Acronis

Acronis Backup 12.5

Update 2

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Содержание

1 Что нового в Acronis Backup

Важно! *Новые функции доступны* ***только в локальных развертываниях****. В будущих версиях планируется внедрить их также в облачные развертывания.*

1.1 Что нового в обновлении 2

Новые функции доступны во всех локальных развертываниях.

Администрирование

- Администрирование учетных записей пользователей доступно на сервере управления, который установлен в Linux (стр. 286)

Установка и инфраструктура

- Устройство Acronis Backup (стр. 35) для автоматического развертывания Linux, сервер управления, агент для Linux и Agent для VMware (Linux) на выделенной виртуальной машине
- При добавлении машины Windows в веб-интерфейсе можно выбрать имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления (стр. 36)
- Автоматическая и ручная проверка обновлений (стр. 53)

Безопасность

- Консоль резервного копирования поддерживает протокол HTTPS по умолчанию (стр. 62)
- Вместо самозаверяющего сертификата, сервер управления может использовать сертификат, выданный доверенным центром сертификации (стр. 69)
- Непривилегированные пользователи могут быть добавлены как администраторы на сервер управления, который установлен в Linux (стр. 288)

Планирование резервного копирования

- Новые параметры расписания (стр. 88):
  - Вывод машины из состояния сна или гибернации для выполнения резервного копирования
  - Отключение перехода в спящий режим или режим гибернации при выполнении резервного копирования
  - Данный параметр позволяет запретить выполнение отсутствующих резервных копий в настройке машины
- Новые условия запуска резервного копирования, удобные для резервного копирования ноутбуков и планшетных ПК Windows:
  - Сэкономить заряд батареи (стр. 95)
  - Не запускать при работе на лимитном подключении (стр. 96)
  - Не запускать при подключении к следующим сетям Wi-Fi (стр. 96)
  - Проверить IP-адрес устройства (стр. 97)
- В расписании **Ежемесячно** можно выбрать отдельные месяцы, в течение которых будут выполняться процессы резервного копирования
- Возможность вручную запустить дифференциальное резервное копирование (стр. 106)

Хранилища резервных копий

- Сохранение резервных копий каждой машины в папке, определенной сценарием (для машин под управлением Windows) (стр. 82)
- Локально развернутое хранилище Acronis Storage может использоваться как хранилище резервных копий (стр. 82)

Приложения

- Восстановление почтовых ящиков Microsoft Office 365 и элементов почтовых ящиков в Microsoft Exchange Server и наоборот (стр. 217)

Поддержка новых операционных систем и платформ виртуализации

- macOS High Sierra 10.13
- Debian 9.1 и 9.2
- Red Hat Enterprise Linux 7.4
- CentOS 7.4
- ALT Linux 7.0
- Red Hat Virtualization 4.1

Повышение удобства в использовании

- Переименование хранилищ на вкладке **Резервные копии** (за исключением хранилищ, которые управляются узлом хранения)
- Возможность изменить vCenter Server или ESXi, которые управляются агентом для VMware в **Настройки** > **Агенты** > подробная информация об агенте.

Новые функции доступны только при наличии расширенной лицензии

Администрирование

- Создание отделов доступно на сервере управления, который установлен в Linux (стр. 286)

Установка и инфраструктура

- При добавлении управляемого хранилища можно выбрать, будут ли агенты иметь доступ к узлу хранения по имени сервера или IP-адресу (стр. 277)

Повышение удобства в использовании

- Добавление управляемого хранилища можно инициировать с панели свойств узла хранения (стр. 277)

Поддержка пленки

- Полная поддержка технологии LTO-8. См. список совместимости оборудования, в котором указаны названия протестированных устройств.

1.2 Что нового в обновлении 1

- Поддержка Citrix XenServer 7.0, 7.1, 7.2 и Red Hat Virtualization 4.1 (стр. 21)
- Поддержка Debian 8.6, 8.7, 8.8, 9, и Ubuntu 17.04
- Поддержка Windows Storage Server 2016
- Возможность использовать базу данных PostgreSQL с сервером управления в Linux (стр. 34)
- Утилита для массового развертывания и обновления агентов.

  Информацию об использовании этой утилиты см. по ссылке http://kb.acronis.com/content/60137

1.3 Что нового в Acronis Backup 12.5

Новые функции доступны во всех локальных развертываниях.

