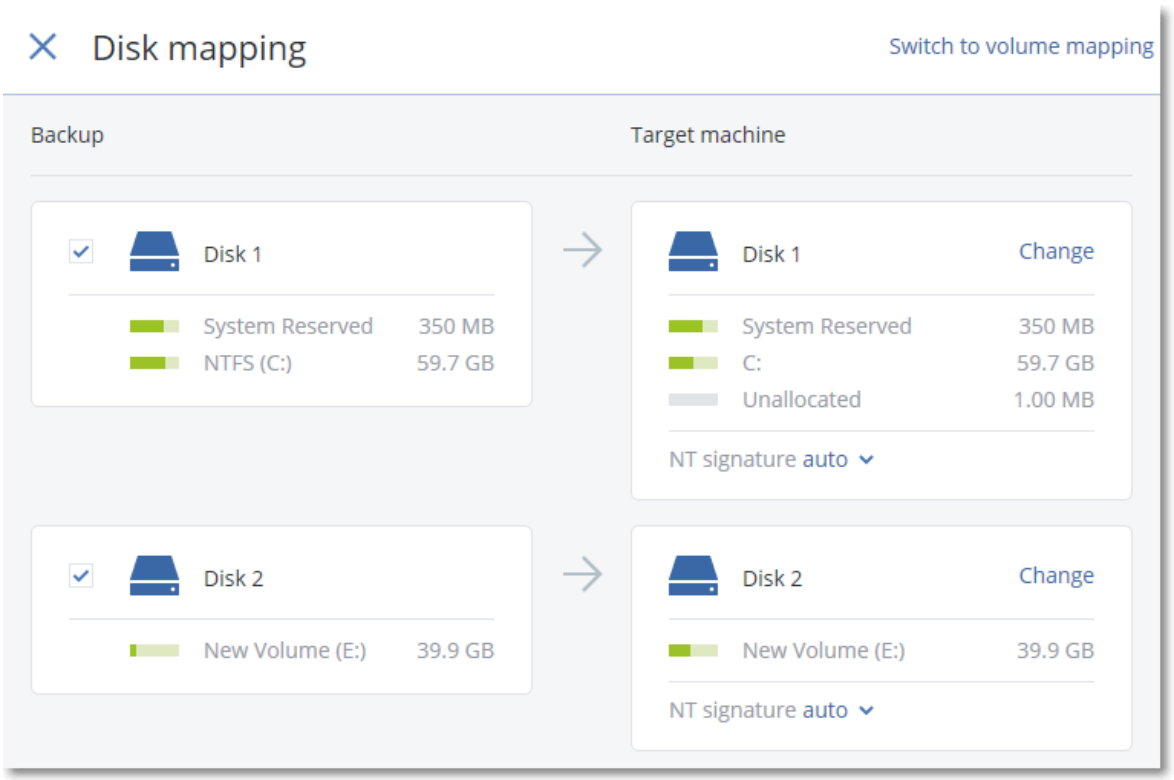
   Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

   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. [Необязательно] Включите **Безопасное восстановление** для сканирования резервных копий на вредоносные программы. Если обнаружена вредоносная программа, она помечается в резервной копии и удаляется сразу же по окончании процесса восстановления.
7. Щелкните **Запуск восстановления**.
8. Подтвердите перезапись дисков версиями из резервной копии. Укажите, следует ли автоматически перезапустить машину.

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

11.10.2.2 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».

Примечание

Невозможно восстановить виртуальные машины macOS на хосты Hyper-V, поскольку Hyper-V не поддерживает macOS. Невозможно восстановить виртуальные машины macOS на хост VMware, установленный на устройстве Mac.

Кроме того, не удается восстановить резервные копии физических машин macOS как виртуальные машины.

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».

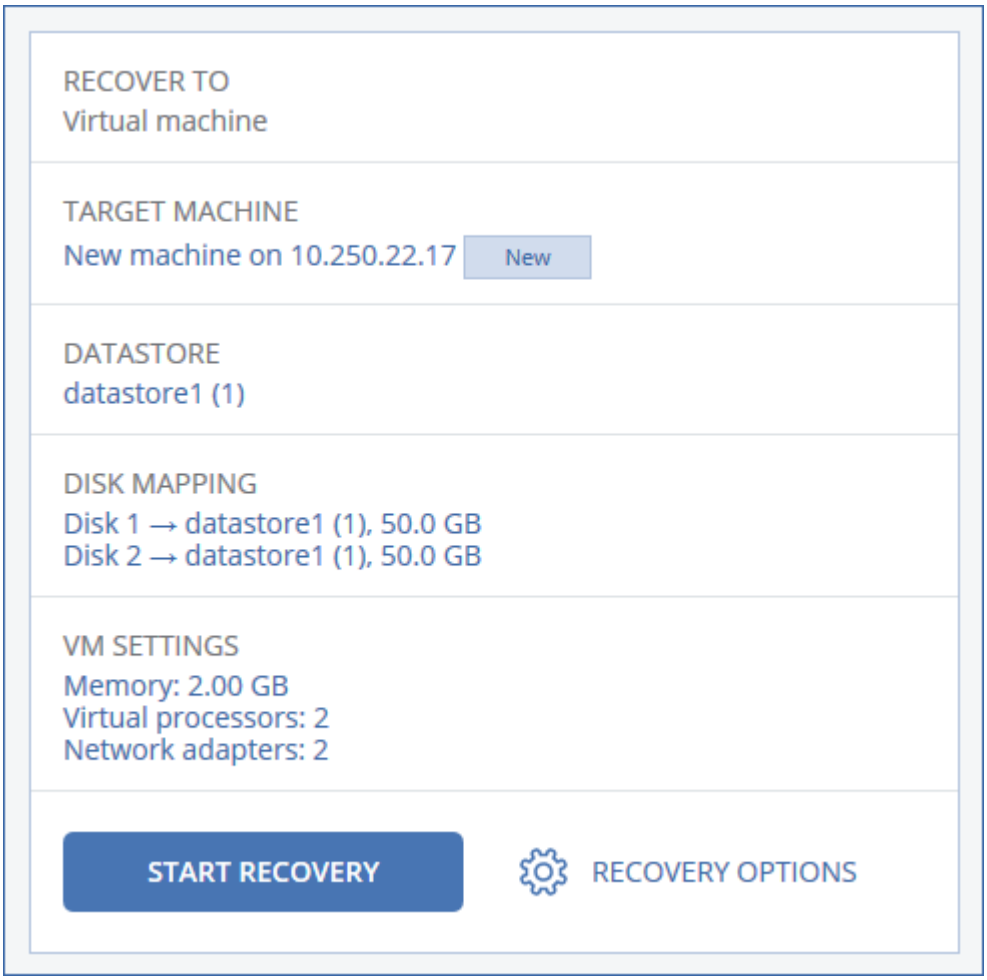
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щелкните **Целевая машина**.
   a. Выберите гипервизор.

   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:
   - [Недоступно для Virtuozzo Hybrid Infrastructure] 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.

     Для Virtuozzo Hybrid Infrastructure можно выбрать только политику хранения для целевых дисков. Для этого выберите желаемый целевой диск, затем щелкните Изменить. В открывшейся колонке щелкните значок шестерни, выберите политику хранения, а затем щелкните Готово.
   - [Необязательно для VMware ESXi, Hyper-V и Red Hat Virtualization/oVirt] Щелкните **Настройки ВМ**, чтобы изменить размер памяти, количество процессоров (для Virtuozzo Hybrid Infrastructure выберите Flavor) и сетевые подключения виртуальной машины.

     Примечание
     Для Virtuozzo Hybrid Infrastructure выбор варианта является обязательным.



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

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

11.10.2.3 Виртуальная машина

Виртуальные машины можно восстановить с их резервных копий.

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

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.

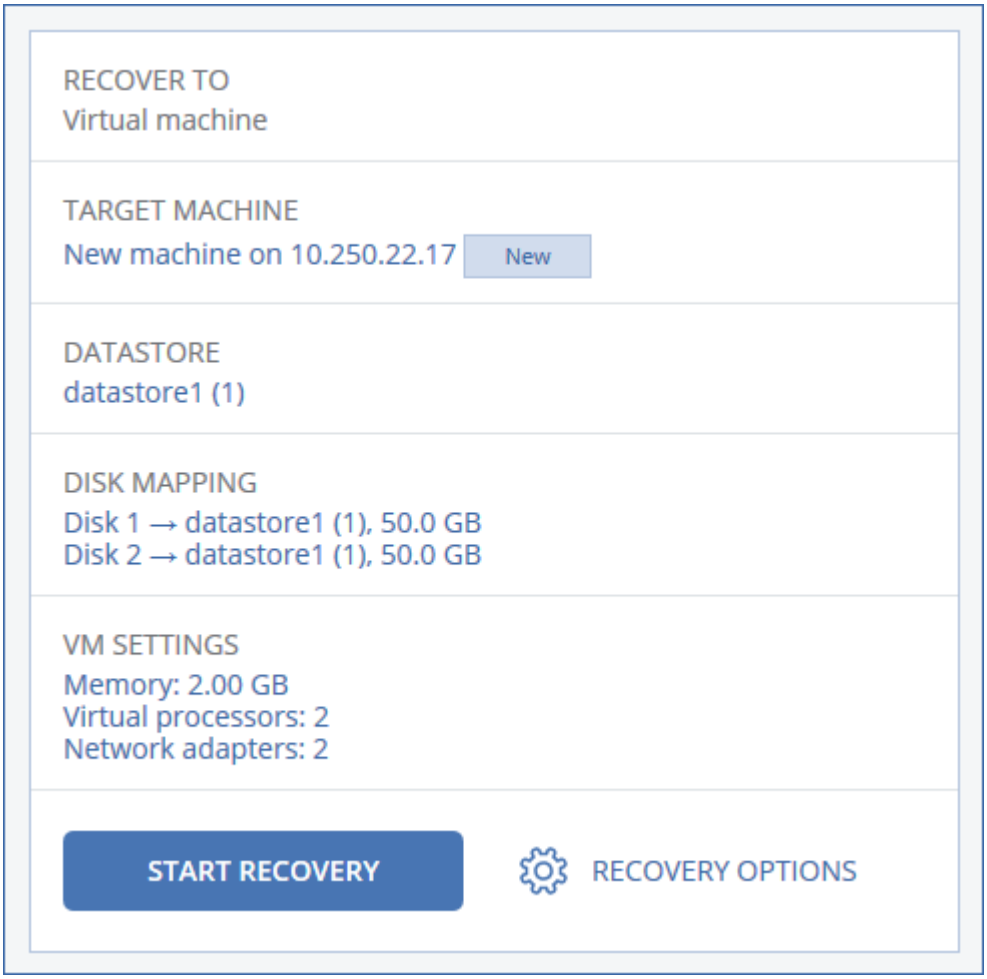
   Если это имеет место, продолжите с шага 4 в разделе «Физическая машина». В противном случае рекомендуется выполнить миграцию V2P, используя загрузочный носитель.
4. [Необязательно] По умолчанию данное программное обеспечение автоматически выбирает исходную машину в качестве целевой. Чтобы выполнить восстановление на = другую виртуальную машину, выберите **Целевая машина** и выполните следующие действия:
   a. Выберите гипервизор (**VMware ESXi**, **Hyper-V**, **Virtuozzo**, **Virtuozzo Hybrid Infrastructure**, **Scale Computing HC3** или **oVirt**).

      Только виртуальные машины Virtuozzo можно восстановить в Virtuozzo. Дополнительную информацию о миграции V2V см. в теме «Миграция машины».
   b. Выберите машину, в которую будут 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.
   - [Недоступно для Virtuozzo Hybrid Infrastructure и Scale Computing HC3] Чтобы выбрать хранилище данных для виртуальной машины, щелкните **Хранилище данных** для ESXi, **Путь** – для Hyper-V и Virtuozzo 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, за исключением случаев, когда восстанавливается контейнер Virtuozzo или виртуальная машина Virtuozzo Hybrid Infrastructure.

     Для Virtuozzo Hybrid Infrastructure можно выбрать только политику хранения для целевых дисков. Для этого выберите желаемый целевой диск, затем щелкните **Изменить**. В открывшейся колонке щелкните значок шестерни, выберите политику хранения, а затем щелкните **Готово**.

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

Примечание
Для Virtuozzo Hybrid Infrastructure выбор варианта является обязательным.



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

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

11.10.2.4 Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе "Создание физического загрузочного носителя" (стр. 281).

Порядок восстановления дисков с помощью загрузочного носителя

1. Загрузите целевую машину с помощью загрузочного носителя.
2. [Только при восстановлении Mac] При восстановлении дисков (томов) в формате APFS на машину, отличную от исходной, или на «голое железо» заново создайте конфигурацию оригинального диска вручную:

a. Щелкните **Утилита проверки диска**.

b. Сотрите всю информацию на целевом диске и отформатируйте его в APFS. Инструкции см. по ссылке https://support.apple.com/en-us/HT208496#erasedisk.

c. Заново создайте конфигурацию оригинального диска. Инструкции см. по ссылке https://support.apple.com/guide/disk-utility/add-erase-or-delete-apfs-volumes-dskua9e6a110/19.0/mac/10.15.

d. Щелкните **Утилита проверки диска** > **Выйти из утилиты проверки диска**.

3. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
4. 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.
5. [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.
6. На экране приветствия нажмите кнопку **Восстановить**.
7. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
8. 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.
9. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
10. В разделе **Содержимое резервной копии** выберите диски, которые нужно восстановить. Нажмите кнопку **OK**, чтобы подтвердить выбор.
11. 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.

12. [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.
13. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
14. Нажмите кнопку **OK**, чтобы начать восстановление.

11.10.2.5 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

11.10.3 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.

11.10.4 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

11.10.5 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.

11.10.6 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

Universal Restore может применяться к операционным системам Linux с версией ядра 2.6.8 или более поздней.

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 **_acronis_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_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- Укажите копию в строке **initrd** конфигурации загрузчика GRUB.

11.10.7 Восстановление файлов

11.10.7.1 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, агент для Virtuozzo, агент для Scale Computing HC3 или агент для oVirt (если файлы изначально находятся на виртуальной машине ESXi, Hyper-V, Virtuozzo, Scale Computing HC3 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**.

11.10.7.2 Загрузка файлов из облачного хранилища данных

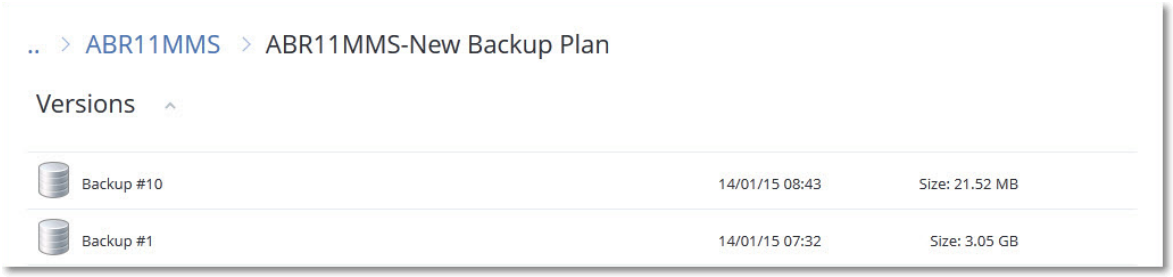
Вы можете просматривать содержимое облачного хранилища данных и резервных копий, а также загружать необходимые файлы.

Ограничения

- резервные копии состояния системы, баз данных SQL и Exchange недоступны для просмотра.
- Скачивание недоступно, если общий размер выбранных файлов превышает 100 МБ.