Резервная копия

- Новый формат резервного копирования (стр. 113), увеличивающий скорость резервного копирования и уменьшающий размер резервных копий
- До пяти хранилищ для репликации в плане резервного копирования (стр. 104)
- Преобразование в виртуальную машину в плане резервного копирования (стр. 102)
- Планирование по событиям (стр. 90)
- Настройка условий для выполнения плана резервного копирования (стр. 92)
- Предопределенная схема резервного копирования «Дед-отец-сын» (GFS) (дублирование ежемесячно, еженедельно и ежедневно) (стр. 88)
- SFTP в качестве хранилища резервных копий (стр. 82)
- Хранение параметров резервного копирования по умолчанию на сервере управления (стр. 285)
- Выбор метода резервного копирования метод (полное или инкрементное) при запуске резервного копирования вручную (стр. 106)
- Параметры резервного копирования:
  - Уведомление по электронной почте (стр. 117):
    - Укажите тему письма с уведомлением
    - Уведомления теперь основаны на оповещениях, а не на результатах активности резервного копирования. Доступна настройка списка оповещений, по которым будет отправляться уведомление.
  - Имя файла резервной копии (стр. 110)
  - Условия запуска резервного копирования (стр. 115)

Восстановление

- Сопоставление диска вручную. Возможность выбирать отдельные диски или тома для восстановления (стр. 136).

Загрузочный носитель

- Startup Recovery Manager (стр. 187)

Приложения

- Резервное копирование почтовых ящиков Microsoft Exchange Server (стр. 204)

Виртуализация

- Возможность назначать виртуальной машины указанному агенту (стр. 239) (привязка виртуальной машины)

Операции с резервными копиями

- Подключение томов в режиме чтения/записи (стр. 159)
- ASign позволяет нескольким людям подписывать файлы в резервной копии (стр. 147)

Уведомления и оповещения

- Возможность настраивать серьезность сообщения (в файле конфигурации) (стр. 250)

- Статус устройства теперь берется из оповещений, а не из результатов активности резервного копирования. Это относится к разнообразным событиям, например, отсутствию резервных копий или вредоносной активности.

Активная защита Acronis

- Проактивная защита от вредоносных программ выявляет подозрительные процессы (стр. 221)

Повышение удобства в использовании

- Панель мониторинга — настраиваемый набор более чем 20 виджетов, отображающих информацию в реальном времени (стр. 247)
- Новый раздел пользовательского интерфейса для отображения всех планов резервного копирования и прочих планов (стр. 161)
- Возможность настраивать зашифрованный пароль в Backup Monitor (стр. 99)

Новые функции доступны только при наличии расширенной лицензии

Администрирование

- Настраиваемые отчеты, которые можно пересылать или сохранять по расписанию (стр. 248)
- Распределение ролей на сервере управления: создание элементов и назначение им администраторов (стр. 286)
- Управление группами: встроенные и задаваемые пользователем группы устройств (стр. 251)
- Acronis Нотаризация: подтверждение целостности файла и отсутствия изменений в нем с момента резервного копирования (стр. 101)

Новые хранилища резервных копий

- Узел хранения Acronis с дедупликацией (стр. 276)
- Поддержка ленточных устройств (стр. 257)

Загрузочный носитель

- Работа с загрузочным носителем из консоли резервного копирования (стр. 184)
- Автоматизация резервного копирования и восстановления посредством выполнения предопределенного или заданного пользователем сценария (стр. 171)
- PXE-сервер для загрузки через сеть (стр. 188)

Приложения

- Поддержка групп обеспечения доступности баз данных (DAG) в Microsoft Exchange Server (стр. 201)
- Поддержка AlwaysOn Availability Group (AAG) в Microsoft SQL Server (стр. 199)
- Защита Oracle Database (стр. 221)

Виртуализация

- Резервное копирование виртуальных машин ESXi с моментальных снимков оборудования NetApp (стр. 234)
- Резервное копирование Citrix XenServer, Red Hat Virtualization (RHV/RHEV), виртуальных машин на основе ядра (KVM) и виртуальных машин Oracle (путем установки агента в гостевую систему) (стр. 14)

Операции с резервными копиями

- Преобразование в виртуальную машину, проверка, репликация и удержание резервных копий может выполняться выделенным агентом по расписанию (стр. 162)
- Каталогизация — отдельная служба каталогов дает возможность поиска по всем резервным копиям в управляемых хранилищах (стр. 281)