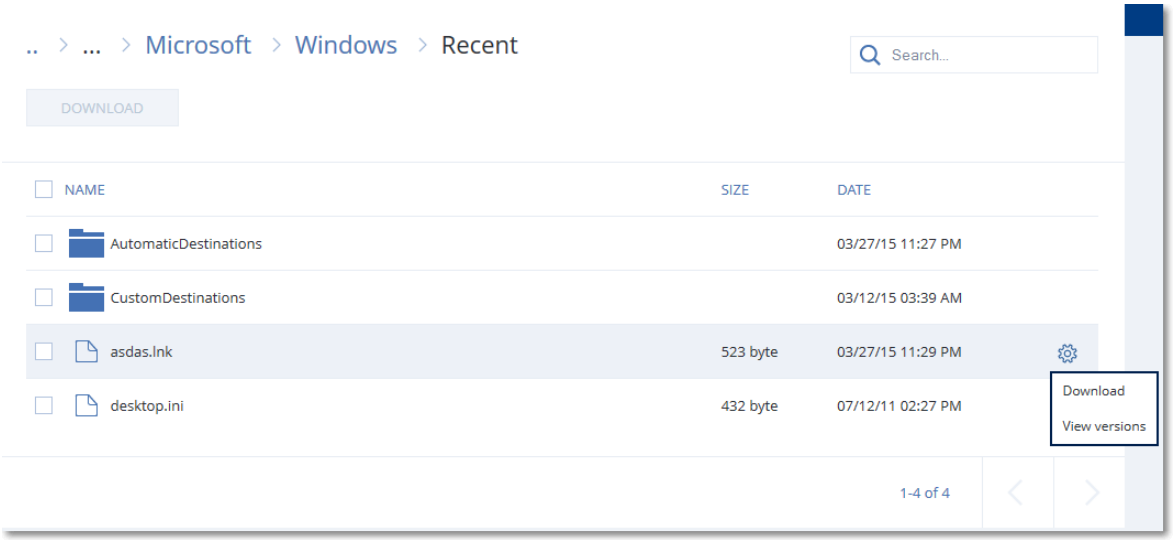
Загрузка файлов из облачного хранилища данных

1. Выберите машину, для которой была создана резервная копия.
2. Последовательно выберите пункты **Восстановить** > **Другие способы восстановления...** > **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** щелчком мыши выберите резервную копию, с которой необходимо восстановить файлы.



При просмотре резервных копий файлов: на следующем этапе вы сможете выбрать дату и время создания резервной копии с помощью значка шестеренки справа от файла. По умолчанию восстанавливаются файлы из самой новой резервной копии.

5. Перейдите к нужной папке или используйте поиск для получения списка нужных файлов.



6. Установите флажки для элементов, которые необходимо восстановить, и щелкните **Скачать**.

   Если выбран один файл, он загружается как есть. В противном случае выбранные данные архивируются в ZIP-файл.
7. Выберите расположение для сохранения данных и щелкните **Сохранить**.

11.10.7.3 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.

11.10.7.4 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 хранится в локальной папке или в сетевой папке (SMB/CIFS).

Порядок извлечения файлов из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды 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.

11.10.8 Восстановление состояния системы

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

1. Выберите машину, для которой хотите восстановить состояние системы.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления состояния системы. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

4. Нажмите **Восстановить состояние системы**.
5. Подтвердите перезапись состояния системы версией из резервной копии.

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

11.10.9 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. 281).

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.

11.10.10 Параметры восстановления

Чтобы изменить параметры восстановления, щелкните **Параметры восстановления** при настройке восстановления.

11.10.10.1 Доступность параметров восстановления

Набор доступных параметров восстановления зависит от следующих факторов.

- Среда, в которой работает агент, выполняющий восстановление (Windows, Linux, macOS 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**	**macOS**	**Загрузочный носитель**	**ESXi, Hyper-V и Virtuozzo**	**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	+

11.10.10.2 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.

11.10.10.3 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 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 копи хранится на ленточном устройстве.

Если перенос системы между UEFI и BIOS не поддерживается, агент работает так, словно выбрана настройка **Как и в машине, для которой есть резервная копия**. Если целевая машина поддерживает как UEFI, так и BIOS, необходимо вручную включить режим загрузки, соответствующий исходной машине. Иначе система не загрузится.

11.10.10.4 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**.

11.10.10.5 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.

11.10.10.6 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.

11.10.10.7 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.

11.10.10.8 Flashback

Этот параметр действует при восстановлении дисков и томов на физических и виртуальных машинах, за исключением Mac.

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**.

11.10.10.9 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**.

11.10.10.10 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.

11.10.10.11 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.

11.10.10.12 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	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.

	восстановление при сбое команды.			

* 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.

11.10.10.13 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, агентом для Scale Computing HC3 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.

11.10.10.14 Управление питанием ВМ

Эти параметры применяются, если восстановление на виртуальную машину выполняется агентом для VMware, агентом для Hyper-V, агентом для Virtuozzo, агентом для Scale Computing HC3 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.

11.10.10.15 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**.

11.11 Операции с резервными копиями

11.11.1 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.

На вкладке **Хранилище резервных копий** можно отфильтровать резервные копии в списке по указанным ниже критериям.

- **Только резервные копии, созданные с помощью функции управления исправлениями до обновления**: показывать только резервные копии, созданные при выполнении управления исправлениями до их установки.

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 будут выполнено восстановление. Чтобы изменить целевое место восстановления, укажите другую машину в поле **Машина для обзора**.

4. Щелкните **Показать резервные копии**.
5. Выберите точку восстановления.

11.11.2 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.

11.11.3 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.

11.12 Защита приложений Microsoft

11.12.1 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. Это означает, что можно использовать единое решение и один план защиты как для аварийного восстановления, так и для защиты данных.

Для Microsoft Exchange Server вы можете выбрать **Резервное копирование почтового ящика**. При выборе 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. Резервное копирование почтовых ящиков поддерживается Microsoft Exchange Server 2010 Service Pack 1 (SP1) и более поздней версии.

11.12.2 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.

11.12.3 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.

11.12.4 Предварительные требования

Перед настройкой резервного копирования приложений убедитесь, что перечисленные ниже требования выполнены.

Чтобы проверить состояние модуля записи VSS, используйте команду vssadmin list writers.

11.12.4.1 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. Если используется Exchange 2010 или более поздней версии, то оболочка Windows PowerShell должна иметь по крайней мере версию 2.0.
- Установлена платформа Microsoft .NET Framework.

  Если используется Exchange 2007, то Microsoft .NET Framework должна иметь по крайней мере версию 2.0.

  Если используется Exchange 2010 или более поздней версии, то Microsoft .NET Framework должна иметь по крайней мере версию 3.5.
- 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.

11.12.4.2 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 к VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- 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 https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - 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**).

11.12.5 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.

11.12.5.1 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.

11.12.5.2 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
2007	Группы хранения	Участие в группе ролей **Администраторы организации Exchange**
2010/2013/2016/2019	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**.

11.12.6 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.

11.12.6.1 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.

11.12.6.2 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».

11.12.6.3 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:

  Соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **sysadmin** в каждом из экземпляров, для которых создается резервная копия.
- Для Exchange Server:

  Exchange 2007: Данная учетная запись должна входить в группу **Администраторы** на данной машине, а также в группу ролей **Администраторы организации Exchange**.

  Exchange 2010 и более поздней версии: Данная учетная запись должна входить в группу **Администраторы** на данной машине, а также в группу ролей **Управление организацией**.
- Для Active Directory:

  Данная учетная запись должна быть администратором домена.

Дополнительные требования для виртуальных машин

Если приложение выполняется на виртуальной машине, резервная копия которой создана агентом для VMware или агентом для Hyper-V, убедитесь, что на этой машине отключен контроль учетных записей (UAC). Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

11.12.7 Резервная копия почтового ящика

Резервное копирование почтовых ящиков поддерживается Microsoft Exchange Server 2010 Service Pack 1 (SP1) и более поздней версии.

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**.

11.12.7.1 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**.

11.12.7.2 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 следующей статье базы знаний Microsoft: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

11.12.8 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.

11.12.8.1 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.

11.12.8.2 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**.

11.12.9 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

2007	Группы хранения	Участие в группе ролей **Администраторы организации Exchange**.
2010/2013/2016/2019	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.

11.12.9.1 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 том, как подключить базы данных, см. в следующих статьях:

- Для Exchange 2010 (или более поздней версии): http://technet.microsoft.com/en-us/library/aa998871.aspx
- Для Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

11.12.10 Восстановление почтовых ящиков Exchange и элементов почтового ящика

В этом разделе описана процедура восстановления почтовых ящиков Exchange и элементов почтового ящика из резервных копий базы данных, резервных копий с поддержкой приложений и из резервных копий почтового ящика. Почтовые ящики или элементы почтового ящика могут быть восстановлены на запущенный Exchange Server.

Можно восстановить следующие элементы:

- почтовые ящики (за исключением архивированных почтовых ящиков);
- общие папки;
- элементы общих папок;
- папки электронной почты;
- сообщения электронной почты;

- события календаря;
- задания;
- контакты;
- записи журнала.
- Примечание

Чтобы найти эти элементы, можно воспользоваться поиском.

11.12.10.1 Восстановление на Exchange Server

Фрагментарное восстановление можно выполнить в Microsoft Exchange Server 2010 Service Pack 1 (SP1) и более поздней версии. Исходная резервная копия может содержать базы данных /или почтовые ящики/ любой поддерживаемой версии Exchange.

Фрагментарное восстановление может быть выполнено агентом для Exchange или агентом для VMware (Windows). Целевой Exchange Server и машина с выполняющимся агентом должны быть в одном лесу Active Directory.

Если почтовый ящик восстанавливается в существующий почтовый ящик, существующие элементы с одинаковыми идентификаторами перезаписываются.

При восстановлении элементов почтового ящика перезапись не происходит. Вместо этого в целевой папке заново создается полный путь к элементу почтового ящика.

Требования к учетным записям пользователей

Почтовый ящик, восстанавливаемый из резервной копии, должен иметь связанную с ним учетную запись пользователя в Active Directory.

Пользовательские почтовые ящики и их содержимое можно восстановить, только если *включены* связанные с ними учетные записи пользователей. Общие почтовые ящики, почтовые ящики помещения и оборудования могут быть восстановлены, только если соответствующие учетные записи пользователей *отключены*.

Почтовый ящик, не соответствующий этим условиям, при восстановлении будет пропущен.

Если некоторые почтовые ящики будут пропущены, восстановление продолжится с предупреждением. Если все почтовые ящики будут пропущены, восстановление завершится сбоем.

11.12.10.2 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.

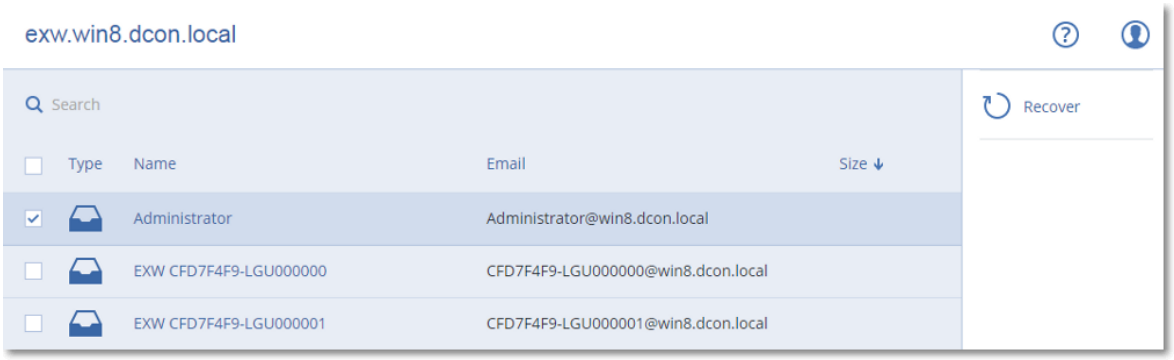
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   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 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 выбранная для просмотра одним из двух указанных выше действий.
4. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
5. Выберите почтовые ящики, которые необходимо восстановить.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.



6. Нажмите кнопку **Восстановить**.

   Чтобы выбрать или изменить целевую машину, щелкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

   Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2010/2013) 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, щелкните **База данных для воссоздания отсутствующих почтовых ящиков**.
9. Щелкните **Запуск восстановления**.

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 щелкните **Восстановить**.

   Можно выполнить поиск по имени почтовых ящиков. Подстановочные символы не поддерживаются.

   Если почтовый ящик был удален, выберите его на вкладке Хранилище резервных копий и щелкните **Показать резервные копии**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
4. Последовательно выберите пункты **Восстановление** > **Почтовый ящик**.
5. Выполняйте шаги 8-11 вышеописанной процедуры.

11.12.10.3 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. Щелкните **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 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 выбранная для просмотра одним из двух указанных выше действий.

4. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
5. Щелкните почтовый ящик, в котором изначально содержались элементы, которые необходимо восстановить.
6. Выберите элементы, которые необходимо восстановить.

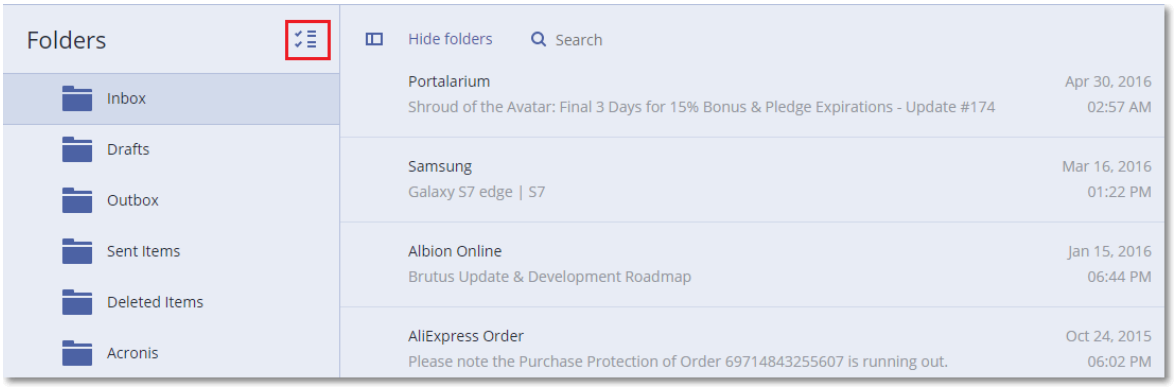
   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - Для сообщений электронной почты: выполните поиск по теме, отправителю, получателю и дате.
   - Для событий: выполните поиск по заголовку и дате.
   - Для задач: выполните поиск по теме и дате.
   - Для контактов: выполните поиск по имени, адресу электронной почты и номеру телефона.

   Когда выбрано это сообщение электронной почты, можно щелкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

   Примечание
   Чтобы загрузить вложенный файл, щелкните его имя.

   Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок.



7. Нажмите кнопку **Восстановить**.
8. Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.

   [Только при восстановлении на Exchange Server] Чтобы выбрать или изменить целевую машину, щелкните **Целевая машина с Microsoft Exchange Server**. Это действие позволит восстановить машину, на которой не запущен агент для Exchange.

   Укажите полное доменное имя (FQDN) машины, на которой включена роль **Клиентский доступ** (в Microsoft Exchange Server 2010/2013) 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. Щелкните **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 удален, выберите его на вкладке Хранилище резервных копий и щелкните **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.

   Когда выбрано это сообщение электронной почты, можно щелкнуть **Показать содержимое**, чтобы показать его содержимое, включая вложения.

   Примечание
   Чтобы загрузить вложенный файл, щелкните его имя.

   Когда выбрано это сообщение электронной почты, можно щелкнуть **Отправить как сообщение электронной почты**, чтобы отправить сообщение по адресу электронной почты. Сообщение отправляется с адреса электронной почты администратора учетной записи.

   Чтобы иметь возможность выбрать папки, щелкните значок восстановления папок 

6. Нажмите кнопку **Восстановить**.
7. Выполните шаги 9-13 вышеописанной процедуры.

11.12.10.4 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 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
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.

11.12.11 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**.

11.13 Защита размещенных данных Exchange

11.13.1 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.

11.13.2 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.

11.13.3 Выбор почтовых ящиков

Выберите почтовый 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**.

11.13.4 Восстановление почтовых ящиков и элементов почтовых ящиков

11.13.4.1 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.

11.13.4.2 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.

11.14 Защита Oracle Database

Защита Oracle Database описана в отдельном документе, который доступен по ссылке https://cyberprotect.ru/ru-RU/support/documentation/CyberBackup/15/OracleBackup.pdf

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

11.15 Специальные операции с виртуальными машинами

11.15.1 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.

11.15.1.1 Примеры использования

- **Аварийное восстановление**

  Мгновенное восстановление виртуальной машины, на которой произошел сбой.

- **Тестирование резервного копирования**

  Запустите машину с резервной копии и убедитесь в том, что гостевая ОС и приложения работают правильно.
- **Доступ к данным приложения**

  Когда машина запущена, воспользуйтесь встроенными инструментами управления в приложении, чтобы получить доступ к требуемым данным и извлечь их.

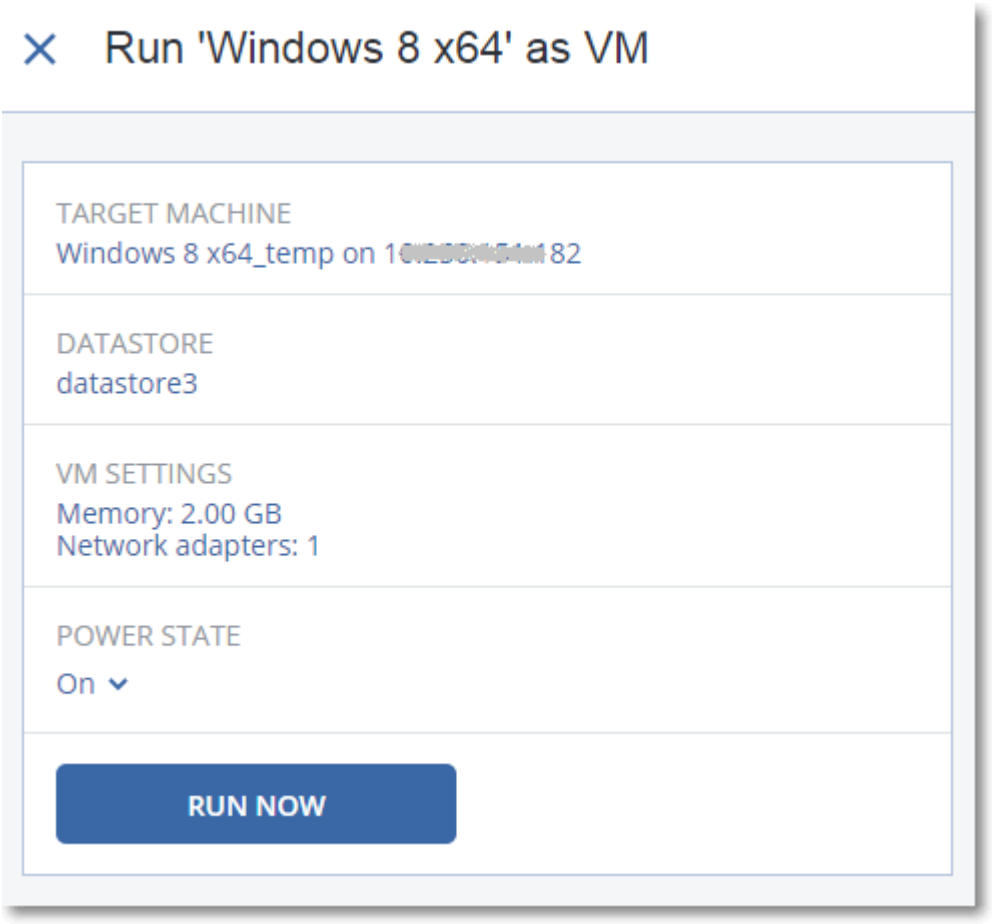
11.15.1.2 Предварительные требования

- 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. Нельзя использовать резервные копии *контейнеров* Virtuozzo.
- 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).

11.15.1.3 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.

11.15.1.4 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.

11.15.1.5 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, 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).

11.15.2 Работа в VMware vSphere

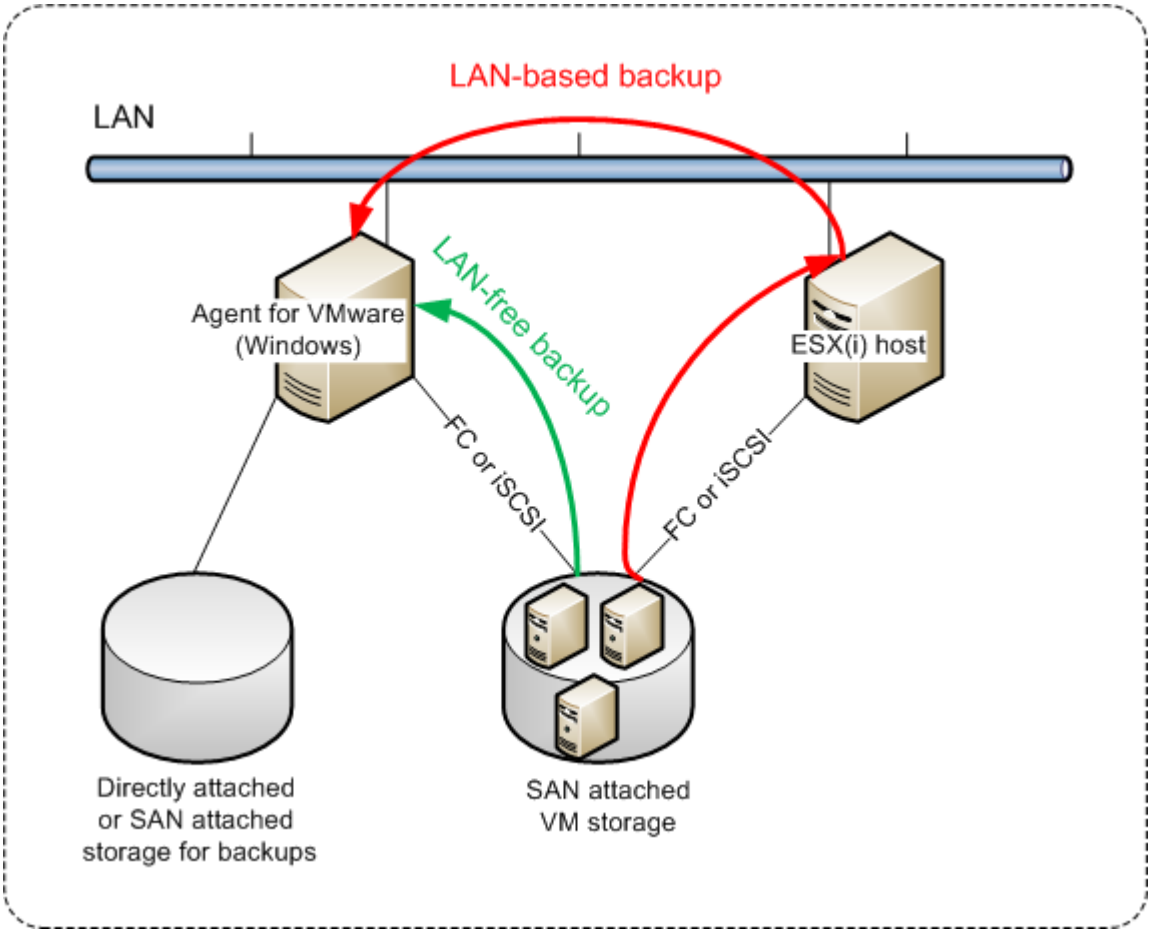
В этом разделе описаны операции, характерные для среды VMware vSphere.

11.15.2.1 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**.

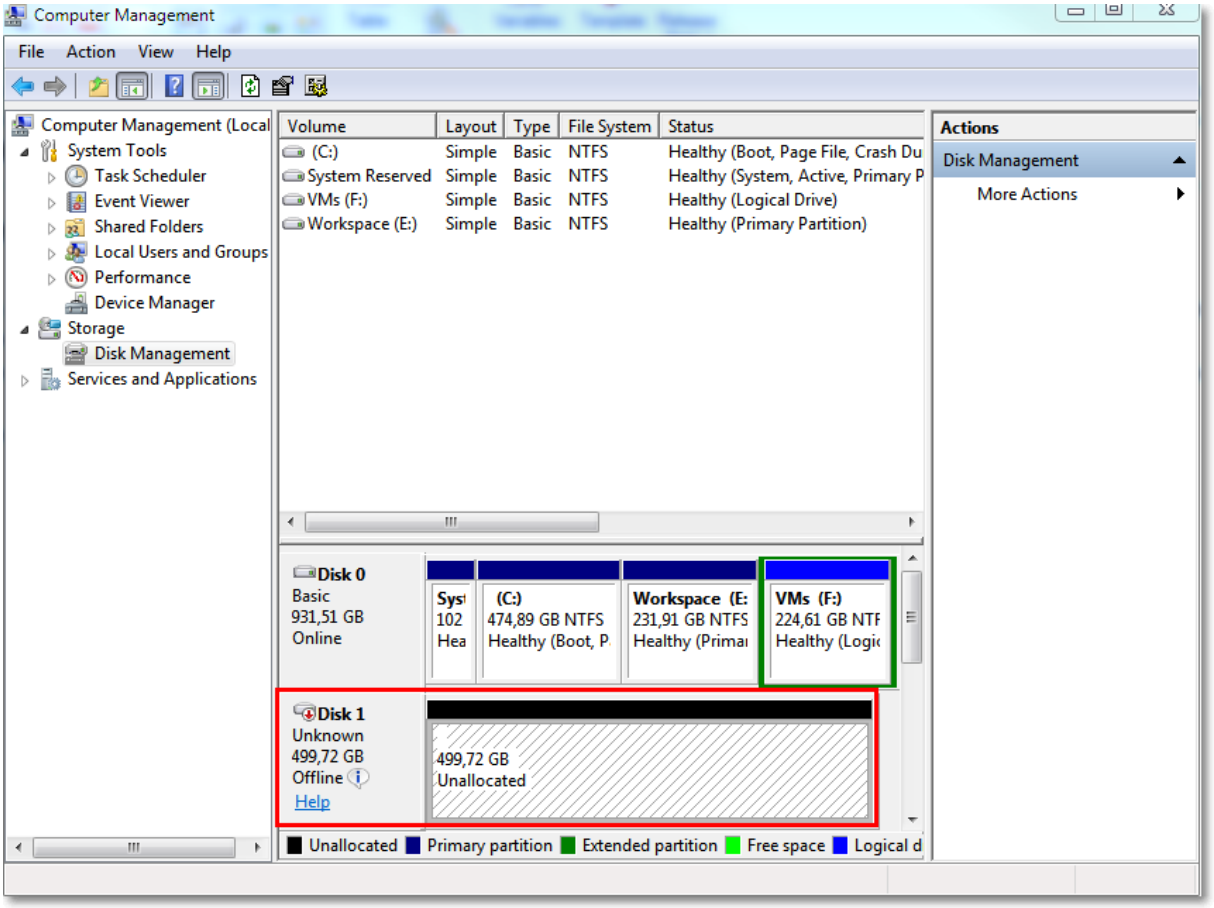
   Примечание
   Чтобы найти приложение **Администрирование**, возможно, необходимо будет изменить представление **панели управления** на отличное от **Главная** или **Категория** или воспользоваться поиском.

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.



11.15.2.2 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 агентаиз 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:**.

11.15.2.3 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.

11.15.2.4 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.

11.15.2.5 Управление средами виртуализации

Можно просмотреть среды vSphere, Hyper-V и Virtuozzo в их собственном представлении. После установки и регистрации соответствующего агента в разделе **Устройства** появляются вкладки **VMware**, **Hyper-V** или **Virtuozzo**.

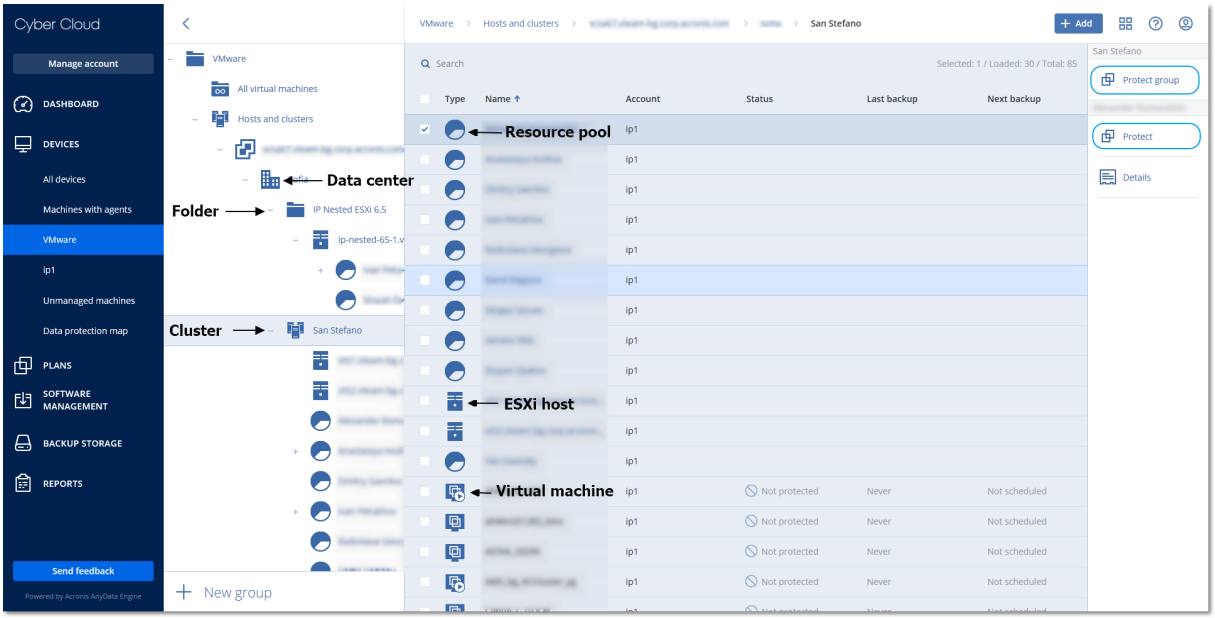
На вкладке **VMware** выполните резервное копирование следующих объектов инфраструктуры vSphere:

- 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 "San Stefano", 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 "San Stefano".



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**.