2 Установка

2.1 Обзор установки

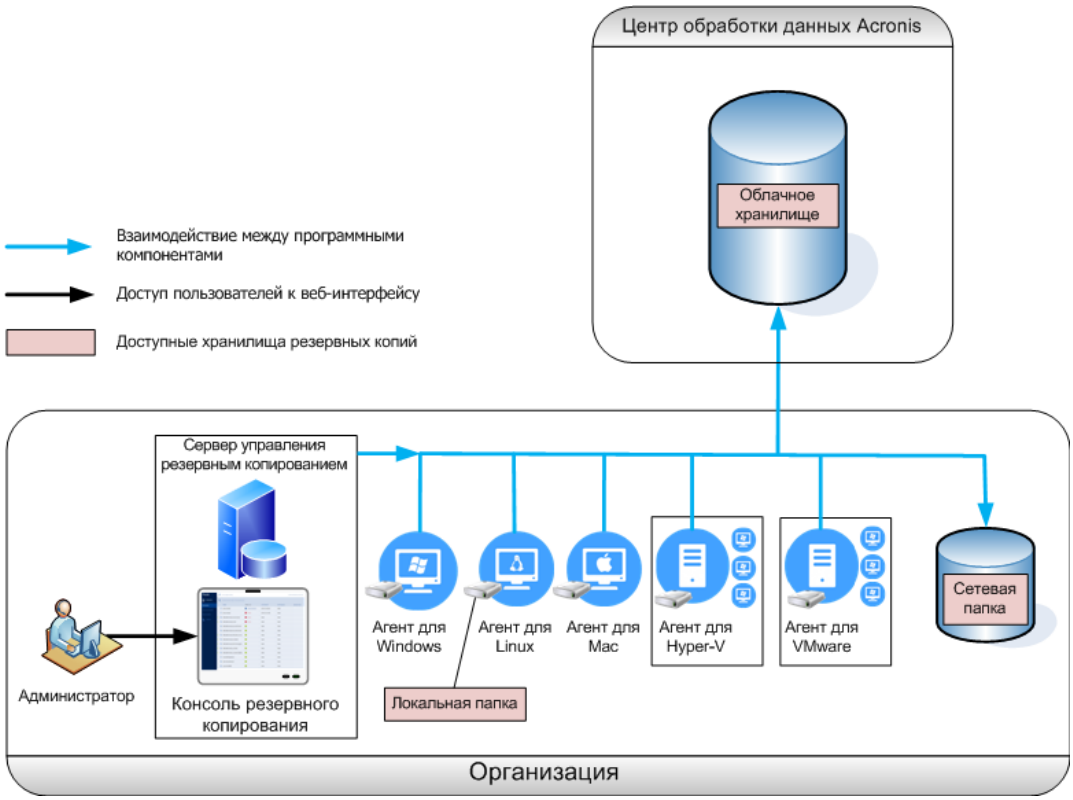
Acronis Backup поддерживает два способа развертывания: в локальной среде и в облаке. Основное различие между ними заключается в месте размещения сервера управления Acronis Backup.

Сервер управления Acronis Backup — это центр управления всеми резервными копиями. При локальном развертывании он устанавливается в локальной сети, а при облачном — в одном из центров обработки данных Acronis. Веб-интерфейс этого сервера называется консолью резервного копирования.

При обоих типах развертывания необходимо установить агент резервного копирования на каждой машине, резервное копирование которой требуется выполнять. Поддерживаемые типы хранилищ также одинаковы. Пространство в облачном хранилище данных продается отдельно от лицензий Acronis Backup.

Локальное развертывание

Локальное развертывание подразумевает установку всех компонентов решения в локальной сети. Это единственный способ развертывания, доступный по бессрочной лицензии. Кроме того, этот способ необходимо использовать, если машины не подключены к Интернету.



Расположение сервера управления

Сервер управления можно установить на машине с ОС Windows или Linux.

Рекомендуется установка в Windows, так как это позволит развертывать агенты с сервера управления на других машинах. Лицензия Advanced позволяет создавать организационные единицы и добавлять администраторов для них. Таким образом, можно делегировать управление резервным копированием другим пользователям, разрешения на доступ для которых явным образом ограничены соответствующими отделами.