11.15.2.6 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**

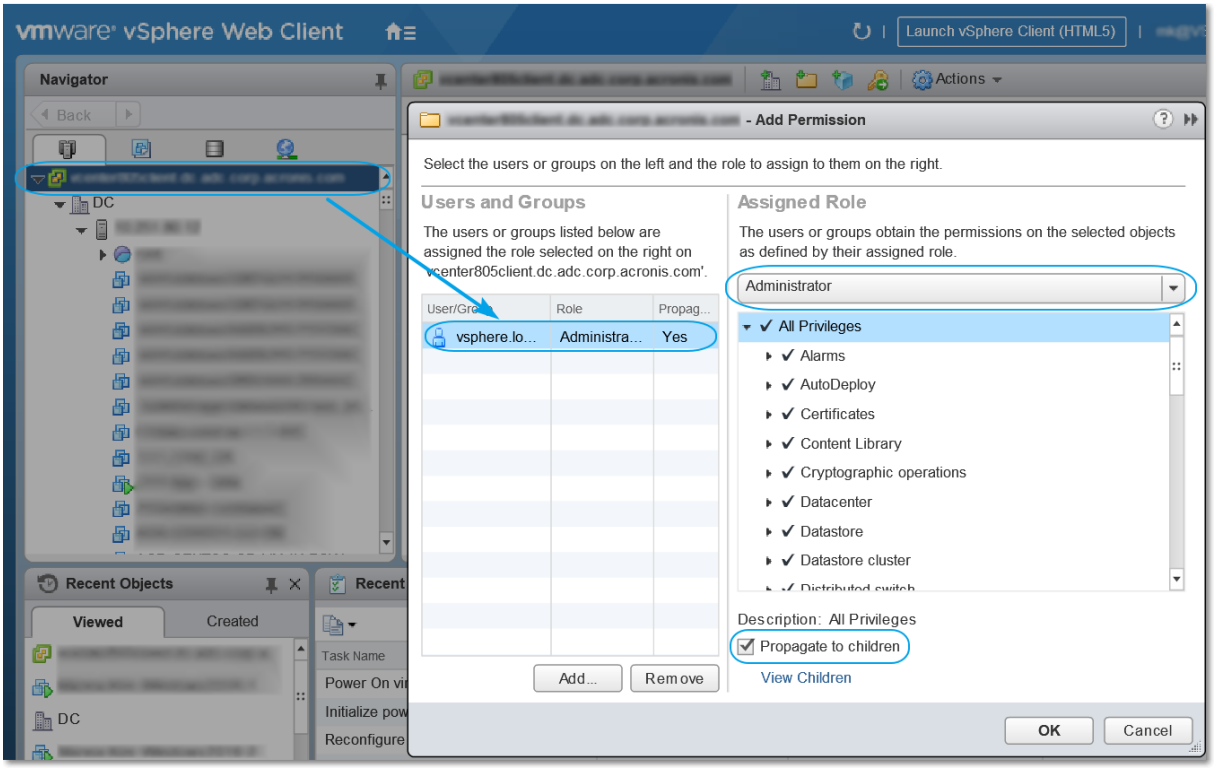
11.15.2.7 Агент для VMware: необходимые привилегии

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 назначения прав пользователю vSphere на уровне vCenter

1. Войдите в веб-клиент vSphere.
2. Щелкните правой кнопкой мыши vCenter, затем щелкните **Добавить право**.
3. Выберите или добавьте нового пользователя с требуемой ролью (роль должна включать в себя все требуемые разрешения с таблицей ниже).
4. Выберите параметр **Propagate to children (Распространить на дочерние элементы)**.



Объект	Привилегия	Операция			
		Резервное копирование ВМ	Восстановление в новую ВМ	Восстановление в существующую ВМ	Запуск ВМ из резервной копии
Операции шифрования (начиная с vSphere 6.5)	Добавить диск	+*			
	Прямой доступ	+*			
Хранилище данных	Распределение пространства		+	+	+
	Обзор хранилища данных				+
	Настройка хранилища данных	+	+	+	+
	Низкоуровневые файловые операции				+

Глобальные	**Лицензии**	+	+	+	+
	Методы отключения	+	+	+	
	Методы включения	+	+	+	
	Управление настраиваемыми атрибутами	+	+	+	
	Задать настраиваемый атрибут	+	+	+	
Хост > Конфигурация	**Конфигурация раздела хранения данных**				+
Хост > Локальные операции	**Создание ВМ**				+
	Удаление ВМ				+
	Перенастройка ВМ				+
Сеть	**Назначение сети**		+	+	+
Ресурс	**Назначение ВМ пулу ресурсов**		+	+	+
Виртуальная машина > Конфигурация	**Добавление существующего диска**	+	+		+
	Добавление нового диска		+	+	+
	Добавление или удаление устройства		+		+
	Дополнительно	+	+	+	
	Изменение числа ЦП		+		
	Отслеживание изменений	+		+	

	диска				
	Аренда диска	+		+	
	Память		+		
	Удаление диска	+	+	+	+
	Переименование		+		
	Настройка аннотации				+
	Настройки		+	+	+
Виртуальная машина > **Гостевые операции**	**Выполнение программы гостевой операции**	+**			
	Запросы гостевой операции	+**			
	Изменения гостевых операций	+**			
Виртуальная машина > **Взаимодействие**	**Получение контрольного билета гостя** (в vSphere 4.1 и 5.0)				+
	Настройка носителя CD		+	+	
	Управление гостевой операционной системой с помощью API VIX (в vSphere 5.1 и более поздних версий)				+
	Отключение			+	+
	Включение		+	+	+
Виртуальная машина >	**Создание из существующей**		+	+	+

Инвентаризация					
	Создание новой		+	+	+
	Регистрация				+
	Удаление		+	+	+
	Отмена регистрации				+
Виртуальная машина > Распределение	**Разрешение доступа к диску**		+	+	+
	Разрешение доступа к диску только для чтения	+		+	
	Разрешение загрузки ВМ	+	+	+	+
Виртуальная машина > Состояние	**Создание моментального снимка**	+		+	+
	Удаление снимка	+		+	+
Импорт	**Добавить виртуальную машину**				+

* Эта привилегия требуется только для резервного копирования зашифрованных машин.

** Эта привилегия требуется только резервных копий с поддержкой приложений.

11.15.3 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.

11.15.3.1 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**.

11.15.4 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.

11.15.5 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 Virtuozzo	Контейнер Virtuozzo	Виртуальная машина Virtuozzo Hybrid Infrastructure	Виртуальная машина Scale Computing HC3	Виртуальная машина RHV/oVirt
Физическая машина	+	+	+	-	-	+	-	+

Виртуальная машина VMware ESXi	+	+	+	-	-	+	-	+
Виртуальная машина Hyper-V	+	+	+	-	-	+	-	+
Виртуальная машина Virtuozzo	+	+	+	+	-	+	-	+
Контейнер Virtuozzo	-	-	-	-	+	-	-	-
Виртуальная машина Virtuozzo Hybrid Infrastructure	+	+	+	-	-	+	-	+
Виртуальная машина Scale Computing HC3	+	+	+	-	-	+	+	+
Виртуальная машина Red Hat Virtualization/oVirt	+	+	+	-	-	+	-	+

Примечание

Невозможно восстановить виртуальные машины macOS на хосты Hyper-V, поскольку Hyper-V не поддерживает macOS. Невозможно восстановить виртуальные машины macOS на хост VMware, установленный на устройстве Mac.

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 миграцию V2V с Virtuozzo 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.

12 Инвентарь оборудования

Функция инвентаря оборудования позволяет просмотреть все компоненты оборудования, доступные:

- на физических устройствах Windows и macOS с лицензией, которая поддерживает функцию "Инвентарь оборудования";
- на виртуальных машинах Windows и macOS, запущенных в следующих платформах виртуализации: VMware, Hyper-V, Citrix, Parallels, Oracle, Nutanix, Virtuozzo и Virtuozo Hybrid Infrastructure. Дополнительную информацию о поддерживаемых версиях платформ виртуализации см. в разделе "Поддерживаемые платформы виртуализации" (стр. 22).

Примечание
Функция "Инвентарь оборудования" для виртуальных машин не поддерживается в устаревших выпусках Кибер Бэкап Облачный.

Функция "Инвентарь оборудования" поддерживается только на машинах, на которых установлен агент защиты.

Чтобы получить данные инвентаря оборудования, можно запустить автоматическое или ручное сканирование устройств.

Данные инвентаризации оборудования позволяют:

- обнаружить все аппаратные ресурсы организации;
- просматривать инвентарь оборудования всех устройств в организации;
- сравнивать компоненты оборудования на нескольких устройствах компании;
- просматривать подробную информацию о компоненте оборудования.

12.1 Включение сканирования инвентаря оборудования

Если сканирование инвентаря оборудования включено на физических устройствах и виртуальных машинах, система автоматически собирает данные об оборудовании каждые 12 часов.

Функция «Сканирование инвентаря оборудования» по умолчанию включена, но при необходимости можно изменить эту настройку.

Примечание
Клиенты пользователя могут включать или отключать сканирование инвентаря оборудования. Клиенты отдела могут только просматривать настройки сканирования инвентаря оборудования, но не могут изменять их.

Порядок включения сканирования инвентаря оборудования

1. В консоли службы выберите пункт **Настройки**.
2. Щелкните **Защитить**.
3. Щелкните **Сканирование инвентаря**.
4. Включите модуль **Сканирование инвентаря оборудования**, щелкнув переключатель рядом с именем модуля.

Выключение сканирования инвентаря оборудования

1. В консоли службы выберите пункт **Настройки**.
2. Щелкните **Защитить**.
3. Щелкните **Сканирование инвентаря**.
4. Отключите модуль **Сканирование инвентаря оборудования**, щелкнув переключатель рядом с именем модуля.

12.2 Ручной запуск сканирования инвентаря оборудования

Можно вручную запустить сканирование инвентаря оборудования для одного устройства и просмотреть текущие данные для компонентов оборудования устройства.

Примечание
Сканирование инвентаря оборудования виртуальных машин поддерживается только в том случае, если текущая дата и время виртуальной машины соответствуют текущей дате и времени по UTC. Чтобы виртуальная машина использовала правильные настройки времени, отключите параметр **Синхронизация времени** виртуальной машины, задайте текущую дату, время и часовой пояс, а затем перезапустите **Agent Core Service** и **Managed Machine Service**.

12.2.0.1 Предварительные требования

- (Для всех устройств) На устройстве должна быть операционная система Windows или macOS.
- (Для всех устройств) Устройство имеет лицензию, которая поддерживает функцию инвентаря оборудования. Обратите внимание, что функция "Инвентарь оборудования" для виртуальных машин не поддерживается в устаревших выпусках Кибер Бэкап Облачный.
- (Для всех устройств) На этом устройстве установлен агент защиты.
- (Для виртуальных машин) Машина запущена на одной из поддерживаемых платформ виртуализации. Дополнительную информацию см. в разделе "Инвентарь оборудования" (стр. 271).

Порядок запуска сканирования инвентаря оборудования на одном устройстве

1. В консоли службы откройте **Устройства**.
2. Щелкните устройство, которое необходимо просканировать, затем щелкните **Инвентаризация**.

3. Откройте вкладку **Оборудование** и щелкните **Сканировать сейчас**.

12.3 Обзор инвентаря оборудования

Позволяет просмотреть данные для всех компонентов оборудования, которые доступны на всех устройствах компании.

12.3.0.1 Предварительные требования

- (Для всех устройств) Устройства используют операционную систему Windows или macOS.
- (Для всех устройств) Устройство имеет лицензию, которая поддерживает функцию инвентаря оборудования. Обратите внимание, что функция "Инвентарь оборудования" для виртуальных машин не поддерживается в устаревших выпусках Кибер Бэкап Облачный.
- (Для всех устройств) На этом устройстве установлен агент защиты.
- (Для всех устройств) Сканирование инвентаря оборудования на устройствах выполнено.
- (Для виртуальных машин) Машина запущена на одной из поддерживаемых платформ виртуализации. Дополнительную информацию см. в разделе "Инвентарь оборудования" (стр. 271).

Порядок просмотра всех компонентов оборудования, доступных на устройствах Windows и macOS в компании

1. В консоли службы откройте **Устройства**.
2. В поле с раскрывающимся списком **Представление:** выберите пункт **Оборудование**.

Примечание
Представление – это набор столбцов, который определяет данные, выводимые на экране. Предварительно настроены представления **Стандартное** и **Оборудование**. Можно создать и сохранить настраиваемые представления с различными наборами столбцов, более подходящими для ваших задач.

В следующей таблице описаны данные, отображаемые в представлении **Оборудование**.

Столбец	Описание
Имя	Имя устройства.
Статус сканирования оборудования	Статус сканирования оборудования. • **Завершено**. • **Не запущено**. • Статус **Не поддерживается** отображается для рабочих нагрузок, для которых не поддерживается функциональность инвентаря оборудования. Это, например, виртуальные машины, мобильные устройства, устройства

Столбец	Описание
	Linux. • Статус **Обновить агент** отображается в том случае, если на устройстве установлена устаревшая версия агента. Если щелкнуть это действие, будет выполнено перенаправление на страницу «Настройки» > «Агенты», на которой администратор может обновить агент. • **Обновить квоту**. Если щелкнуть это действие, откроется диалоговое окно, в котором администратор может перейти от использования текущей лицензии к одной их других доступных лицензий для клиента
Процессор	Модели всех процессоров устройства.
Ядра процессора	Количество ядер всех процессоров устройства.
Дисковое хранилище	Используемый и общий объем хранилища данных всех дисков устройства.
Память	Общий объем ОЗУ на данном устройстве.
Дата сканирования	Дата и время последнего сканирования инвентаря оборудования.
Материнская плата	Материнская плата устройства.
Серийный номер материнской платы	Серийный номер материнской платы.
Версия BIOS	Версия BIOS системы.
Организация	Организация, которой принадлежит устройство.
Владелец	Владелец устройства.
Домен	Домен устройства.
Операционная система	Операционная система устройства.
Сборка операционной системы	Сборка операционной системы устройства.

3. Чтобы добавить столбцы в таблицу, щелкните значок параметров столбца и выберите столбцы, которые нужно отобразить в таблице.
4. Для конкретизации выводимой информации воспользуйтесь фильтрами.
   a. Щелкните **Поиск**.
   b. Щелкните стрелку, а затем щелкните **Оборудование**.
   c. Выберите один фильтр или комбинацию нескольких фильтров.

В следующей таблице описаны данные фильтры, доступные в представлении **Оборудование**.

Фильтр	Описание
Модель процессора	Можно выбрать несколько вариантов. Этот фильтр позволяет вывести данные об оборудовании устройств, которые имеют модель процессора, выбранную в фильтре.
Ядра процессора	Этот фильтр позволяет вывести данные об оборудовании устройств, процессоры которых имеют указанное количество ядре.
Общий размер диска	Этот фильтр позволяет вывести данные об оборудовании устройств, которые имеют указанный общий размер диска.
Объем памяти	Этот фильтр позволяет вывести данные об оборудовании устройств, которые имеют указанный объем ОЗУ.

d. Нажмите кнопку **Применить**.

5. Чтобы отсортировать данные по возрастанию, щелкните имя таблицы.

12.4 Просмотр инвентаря одного устройства

Можно просмотреть подробную информацию о материнской плате, процессорах, памяти, графическом процессоре, дисках хранения данных, сети и системы определенного устройства.

12.4.0.1 Предварительные требования

- (Для всех устройств) На устройстве должна быть операционная система Windows или macOS.
- (Для всех устройств) Устройство имеет лицензию, которая поддерживает функцию инвентаря оборудования. Обратите внимание, что функция "Инвентарь оборудования" для виртуальных машин не поддерживается в устаревших выпусках Кибер Бэкап Облачный.
- (Для всех устройств) На этом устройстве установлен агент защиты.
- (Для всех устройств) Сканирование инвентаря оборудования на устройстве выполнено.
- (Для виртуальных машин) Машина запущена на одной из поддерживаемых платформ виртуализации. Дополнительную информацию см. в разделе "Инвентарь оборудования" (стр. 271).

Порядок просмотра подробной информации об оборудовании определенного устройства

1. В консоли службы последовательно выберите пункты **Устройства** > **Все устройства**.
2. В поле с раскрывающимся списком **Представление:** выберите пункт **Оборудование**.
3. Найдите устройство, которое необходимо проверить, с помощью одного из указанных ниже методов.

- Поиск устройства с помощью функции **Фильтр**
  a. Щелкните **Фильтр**.
  b. Чтобы найти устройство, выберите один параметр фильтра или комбинацию нескольких параметров фильтра.
  c. Нажмите кнопку **Применить**.
- Найдите устройство, используя функцию **Поиск**:
  a. Щелкните **Поиск**.
  b. Введите полное имя устройства или его часть и щелкните **Ввести**.

4. Щелкните строку, в которой указано устройство, и щелкните **Инвентаризация**.
5. Откройте вкладку **Оборудование**.

   Доступны указанные ниже данные об оборудовании.

Компонент оборудования	Отображаемая информация
Материнская плата	Название, производитель, модель и серийный номер материнской платы устройства.
Процессоры	Производитель, модель, тактовая частота и количество ядер каждого процессора устройства.
Память	Объем, производитель и серийный номер памяти на устройстве.
Графика	Производитель и модель графических процессоров устройства.
Диски хранения	Модель, тип носителя, доступное место и размер дисков хранилища данных устройства.
Сеть	MAC-адрес, IP-адрес и тип сетевых адаптеров устройства.
Система	Идентификатор продукта, дата первоначальной установки, время загрузки системы, производитель системы, модель системы, версия BIOS, загрузочное устройство, язык системы и часовой пояс 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
- Сканирование резервной копии
- Резервная копия приложений в облаке

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

13.2 План сканирования резервных копий

Если необходимо сканировать резервные копии на вредоносные программы, можно создать план сканирования резервных копий.

Обратите внимание на следующее:

- Для сканирования можно выбрать резервные копии с точками восстановления CDP, но сканируются только регулярные точки восстановления (исключая точки восстановления CDP).
- Если резервная копия CDP выбрана для безопасного восстановления всей машины, машина безопасно восстанавливается без данных в точке восстановления CDP. Чтобы восстановить данные CDP, запустите действие восстановления файлов и папок.

Порядок создания плана сканирования резервных копий

1. В консоли службы последовательно выберите пункты **Планы** > **Сканирование резервной копии**.
2. Нажмите **Создать план**.
3. Укажите имя плана и указанные ниже параметры.
   - **Тип сканирования**:
     - **Облако**: этот параметр невозможно переопределить. Резервные копии сканируются в облачном центре обработки данных облачным агентом. Система автоматически выбирает облачный агент, который выполнит сканирование.
   - **Резервные копии для сканирования**:
     - **Расположения**: выберите расположения с резервными копиями, которые необходимо отсканировать.
     - **Резервные копии**: выберите резервные копии, которые необходимо отсканировать.
   - **Сканировать на**:
     - **Вредоносная программа**: этот параметр невозможно переопределить. Он обеспечивает проверку резервных копий на присутствие вредоносных программ.
   - **Шифрование**: предоставляет пароль для сканирования защищенных резервных копий. Если выбрано хранилище или несколько резервных копий, можно указать один пароль для всех резервных копий. Если указан неправильный пароль для резервной копии, система возвращает оповещение.
   - **Расписание**: этот параметр невозможно переопределить. Действие сканирования можно автоматически запустить в облачном хранилище данных.
4. После этого щелкните **Создать**.

В результате создается план сканирования резервных копий. Указанные расположения или резервные копии сканируются облачным агентом автоматически.

13.3 Планы резервного копирования для облачных приложений

В разделе **Планы** > **Резервные копии приложений в облаке** отображаются планы резервного копирования «облако в облако». Эти планы создают резервную копию приложений, которые выполняются в облаке посредством агентов, запущенных в облаке, и используют облачное хранилище данных в качестве хранилища резервных копий.

В этом разделе можно выполнить указанные ниже операции:

- Создавать, просматривать, запускать, останавливать, изменять и удалять план резервного копирования
- Просматривать действия, относящиеся к каждому плану резервного копирования
- Просматривать оповещения, относящиеся к каждому плану резервного копирования

13.3.0.1 Запуск процессов резервного копирования «облако в облако» вручную

Во избежание прерывания работы службы Кибер Бэкап Облачный количество ручных запусков резервного копирования «облако в облако» ограничено 10 запусками в час на одну организацию. По достижении этого количества число разрешенных запусков сбрасывается до одного в час, а каждый последующий час становится доступным один дополнительный запуск. Пример: первый час – 10 запусков, второй час – 1 запуск, третий час – 2 запуска и т. д. до достижения показателя в 10 запусков в час.

Невозможно вручную запустить планы резервного копирования, которые применены к группам устройств (почтовым ящикам, дискам, площадкам) или содержат более 10 устройств.

14 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.

14.1 Настраиваемый или готовый загрузочный носитель?

Используя мастер создания загрузочных носителей, можно создать настраиваемый загрузочный носитель (на основе Linux или на основе WinPE) для компьютеров Windows, Linux или macOS. 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.

14.2 Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE/WinRE?

14.2.1 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.

14.2.2 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).

14.3 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. Чтобы восстановить macOS, создайте отдельный носитель на машине с macOS.

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. 282).
   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.

Порядок создания физического загрузочного носителя в macOS

1. На машине с установленным агентом для Mac щелкните **Приложения** > **Конструктор аварийного диска**.
2. В программе отобразятся подключенные съемные носители. Выберите носитель, который требуется сделать загрузочным.

   Предупреждение
   Все данные на диске будут удалены.

3. Нажмите кнопку **Создать**.
4. Дождитесь создания загрузочного носителя.

14.4 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.

14.4.1 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.

14.4.2 32-разрядная или 64-разрядная версия?

Мастер создания загрузочных носителей позволяет создавать загрузочные носители как с 32-разрядными, так и 64-разрядными компонентами. В большинстве случаев для загрузки машины, которая использует интерфейс UEFI, требуется 64-разрядный носитель.

14.4.3 Загрузочные носители на основе Linux

Как создать загрузочный носитель на основе Linux

1. Запустите **мастер создания загрузочных носителей**.
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. 283).
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. 286).
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. 295).
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**.

14.4.3.1 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.

14.4.3.2 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 http://www.tldp.org/LDP/abs/html. Спецификация JSON доступна на сайте http://www.json.org.

Файлы сценария

Сценарий должен быть расположен в указанных ниже каталогах на машине, в которой установлен мастер создания загрузочных носителей:

- В ОС Windows: %**ProgramData%\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 https://busybox.net/downloads/BusyBox.html. Также могут быть использованы следующие команды:
  - acrocmd – утилита командной строки для создания резервной копии и восстановления
  - product – команда, запускающая пользовательский интерфейс загрузочного носителя

  Этот файл и все другие включенные в сценарий дополнительные файлы (например, посредством использования команды с точкой) должны быть расположены в подпапке **bin**. В сценарии укажите дополнительные пути к файлам в виде **/ConfigurationFiles/bin/<файл>**.
- **autostart** – файл для запуска **<файл_сценария>.sh**. Содержимое файла должно быть следующим:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<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

14.4.4 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).

14.4.5 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.

14.4.6 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
            }
        }
}
```

14.4.7 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).

14.4.7.1 Образы WinRE

Создание образов на основе WinRE поддерживается для следующих операционных систем:

- Windows 7 (64-разрядная версия)
- Windows 8, 8.1, 10 (32-разрядная и 64-разрядная версии)
- Windows Server 2012, 2016, 2019 (64-разрядная версия)

14.4.7.2 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)

Мастер создания загрузочных носителей поддерживает как 32-разрядные, так и 64-разрядные дистрибутивы WinPE. 32-разрядные дистрибутивы WinPE могут работать и на 64-разрядном оборудовании. Однако 64-разрядный дистрибутив требуется для загрузки машины, которая использует интерфейс UEFI.

Примечание
Для работы образов среды предустановки на основе WinPE 4 (и более поздних версий) требуется около 1 ГБ ОЗУ.

14.4.7.3 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.

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). Кроме этого, необходимо выполнить следующие действия:

   a. Выберите **Загрузить подключаемый модуль для WinPE (32-разрядный)**.

   b. Сохраните подключаемый модуль в каталог **%PROGRAM_ FILES%\BackupClient\BootableComponents\WinPE32**.
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. 295).
8. [Необязательно] Укажите драйверы Windows, которые нужно добавить в загрузочный носитель.

   После загрузки Windows PE или Windows PE на машину эти драйверы помогут получить доступ к устройствам, на которых расположена резервная копия. Добавьте 32-разрядные драйверы, если используется 32-разрядный дистрибутив WinPE или WinRE, или 64-разрядные драйверы, если используется 64-разрядный дистрибутив WinPE или WinRE.

   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.

14.4.7.4 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 Vista (PE 2.0):
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=ru
   Набор средств автоматизированной установки (AIK) для Windows Vista SP1 и Windows Server 2008 (PE 2.1):
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=ru
   Набор средств автоматизированной установки (AIK) для Windows 7 (PE 3.0):
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=ru
   Набор средств автоматизированной установки (AIK) для Windows 7 SP1 (PE 3.1):
   http://www.microsoft.com/download/en/details.aspx?id=5188
   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 (NETFXx86 или NETFXx64 в зависимости от оборудования).
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.

14.4.7.5 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 ра��вертывания и оценки (ADK).

   Комплект средств для развертывания и оценки Windows (ADK) для Windows 8 (PE 4.0): http://www.microsoft.com/en-us/download/details.aspx?id=30652.

   Комплект средств для развертывания и оценки Windows (ADK) для Windows 8.1 (PE 5.0): http://www.microsoft.com/ru-ru/download/details.aspx?id=39982.

   Комплект средств для развертывания и оценки Windows (ADK) для Windows 10 (PE для Windows 10): https://msdn.microsoft.com/en-us/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

   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.

14.4.8 Регистрация загрузочного носителя

Регистрация загрузочного носителя в службе Кибер Бэкап Облачный позволяет получить доступ к облачному хранилищу данных для ваших резервных копий. При создании загрузочного носителя можно предварительно настроить регистрацию. Если регистрация не настроена предварительно, можно зарегистрировать носитель после загрузки машины с его использованием.

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.
   - **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**.
3. В поле **Сервер** укажите адрес службы Кибер Бэкап Облачный.
4. В поле **Маркер регистрации** введите маркер регистрации.
5. Щелкните **Зарегистрироваться**.

14.4.9 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.

14.4.9.1 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.

14.5 Подключение машины, загруженной с загрузочного носителя

14.5.1 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.

14.5.2 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.

14.5.2.1 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**.

14.6 Операции с загрузочным носителем

Операции с загрузочным носителем подобны операциям резервного копирования и восстановления, которые выполняются при запущенной операционной системе. Отличие состоят в следующем:

1. Если используется загрузочный носитель с представлением томов по типу Windows, том имеет такую же букву диска, как в Windows. Томам, которые не имеют букв диска в Windows (например, том Зарезервировано системой), присваиваются свободные буквы в порядке их следования на диске.

   Если загрузочный носитель не обнаруживает ОС Windows на машине или обнаруживает несколько систем, всем томам (даже если они не имеют букв дисков), присваиваются буквы в порядке их следования на диске. Поэтому буквы томов могут отличаться от букв томов, отображаемых в Windows. Например, диск D: на загрузочном носителе может соответствовать диску E: в Windows.

   Примечание
   Рекомендуется назначить уникальные имена томам.

2. Загрузочный носитель с представлением томов по типу Linux отображает локальные диски и тома как отключенные (sda1, sda2...).
3. Задания невозможно запланировать в расписании. Если требуется повторить операцию, настройте ее с нуля.
4. Время существования журнала ограничено текущим сеансом. Весь журнал или отфильтрованные записи журнала можно сохранить в файл.
5. Централизованные хранилища не отображаются в дереве папок окна **Архив**.

   Для доступа к управляемому хранилищу введите следующую строку в поле **Путь**:
   bsp://адрес_узла/имя_хранилища/

   Для доступа к неуправляемому централизованному хранилищу введите полный путь к папке хранилища.

   После ввода учетных данных для доступа будет отображен список архивов, расположенных в хранилище.

14.6.1 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**.

14.6.2 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**.

14.7 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 утилиту аварийного восстановления 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).

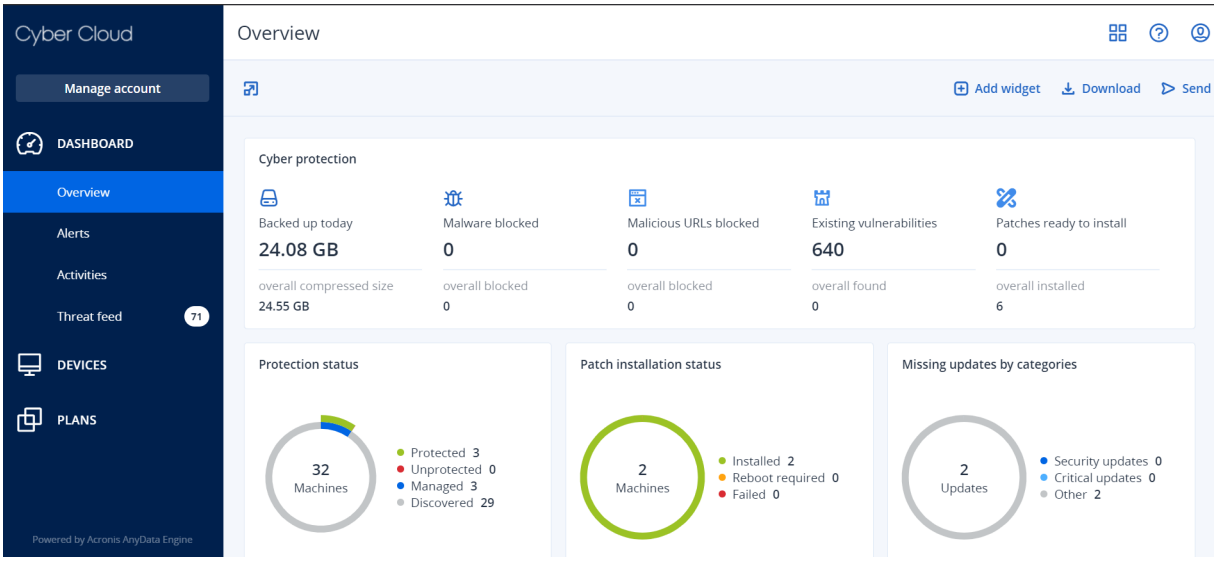
15 Мониторинг

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).

15.1 Статус защиты

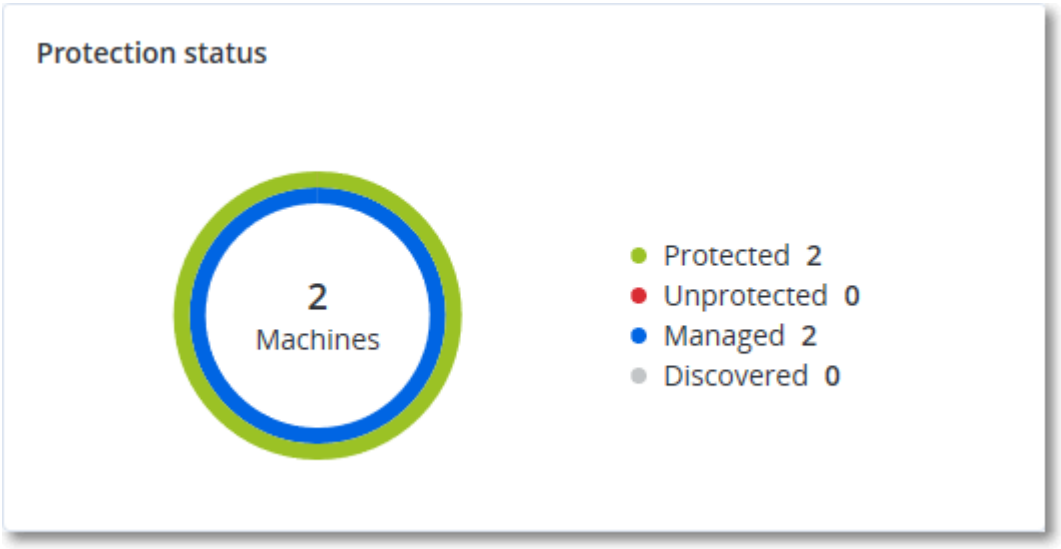
15.1.1 Статус защиты

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.



15.1.2 Обнаруженные машины

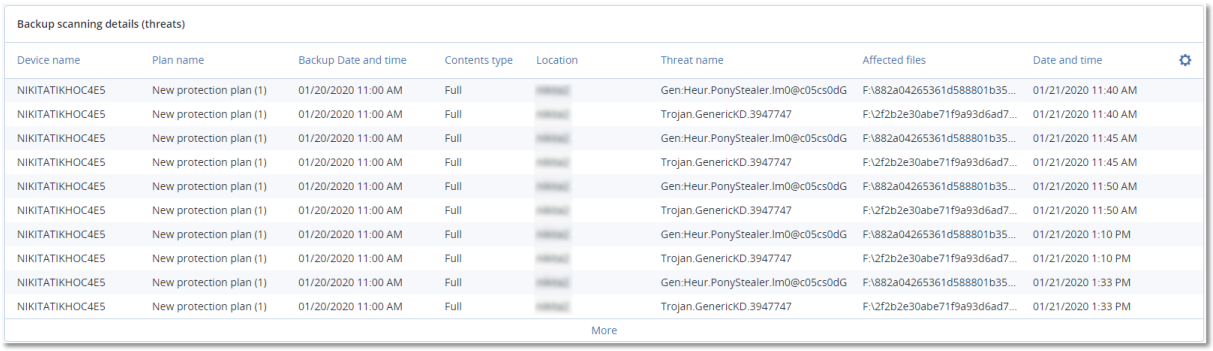
В этом виджете показан список машин, обнаруженных за указанный период времени.

Discovered machines

Device name ↑	IP address	OS	Organizational unit	Discovery type
Windows Server 2012 R2				
win-6g34mv70qa3	10.248.90.221	Windows Server 2012 R2	-	Local Network
Windows 10 Enterprise 2016 LTSB				
device1	10.248.90.238	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Local Network
device2	-	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory
device3	10.248.91.243	Windows 10 Enterprise 2016 LTSB	OU1	Active Directory, Manual, Loc...
device4	10.248.91.125	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Local Network
device5	-	Windows 10 Enterprise 2016 LTSB	-	Active Directory, Manual
-				
-	10.250.41.189	-	-	Manual
-	10.248.44.199	-	-	Manual

15.2 Сведения о сканировании резервной копии

В этом виджете показана подробная информация об обнаруженных угрозах в резервных копиях.



Backup scanning details (threats)

Device name	Plan name	Backup Date and time	Contents type	Location	Threat name	Affected files	Date and time
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:40 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:45 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 11:50 AM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:10 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Gen:Heur.PonyStealer.lm0@c05cs0dG	F:\882a04265361d588801b35...	01/21/2020 1:33 PM
NIKITATIKHOC4E5	New protection plan (1)	01/20/2020 11:00 AM	Full	[redacted]	Trojan.GenericKD.3947747	F:\2f2b2e30abe71f9a93d6ad7...	01/21/2020 1:33 PM

More

15.3 Облачные приложения

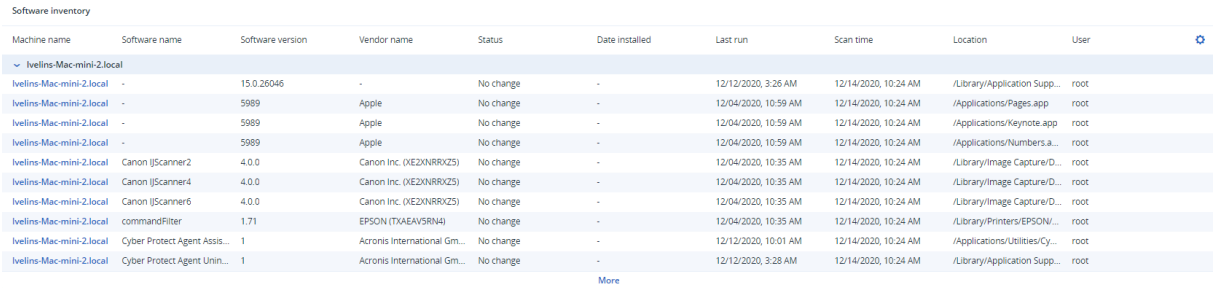
В этом виджете показана подробная информация о ресурсах "облако в облако".

Дополнительная информация о ресурсах "облако в облако" также доступна в следующих виджетах:

- Действия
- Список действий
- 5 последних оповещений
- Журнал оповещений
- Сводка по активным оповещениям
- Сводка по истории активных оповещений
- Подробная информация об активных оповещениях
- Сводные данные о хранилищах

15.4 Виджеты «Инвентаризация программного обеспечения»

В табличном виджете **Инвентаризация программного обеспечения** отображается подробная информация обо всем программном обеспечении, которое установлено на устройствах Windows и macOS в вашей организации.

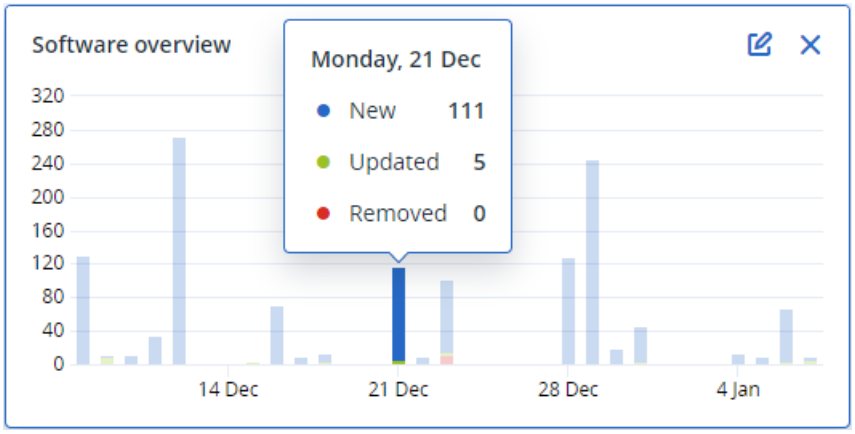


Software inventory

Machine name	Software name	Software version	Vendor name	Status	Date installed	Last run	Scan time	Location	User
Ivelins-Mac-mini-2.local									
Ivelins-Mac-mini-2.local	-	15.0.26046	-	No change	-	12/12/2020, 3:26 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Pages.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Keynote.app	root
Ivelins-Mac-mini-2.local	-	5989	Apple	No change	-	12/04/2020, 10:59 AM	12/14/2020, 10:24 AM	/Applications/Numbers.a...	root
Ivelins-Mac-mini-2.local	Canon IJScanner2	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon IJScanner4	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	Canon IJScanner6	4.0.0	Canon Inc. (XE2XNRRXZ5)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Image Capture/D...	root
Ivelins-Mac-mini-2.local	commandFilter	1.71	EPSON (TXAEAV5RN4)	No change	-	12/04/2020, 10:35 AM	12/14/2020, 10:24 AM	/Library/Printers/EPSON/...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Assis...	1	Acronis International Gm...	No change	-	12/12/2020, 10:01 AM	12/14/2020, 10:24 AM	/Applications/Utilities/Cy...	root
Ivelins-Mac-mini-2.local	Cyber Protect Agent Unin...	1	Acronis International Gm...	No change	-	12/12/2020, 3:28 AM	12/14/2020, 10:24 AM	/Library/Application Supp...	root

More

В табличном виджете **Обзор программы** отображается информация о новых, обновленных и удаленных приложениях на устройствах Windows и macOS в вашей организации за указанный период времени (7 дней, 30 дней или текущий месяц).



Если навести курсор на определенную полосу на диаграмме, отобразится подсказка со следующей информацией:

Новое: количество новых установленных приложений.

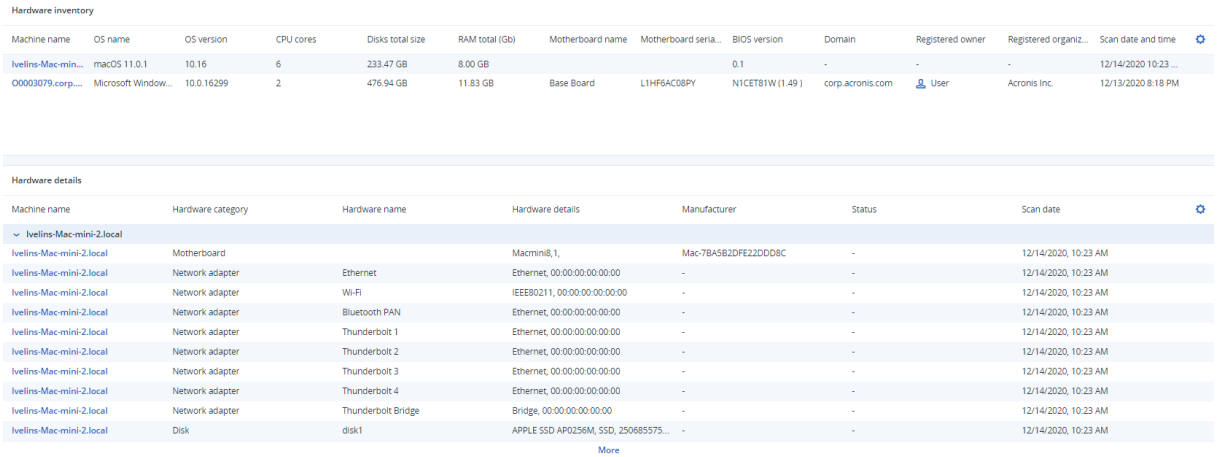
Обновлено: количество обновленных приложений.

Удаленные: количество удаленных приложений.

Если щелкнуть часть полосы для определенного статуса, будет выполнено перенаправление на страницу **Управление программным обеспечением** -> **Инвентаризация программного обеспечения**. Информация на этой странице отфильтрована по дате и состоянию.

15.5 Виджеты «Инвентарь оборудования»

В табличных виджетах **Инвентарь оборудования** и **Сведения об оборудовании** отображается информация обо всем оборудовании, которое установлено на физических и виртуальных устройствах Windows и macOS в вашей организации.


Hardware inventory

Machine name	OS name	OS version	CPU cores	Disks total size	RAM total (Gb)	Motherboard name	Motherboard seria...	BIOS version	Domain	Registered owner	Registered organiz...	Scan date and time
Ivelins-Mac-min...	macOS 11.0.1	10.16	6	233.47 GB	8.00 GB			0.1	-	-	-	12/14/2020 10:23 ...
O0003079.corp....	Microsoft Window...	10.0.16299	2	476.94 GB	11.83 GB	Base Board	L1HF6AC08PY	N1CET81W (1.49)	corp.acronis.com	User	Acronis Inc.	12/13/2020 8:18 PM

Hardware details

Machine name	Hardware category	Hardware name	Hardware details	Manufacturer	Status	Scan date
Ivelins-Mac-mini-2.local						
Ivelins-Mac-mini-2.local	Motherboard		Macmini8,1,	Mac-7BA5B2DFE22DDD8C	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Ethernet	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Wi-Fi	IEEE80211, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Bluetooth PAN	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 1	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 2	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 3	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt 4	Ethernet, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Network adapter	Thunderbolt Bridge	Bridge, 00:00:00:00:00:00	-	-	12/14/2020, 10:23 AM
Ivelins-Mac-mini-2.local	Disk	disk1	APPLE SSD AP0256M, SSD, 250685575...	-	-	12/14/2020, 10:23 AM

More

В табличном виджете **Изменения оборудования** отображается информация о добавленном, удаленном и измененном оборудовании на физических и виртуальных устройствах Windows и macOS в вашей организации за указанный период времени (7 дней, 30 дней или текущий месяц).


Hardware changes

Machine name	Hardware category	Status	Old value	New value	Modification date and time
DESKTOP-0FF9TTF					
DESKTOP-0FF9TTF	Network adapter	Changed	Oracle Corporation, Ethernet 802.3,...	Oracle Corporation, Ethernet 802.3, ...	01/11/2021 9:28 AM
DESKTOP-0FF9TTF	Network adapter	New	-	Realtek Semiconductor Corp., Ether...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Motherboard	New	-	LENOVO, Torronto 5C1, PF0PJB10	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	GPU	New	-	Intel(R) HD Graphics Family	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Disk	New	-	(Standard disk drives), WDC WD10JP...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Cisco Systems, Ethernet 802.3, 00:0...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	Oracle Corporation, Ethernet 802.3, ...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Samsung, 985D7122, 4.00 GB	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	Network adapter	New	-	TAP-NordVPN Windows Provider V9...	01/04/2021 2:37 PM
DESKTOP-0FF9TTF	RAM	New	-	Micron, 00000000, 4.00 GB	01/04/2021 2:37 PM

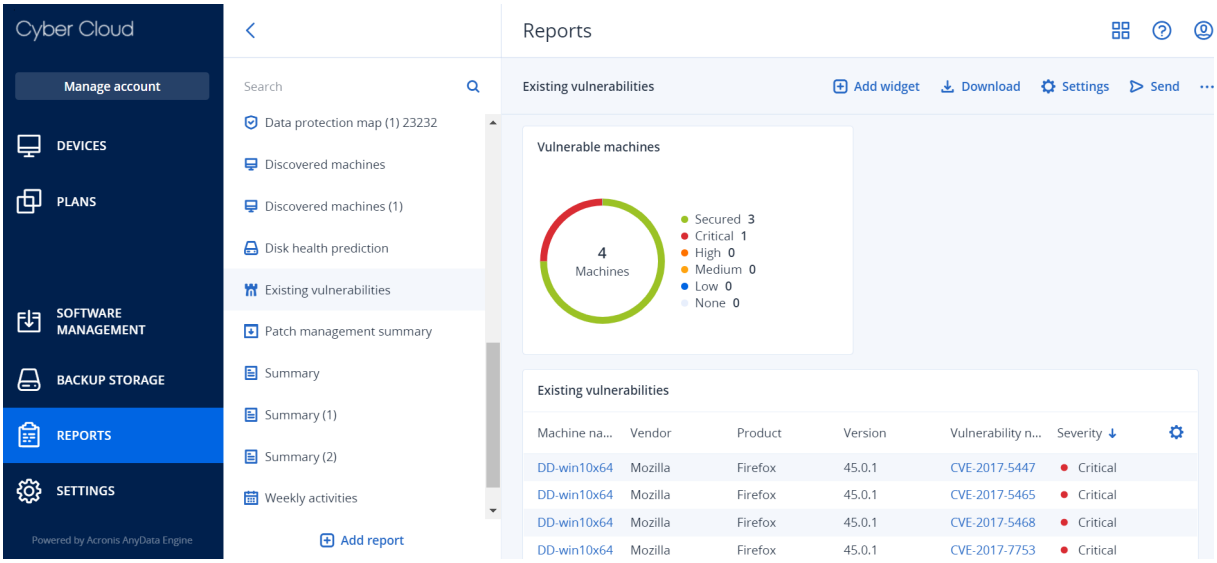
More

16 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.
Сведения о сканировании резервной копии	Показывает подробную информацию об угрозах, выявленных в резервных копиях.
Ежедневные задания	Показывает сводную информацию о действиях, выполненных за указанный период времени.
Карта защиты данных	Показывает подробную информацию о количестве, размере, расположении, статусе защиты всех важных файлов на машинах.
Обнаруженные угрозы	Показывает сведения о машинах, на которых выявлены проблемы: количество заблокированных угроз, а также количество машин без уязвимостей и с уязвимостями.
Обнаруженные	Показывает все найденные машины в сети организации.

машины	
Прогноз работоспособности диска	Показывает прогнозы относительно времени выхода дисков HDD/SSD из строя, а также информацию о текущем состоянии дисков.
Имеющиеся уязвимости	Показывает имеющиеся уязвимости операционной системы и приложений в вашей организации. В этом отчете также указаны сведения о машинах в вашей сети, на которых выявлены проблемы, для каждого продукта в списке.
Инвентаризация программного обеспечения	Отображает информацию о программном обеспечении, которое установлено на устройствах компании.
Инвентарь оборудования	Отображает информацию об оборудовании, которое доступно на устройствах компании.
Сводка управления исправлениями	Показывает количество отсутствующих исправлений, установленных исправлений и применимых исправлений. При поиске в отчетах можно найти информацию об отсутствующих/установленных исправлениях, а также сведения обо всех системах.
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.

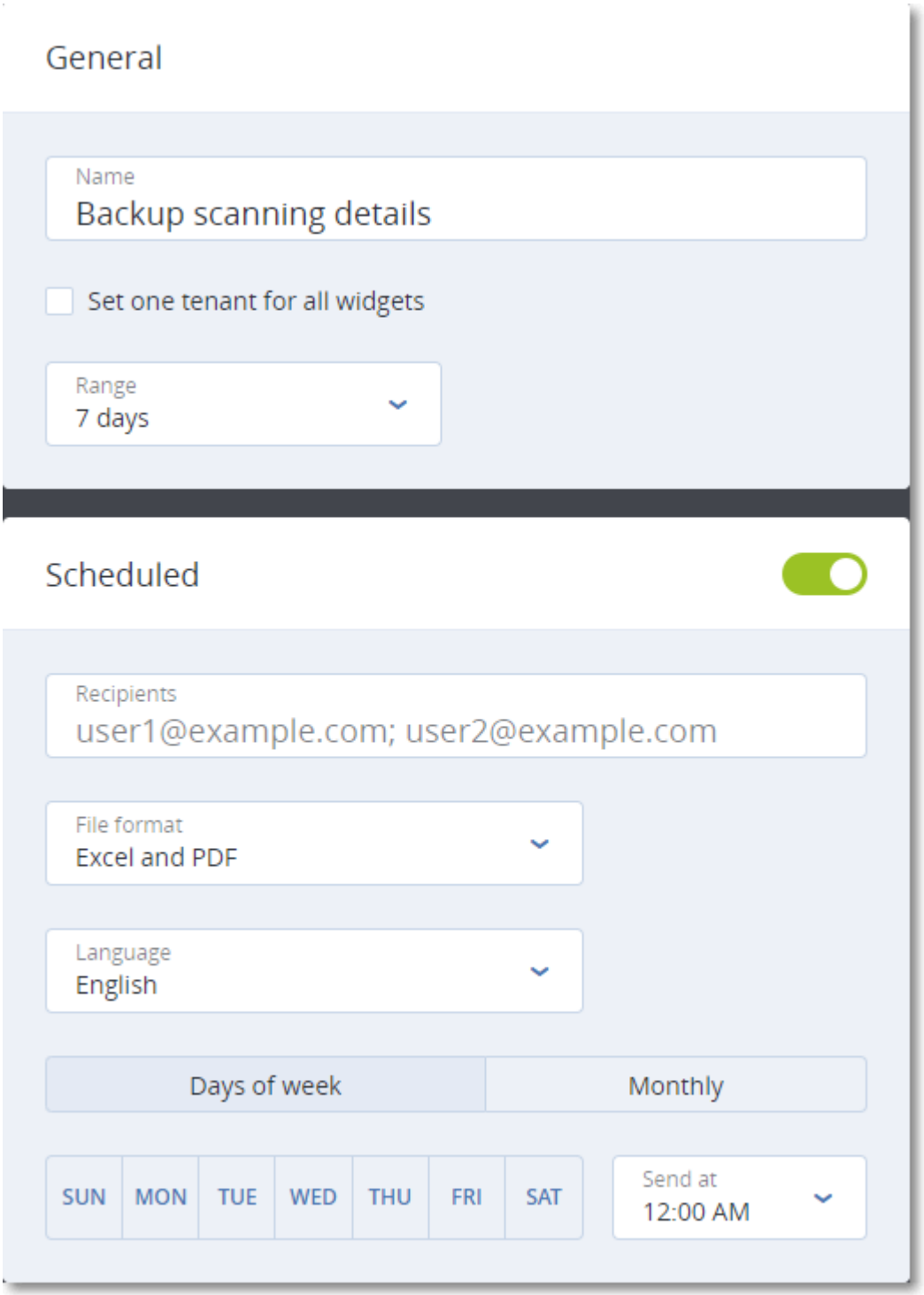
16.0.1 Добавление отчета

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.

16.0.2 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.



16.0.3 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.

16.0.4 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**.

16.0.5 Скачивание отчета

Чтобы скачать отчет, щелкните **Скачать** и выберите необходимые форматы:

- Excel и PDF
- Excel
- PDF

16.0.6 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.

17 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

R

Runbook

[Аварийное восстановление] Запланированный сценарий из настраиваемых шагов, которые автоматизируют операции аварийного восстановления.

A

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.

B

Виртуальная машина

Виртуальная машина, резервное копирование которой выполняется на уровне гипервизора сторонним агентом, например агентом для VMware или агентом для Hyper-V. Виртуальная машина, которая содержит агент, воспринимается службой резервного копирования как физическая.

Возврат из реплики

Перенос рабочей нагрузки с резервного сервера (например, с реплики виртуальной машины или сервера восстановления в облаке) на рабочий сервер.

Д

Директивные точки восстановления (Recovery point objective, RPO)

[Аварийное восстановление] Объем утраченных данных при сбое, продолжительность которого соответствует продолжительности планового простоя или аварийного сбоя. Порог директивной точки восстановления определяет максимальный интервал времени, разрешенный между последней точкой восстановления, подходящей для перехода к реплике, и текущим временем.

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.

Л

Локальный сайт

[Аварийное восстановление] Локальная инфраструктура, развернутая внутри вашей компании.

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

О

Облачная площадка (или площадка аварийного восстановления)

[Аварийное восстановление] Удаленная площадка в облаке, которая используется для выполнения инфраструктуры восстановления в случае аварии.

Облачный сервер

[Аварийное восстановление] Общее название сервера восстановления или основного сервера.

Общедоступный IP-адрес

[Аварийное восстановление] IP- адрес, необходимый для доступности облачных серверов через Интернет.

Основной сервер

[Аварийное восстановление] Виртуальная машина, которая не имеет связанной машины (например, сервера восстановления) на локальной площадке. Основные серверы используются для защиты приложения или запуска различных вспомогательных служб (например, веб-сервера).

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», «Антивирус и защита от вредоносных программ», «Фильтрация URL- адресов», «Антивирусная программа "Защитник Windows"», Microsoft Security Essentials, «Оценка уязвимостей», «Управление исправлениями», «Карта защиты данных», «Контроль устройств».

Подключение «сеть-сеть» (site-to-site, S2S)

[Аварийное восстановление] Подключение, которое распространяет локальную сеть на облако посредством безопасного туннелирования VPN.

Подключение «точка-сеть» (point-to-site, P2S)

[Аварийное восстановление] Безопасное подключение VPN извне к облачным и локальным площадкам с конечных точек (например, с компьютера или ноутбука).

Полная резервная копия

Самостоятельная резервная копия, содержащая все необходимые данные. Для восстановления данных из нее не нужен доступ к какой-либо другой резервной копии.

Проверочный IP-адрес

[Аварийное восстановление] IP- адрес, необходимый при использовании проверочного перехода к реплике во избежание дублирования IP- адреса, используемого в рабочей среде.

Программно-аппаратный комплекс VPN

[Аварийное восстановление] Специальная виртуальная машина, которая обеспечивает подключение между локальной сетью и облачной площадкой через безопасный туннель VPN. Программно- аппаратный VPN развертывается на локальной площадке.

Р

Рабочая сеть

[Аварийное восстановление] Внутренняя сеть, расширенная средствами туннелирования VPN и охватывающая как локальные, так и облачные площадки. В рабочей сети локальные и облачные серверы могут обмениваться данными друг с другом.

С

Сервер восстановления

[Аварийное восстановление] Виртуальная машина — реплика первоначальной машины, созданная на основе резервных копий

защищенного сервера, сохраненных в облаке. Серверы восстановления используются для переноса рабочих нагрузок с оригинальных серверов в случае аварии.

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.

Т

Тестовая сеть

[Аварийное восстановление] Изолированная виртуальная сеть, которая используется для тестирования процесса перехода к реплике.

Ф

Физическая машина

Компьютер, резервное копирование которого выполняется с помощью агента, установленного в операционной системе.

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.

Ш

Шлюз VPN (старое название — сервер VPN или шлюз подключения)

[Аварийное восстановление] Специальная виртуальная машина, которая обеспечивает подключение между сетями локальной площадки и облачной площадки чрез безопасный туннель VPN. Шлюз VPN развернут на облачной площадке.

Указатель

.

...мне нужно использовать другое устройство второго фактора? 33

...потеряно устройство второго фактора? 33

3

32-разрядная или 64-разрядная версия? 282

F

Flashback 214

L

Linux 135

M

Mac 135

McAfee Endpoint Encryption и PGP Whole Disk Encryption 28

Microsoft Exchange Server 171

Microsoft SQL Server 170

O

oVirt/Red Hat Virtualization 4.2 и 4.3 99

oVirt/Red Hat Virtualization 4.4 99

S

Storage vMotion 260

U

Universal Restore в Linux 203

Universal Restore в Windows 201

V

vMotion 260

W

Windows 135

A

Автоматическая установка и удаление в macOS 64

Автоматические обновления компонентов 106

Автоматический поиск драйверов 202

Автоматическое и ручное обнаружение 73

Автоматическое обнаружение машин 70

Автоматическое установка или автоматическое удаление 52

Автоматическое установка или автоматическое удаление в Linux 58

Автоматическое установка или автоматическое удаление в Windows 52

Агент для Exchange (для резервного копирования почтового ящика) 18

Агент для Hyper-V 20

Агент для Linux 19

Агент для Mac 19

Агент для Oracle 18

Агент для oVirt 21

требуемые роли и порты 99

Агент для Scale Computing HC3 20

требуемые роли 87

Агент для SQL, агент для Active Directory, агент

для Exchange (для резервного копирования базы данных и резервного копирования с поддержкой приложений) 18

Агент для Virtuozzo 20

Агент для Virtuozzo Hybrid Infrastructure 20

Агент для VMware

необходимые привилегии 262

Агент для VMware – резервное копирование без использования локальной сети 253

Агент для VMware (Windows) 20

Агент для VMware (виртуальное устройство) 20

Агент для Windows 17

Агент службы предотвращения утечки данных 18

Активация учетной записи 32

Алгоритм распределения 257

Б

Базовые параметры 53, 59

Безопасность на уровне файлов 214

Быстрое инкрементное/дифференциальное резервное копирование 173

В

В macOS 46, 50, 105

В Windows 44, 48, 104

В интервале времени 153

В ОС Linux 45, 48, 105

В случае ошибки повторить попытку 172, 213

Виджеты «Инвентаризация программного обеспечения» 304

Виджеты «Инвентарь оборудования» 305

Виртуальная машина 197

Вкладка «Планы» 277

Вкладка «Хранилище резервных копий» 218

Включение доступа к сети VLAN через магистральный порт 297

Включение сканирования инвентаря оборудования 271

Включение фильтров файлов 174

Включите целевую виртуальную машину по окончании восстановления. 218

Включить полное резервное копирование VSS 190

Возврат к исходному начальному RAM-диску 204

Восстановление 191, 299

памятка 191

Восстановление с сетевой папки 286

Восстановление баз данных Exchange 235

Восстановление баз данных Exchange в виде файлов 237

Восстановление баз данных SQL 231

Восстановление баз данных SQL в виде файлов 233

Восстановление базы данных master 234

Восстановление базы данных в запущенный экземпляр SQL Server 232

Восстановление дисков с помощью загрузочного носителя 199

Восстановление из облачного хранилища 286

Восстановление конфигурации ESXi 209

Восстановление машины 193

Восстановление на Exchange Server 239

Восстановление полного пути 215

Восстановление почтовых ящиков 239, 246

Восстановление почтовых ящиков Exchange и элементов почтового ящика 238

Восстановление почтовых ящиков и элементов почтовых ящиков 246

Восстановление при загрузке 299

Восстановление приложений 223

Восстановление системных баз данных 234

Восстановление состояния системы 208

Восстановление файлов 204

Восстановление файлов с помощью веб-интерфейса 204

Восстановление файлов с помощью загрузочного носителя 207

Восстановление физической машины 193

Восстановление физической машины в виртуальную 195

Восстановление физической машины как виртуальной 195

Восстановление элементов почтовых ящиков 241, 247

Встроенные группы 114

Выбор баз данных SQL 226

Выбор данных Exchange Server 227

Выбор данных для резервного копирования 133

Выбор дисков и томов 133

Выбор компонентов для установки 77

Выбор конфигурации ESXi 138

Выбор места назначения 139

Выбор почтовых ящиков 245

Выбор почтовых ящиков Exchange 231

Выбор почтовых ящиков сервера Exchange 231

Выбор состояния системы 138

Выбор файлов и папок 136

Выключать целевые виртуальные машины при запуске восстановления 218

Выключение сканирования инвентаря оборудования 272

Высокая доступность восстановленной машины 267

Г

Где можно просмотреть имена файлов резервных копий? 164

Группы устройств 114

Д

Дамп данных отчета 310

Дата и время для файлов 213

Двухфакторная проверка подлинности 32

Дедупликация в архиве 168

Дедупликация данных 30

Действия при сбое задания 188

Для восстановления баз данных Exchange на запущенный сервер Exchange Server 236

Для изменения используемых по умолчанию параметров 159

Для изменения учетных данных Exchange Server для доступа к резервной копии почтового ящика 244

Для изменения учетных данных для доступа к SQL Server или Exchange Server 244

Для каких элементов можно создавать резервные копии? 245

Для настройки виртуального приложения 86, 93, 98

Для резервного копирования и репликации виртуальных машин VMware необходимы порты TCP 39

Для чего используется мастер создания загрузочных носителей? 282

Добавление VLAN 297

Добавление отчета 308

Добавление устройств в статические группы 115

Дополнительные параметры 56, 61

Дополнительные параметры расписания 145

Дополнительные требования для виртуальных машин 229

Дополнительные требования для операций резервного копирования с поддержкой приложений 225

Доступ к службе Кибер Бэкап Облачный 34

Доступность параметров восстановления 210

Доступность параметров резервного копирования 159

Доступные действия с планами защиты 127

Драйверы запоминающих устройств для обязательной установки 202

Е

Еженедельное резервное копирование 191

Если вы удалили локальные резервные копии в диспетчере файлов 222

Ж

Журнал событий Windows 191, 218

З

За указанное количество дней подряд не создано успешно ни одной резервной копии. 162

Загрузка файлов из облачного хранилища данных 205-206

Загрузочные носители на основе Linux 282

Загрузочный носитель 280

Загрузочный носитель на основе Linux или загрузочный носитель на основе WinPE/WinRE? 280

Загрузочный носитель на основе WinPE и WinRE 291

Запуск виртуальной машины из резервной копии (мгновенное восстановление) 249

Запуск машины 250

Запуск процессов резервного копирования «облако в облако» вручную 279

Запуск резервного копирования вручную 158

Защита Microsoft SQL Server и Microsoft Exchange Server 223

Защита Oracle Database 249

Защита контроллера домена 223

Защита приложений Microsoft 223

Защита размещенных данных Exchange 245

Заявление об авторских правах 2

И

Извлечение файлов из локальных резервных копий 208

Изменение идентификатора безопасности 217

Изменение квоты службы машин 109

Изменение отчета 308

Изменение портов, используемых агентом Cyber Protection 40

Изменение учетной записи входа на машинах Windows 50

Изменение учетных данных для доступа к SQL Server или Exchange Server 244

Изменение учетных данных доступа vCenter Server или хоста ESXi 261

Изменение формата резервной копии на "Версия 12" (TIBX) 168

Имена без переменных 166

Именение параметров прокси-сервера в Linux 45

Имя файла резервной копии 163

Имя файла резервной копии по умолчанию 165

Инвентарь оборудования 271

Исключения файлов 214

Исключить системные файлы и папки 175

Исключить скрытые файлы и папки 175

Исключить файлы, соответствующие определенным критериям 174

Использование Universal Restore 201

Использование локально присоединенного хранилища 256

Использование переменных 166

Использование правил политики 133, 137

К

Как выбрать локально присоединенное хранилище в качестве места назначения резервной копии 257

Как отвязать машину от агента 259

Как отключить UAC 76

Как подготовить машину с ADK 294

Как подготовить машину с AIK 294

Как подключить агент для Exchange к CAS 230

Как подключить базу данных 235

Как прикрепить хранилище к уже работающему агенту 257

Как создать загрузочный носитель на основе Linux 282

Как указать команду или исполняемый файл, которые будут выполнены после завершения восстановления 217

Как указать команду или исполняемый файл, которые будут выполнены после завершения резервного копирования 183

Как указать команду или пакетный файл, выполняемый перед началом восстановления 216

Как указать команду или пакетный файл, которые будут выполнены до захвата данных 184

Как указать команду или пакетный файл, которые будут выполнены перед началом резервного копирования 182

Как указать команду или пакетный файл, которые будут выполнены после захвата данных 185

Какие элементы можно восстановить? 245

Какой агент необходим? 35

Команда до захвата данных 184

Команда до резервного копирования 182

Команда после восстановления 217

Команда после захвата данных 185

Команда после резервного копирования 183

Команда, выполняемая перед восстановлением 216

Команды до и после захвата данных 184

Команды до и после процедуры 182, 215

Консолидация резервных копий 162

Консоль службы 111

Копирование библиотек Microsoft Exchange Server 244

Л

Локальное подключение 297

М

Мастер создания загрузочных носителей 282

Миграция машины 268

Многотомные моментальные снимки 178

Моментальные снимки резервных копий на уровне файлов 175

Мониторинг 301

Н

На загрузочном носителе 47

На основе Linux 280

На основе WinPE/WinRE 280

Назначение прав пользователя 51

Настраиваемый или готовый загрузочный носитель? 280

Настройка виртуального устройства 82, 86, 93, 98

Настройка режима отображения 298

Настройка сетей в Virtuozzo Hybrid Infrastructure 89

Настройка сети 297

Настройка учетных записей пользователей в Virtuozzo Hybrid Infrastructure 89

Настройки Universal Restore 202

Настройки безопасности 106

Настройки прокси-сервера 44

Не запускать при подключении к следующим сетям Wi-Fi 155

Не запускать при работе на лимитном подключении 154

Не отображать во время обработки сообщения и диалоговые окна (режим без вывода сообщений) 172, 213

Необходимые порты 99

Непосредственный выбор 133, 136

О

О программе Зона безопасности 141

Обзор инвентаря оборудования 273

Облачное хранилище данных 172

Облачные приложения 304

Обнаружение машин 73

Обнаруженные машины 303

Обновление агентов 102

Обновление определений Cyber Protection согласно расписанию 108

Обновление определений киберзащиты на машине 104

Обновление определений киберзащиты по требованию 108

Обработка ошибок 172, 213

Образы WinPE 292

Образы WinRE 292

Общее правило резервного копирования 28

Общие требования 224

Объект высшего уровня 288

Объект переменной 288

Ограничение общего количества виртуальных машин, для которых одновременно выполняется резервное копирование 267

Ограничения 26, 89, 96, 139, 141, 206, 213, 255

Ограничения для имени файла резервной копии 165

Ожидать выполнения условий расписания 189

Окно резервного копирования 179

Операторы 122

Операции с загрузочным носителем 298

Операции с планами защиты 127

Операции с резервными копиями 218

Оповещения 162

Отключение автоматического назначения для агента 259

Отключить автоматический DRS для агента 81

Отмена регистрации машины 68

Отчеты 307

П

Пакеты Linux 41

Параметры 284

Параметры автоматической установки или автоматического удаления 53, 59

Параметры восстановления 210

Параметры для устаревших функций 63

Параметры информации 62

Параметры регистрации 55, 60

Параметры резервного копирования 159

Параметры резервного копирования по умолчанию 159

Параметры удаления 57, 63

Параметры установки 53, 59

Параметры ядра 283

Пароли со специальными символами или пробелами 69

Перед началом 80, 84, 87, 95

Перераспределение 258

План защиты 277

памятка 131

План защиты и модули 125

План конфликтует с уже примененными планами. 126

План сканирования резервных копий 278

План устройства конфликтует с планом группы 126

Планирование 186

Планирование отчета 310

Планирование по событиям 147

Планы резервного копирования для облачных приложений 279

По событию в журнале событий Windows 149

Повтор попытки в случае ошибки при создании моментального снимка виртуальной машины 173

Подготовка 38, 201

Подготовка WinPE 2.x и 3.x 294

Подготовка WinPE 4.0 и более поздние версии 294

Подготовка машины для удаленной установки 76

Подготовьте драйверы 201

Поддерживаемые веб-браузеры 17

Поддерживаемые версии Microsoft Exchange Server 21

Поддерживаемые версии Microsoft SQL Server 21

Поддерживаемые версии Oracle Database 21

Поддерживаемые версии SAP HANA 21

Поддерживаемые операционные системы и среды 17

Поддерживаемые платформы виртуализации 22

Поддерживаемые функции Кибер Бэкап Облачный по операционным системам 11

Поддержка миграции VM 260

Поддержка мультитенантности 124

Поддержка файловых систем 29

Подключение баз данных Exchange Server 238

Подключение баз данных SQL Server 235

Подключение машины, загруженной с загрузочного носителя 297

Подключение томов из резервной копии 220

Полезная информация о финализации 253

Получение журналов 312

Пользователи завершили сеанс 152

Пользователь неактивен 151

Пользовательские группы 114

Пользовательские сценарии 287

Порты, требуемые для компонента "Загрузчик" 40

Порядок активации Восстановление при загрузке на машине без агента 300

Порядок активации Восстановление при загрузке на машине с агентом для Windows или агентом для Linux 300

Порядок включения прямого доступа к хранилищу данных для агента. 254

Порядок включения сканирования инвентаря оборудования 271

Порядок восстановления дисков с помощью загрузочного носителя 199

Порядок восстановления конфигурации ESXi 209

Порядок восстановления почтового ящика из резервной копии почтового ящика 241

Порядок восстановления почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных 239

Порядок восстановления элемента почтового ящика из резервной копии почтового ящика 243

Порядок восстановления элементов почтовых ящиков из резервной копии с поддержкой приложений или резервной копии базы данных 241

Порядок входа в службу Кибер Бэкап Облачный 34

Порядок выбора баз данных SQL 226

Порядок выбора данных Exchange Server 227

Порядок выбора конфигурации ESXi 139

Порядок добавления виджета 301

Порядок запуска сканирования инвентаря оборудования на одном устройстве 272

Порядок защиты виртуальных машин в кластере Scale Computing HC3 86

Порядок защиты виртуальных машин в кластере Virtuozzo Hybrid Infrastructure 95

Порядок извлечения файлов из резервной копии 208

Порядок изменения виджета 301

Порядок изменения плана защиты 127

Порядок изменения расположения виджетов на панели мониторинга 301

Порядок использования Universal Restore 201

Порядок назначения роли "Средство обновления" агенту 104

Порядок назначения роли "Средство обновления" агенту защиты 107

Порядок настройки двухфакторной проверки подлинности для вашей учетной записи 32

Порядок обновления агента для VMware (виртуальное устройство) версий, более ранних, чем 12.5.23094 103

Порядок обновления агента через консоль службы 103

Порядок обновления определений киберзащиты для определенной машины по требованию 108

Порядок отзыва плана защиты с машин 128

Порядок отключения ограничений удаленного контроля учетных записей (UAC) 77

Порядок отключения тома 221

Порядок подготовки машины для роли «Средство обновления» 107

Порядок подключения тома из резервной копии 220

Порядок получения информации об агенте, управляющем конкретной машиной 84, 88, 96

Порядок предварительной настройки регистрации в службе Кибер Бэкап Облачный 295

Порядок предоставления доступа ко всем проектам в домене "По умолчанию" 89

Порядок предоставления доступа ко всем проектам в другом домене 90

Порядок привязки машины к агенту 258

Порядок применения существующего плана резервного копирования 127, 130

Порядок проверки действующих ролей во всех проектах 91

Порядок проверки назначенных ролей 90

Порядок просмотра всех компонентов оборудования, доступных на устройствах Windows и macOS в компании 273

Порядок просмотра подробной информации об оборудовании определенного устройства 275

Порядок регистрации агента для Mac 64

Порядок регистрации загрузочного носителя после загрузки машины с него 295

Порядок регистрации машины 66

Порядок сброса пароля 34

Порядок скачивания установочного файла (.dmg) 64

Порядок создания PE-образа (ISO-файла) из получившегося WIM-файла 293

Порядок создания загрузочного носителя в Windows и Linux 281

Порядок создания загрузочного носителя на базе WinPE или WinRE 292

Порядок создания Зона безопасности 142

Порядок создания первого плана защиты в разделе «Устройства» 125

Порядок создания первого плана защиты с включенным модулем "Резервное копирование" 129

Порядок создания плана резервного копирования 277

Порядок создания плана сканирования резервных копий 278

Порядок создания физического загрузочного носителя в macOS 282

Порядок удаление машины с консоли службы вручную 106

Порядок удаление резервных копий на любой машине 221

Порядок удаления агента для Mac 66

Порядок удаления виджета 302

Порядок удаления виртуальной машины или хоста ESXi без агента 112

Порядок удаления виртуальной машины, которая запущена из резервной копии 252

Порядок удаления Зона безопасности 143

Порядок удаления кэшированных данных на агенте 104

Порядок удаления машины из консоли службы 112

Порядок удаления плана защиты 128

Порядок удаления резервных копий машины, которая включена и присутствует в консоли службы 221

Порядок удаления резервных копий непосредственно из облачного хранилища данных 222

Порядок установки или удаления агента защиты 58

Порядок финализации машины, которая запущена из резервной копии 252

Посекторное резервное копирование 187

Почему нужно использовать раздел Зона безопасности? 141

Почему нужно использовать резервное копирование с поддержкой приложений? 228

Права, требуемые для учетной записи входа 50

Правила выбора для Linux 137

Правила выбора для macOS 138

Правила выбора для Windows 137

Правила для Linux 134

Правила для macOS 134

Правила для Windows 134

Правила для Windows, Linux и macOS 133

Правила хранения 157

Предварительная настройка нескольких сетевых подключений 296

Предварительные требования 71, 100, 103, 139, 197, 224, 250, 272-273, 275

Предопределенный сценарий 286

Преобразование диска в результате создания раздела Зона безопасности 142

Привязка виртуальной машины 257

Привязка вручную 258

Применение нескольких планов к устройству 126

Применение плана защиты к группе 123

Пример 90-91, 151-156

Установка пакетов вручную в Fedora 14 43

Пример. Аварийное резервное копирование при обнаружении «плохого блока» 150

Примеры 57, 63-65

Примеры использования 166, 249, 259

Примечание для пользователей Mac 192

Принципы работы 70

Приоритет ЦП 180

Проблемы с лицензией 126

Проверить IP-адрес устройства 156

Проверка резервных копий 169, 211

Проверьте наличие доступа к драйверам в загрузочной среде 202

Производительность 215

Производительность и окно резервного копирования 178

Пропуск поврежденных секторов 173

Пропустить задание 189

Просмотр инвентаря одного устройства 275

Просмотр результата распределения 258

Просмотр статуса резервного копирования в клиенте vSphere 262

Процедура 197

Процедуры восстановления для конкретных программ 28

Процесс Universal Restore 203

Процесс обнаружения машины 71

P

Работа в VMware vSphere 253

Разбиение 188

Развертывание агента для oVirt (виртуальное устройство) 95

Развертывание агента для Scale Computing HC3 (виртуальное устройство) 84

Развертывание агента для Virtuozzo Hybrid Infrastructure (виртуальное устройство) 87

Развертывание агента для VMware (виртуальное устройство) 80

Развертывание агентов с использованием групповой политики 100

Развертывание шаблона OVA 97

Развертывание шаблона OVF 81

Развертывание шаблона QCOW2 85, 92

Разрешение конфликтов плана 125-126

Расписание 144

Расширенный выбор расположений хранения 140

Регистрация загрузочного носителя 295

Регистрация машин вручную 66

Режим загрузки 212

Резервная копия почтового ящика 230

Резервное копирование 129

Резервное копирование базы данных 226

Резервное копирование и восстановление 129

Резервное копирование кластеризованных машин Hyper-V 266

Резервное копирование с поддержкой приложений 228

Рекомендации 212

Ручной запуск сканирования инвентаря оборудования 272

C

Сведения о сканировании резервной копии 303

Свойства событий 149

Сетевые настройки 296

Системные требования для агента 80, 84, 88, 95

Системные требования для агентов 37

Скачивание отчета 310

Сколько агентов необходимо? 81, 84, 88, 96

Скорость вывода при резервном копировании 181

Служба теневого копирования томов (VSS) 189

Служба теневого копирования томов (VSS) для виртуальных машин 190

Совместимость с программами шифрования 27

Создание MST-преобразования и извлечение пакетов установки 52

Создание динамической группы 116

Создание загрузочного носителя на базе WinPE или WinRE 292

Создание моментальных снимков LVM 176

Создание плана защиты 125

Создание статической группы 115

Создание физического загрузочного носителя 281

Сокращение журнала 176

Сохранить сведения о системе при сбое восстановления с перезагрузкой 214

Специальные операции с виртуальными машинами 249

Способ использования Зона безопасности 28

Способ резервного копирования кластера 170

Сравнение финализации и обычного восстановления 253

Статус защиты 302

Структура autostart.json 288

Схемы резервного копирования 144

Сценарии на загрузочных носителях 286

Сэкономить заряд батареи 154

Т

Тип элемента управления 289

Типичные правила установки 28

Точки подключения 177, 215

Требования 208, 220

Требования для виртуальных машин ESXi 225

Требования для виртуальных машин Hyper-V 225

Требования к контролю учетных записей пользователей (UAC) 76

Требования к программному обеспечению 17

Требования к сети для агента для Virtuozzo Hybrid Infrastructure (виртуальное устройство) 89

Требования к учетным записям пользователей 239

Требуемые права пользователя 229, 231

Требуемые роли 99

У

Удаление агента для VMware (виртуальное устройство) 105

Удаление агентов 104

Удаление машин с консоли службы 106

Удаление машины 252

Удаление резервных копий 221

Удаленное подключение 109

Указание параметров прокси-сервера в macOS 46

Указание параметров прокси-сервера в Windows 44

Управление обнаруженными машинами 78

Управление питанием BM 218

Управление средами виртуализации 260

Уровень сжатия 171

Условия 174

Условия запуска 150

Условия запуска задания 188

Условия поиска 116

Установка агента для Mac 64

Установка агентов 48

Установка или удаление продукта с указанием параметров вручную 53

Установка ограничения на общее количество виртуальных машин, для которых может создавать резервные копии агент для VMware (Windows) или агент для Hyper-V 267

Установка ограничения на общее количество виртуальных машин, резервные копии которых может создавать агент для VMware (виртуальное устройство) 268

Установка пакетов вручную 43

Установка пакетов из репозитория 42

Установка программного обеспечения 35

Установка продукта с использованием преобразования MST 52

Установлены ли необходимые пакеты? 41

Устранение неисправностей 79, 312

Ф

Файлы сценария 287

Физическая машина 193

Фильтры файлов 174

Финализация машин, запушенных из резервных копий в облаке 253

Финализация машины 252

Формат резервной копии 167

Формат резервной копии и файлы резервных копий 167

Формирование маркера регистрации 100

Функция Changed Block Tracking (CBT) 169

Х

Хост хранилища резервных копий доступен 152

Хранилище кэша 108

Ч

Что если... 33

Что еще нужно знать 158

Что необходимо для использования резервного копирования с поддержкой приложений? 228

Что содержится в резервных копиях томов или дисков 134

Что такое файл резервной копии? 164

Чтобы защитить виртуальную машину в центре обработки данных Red Hat Virtualization/oVirt 99

Ш

Шаг 1 38

Шаг 1. Формирование маркера регистрации 100

Шаг 2 38

Шаг 2. Создание MST-преобразования и извлечение пакета установки 101

Шаг 3 38

Шаг 3. Настройка объектов групповой политики 101

Шаг 4 38

Шаг 5 39

Шаг 6 40

Шифрование дисков Microsoft BitLocker 28

Э

Экспорт и импорт структуры отчета 310