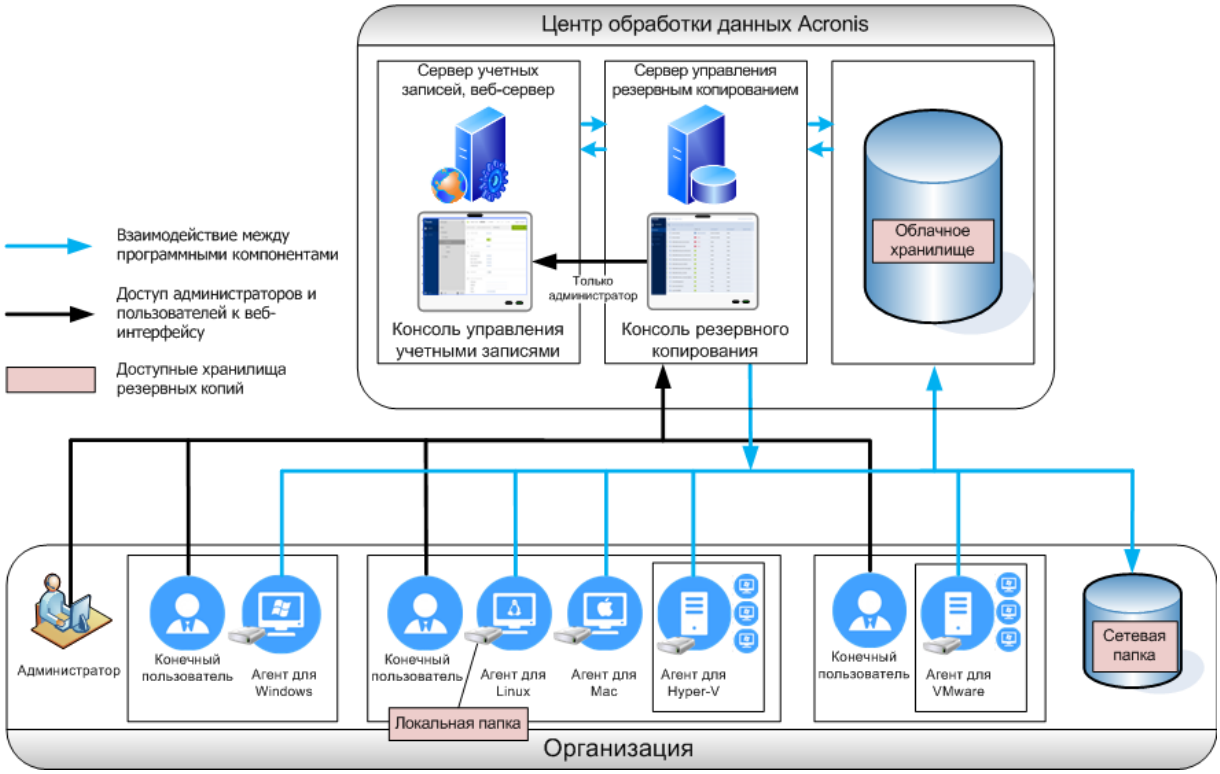
Установка в Linux рекомендуется в средах на основе исключительно систем Linux. Агент потребуется установить локально на машинах, резервное копирование которых необходимо выполнять.

Облачное развертывание

Облачное развертывание означает, что сервер управления находится в одном из центров обработки данных Acronis. Преимущество этого подхода состоит в том, что не нужно обслуживать сервер управления в локальной сети. Acronis Backup можно представить как сервис резервного копирования, предоставляемый Acronis.

Благодаря доступу к серверу учетных записей можно создавать учетные записи пользователей, устанавливать для них квоты использования сервиса и создавать группы пользователей (отделов), отражающие структуру организации. Каждый пользователь может открыть консоль резервного копирования, загрузить требуемый агент и установить его на свои машины за несколько минут.

Учетные записи администраторов можно создавать на уровне отделов или организации. У каждой учетной записи есть подконтрольная ей область. Пользователи имеют доступ только к собственным резервным копиям.



В приведенной ниже таблице показаны различия между локальным и облачным развертываниями.

Локальное развертывание	Облачное развертывание
▪ Локальный сервер управления ▪ Управление отделами и учетными записями только с помощью лицензии Advanced ▪ Можно использовать как подписки, так и бессрочные лицензии ▪ Агент для VMware (виртуальное устройство) и агент для VMware (Windows) ▪ Оптимизация глобальной сети для репликации виртуальных машин (сохранение реплик) ▪ Мастер создания загрузочных носителей ▪ Резервное копирование и управление дисками на загрузочном носителе ▪ Переход с предыдущих версий решений Acronis Backup, включая Acronis Backup для VMware ▪ Участие в программе улучшения качества Acronis ▪ Функции, представленные в версии 12.5, которые влияют только локальное развертывание. См. тему «Что нового в Acronis Backup» (стр. 7).	▪ Управление отделами и учетными записями ▪ Требуется лицензия по подписке ▪ Агент для VMware (виртуальное устройство) отсутствует ▪ Резервное копирование мобильных данных в облаке

2.2 Компоненты

Агенты

Агенты — это приложения, выполняющие резервное копирование данных, их восстановление и другие операции на машинах под управлением Acronis Backup.

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

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

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?	Доступность агента	
			Локально	В облаке
Физические машины				
Диски, тома и файлы на физических машинах под управлением Windows	Агент для Windows	На машину, резервная копия которой будет создана.	+	+
Диски, тома и файлы на физических машинах под управлением Linux	Агент для Linux		+	+
Диски, тома и файлы на физических машинах под управлением macOS	Агент для Mac		+	+
Приложения				
Базы данных SQL	Агент для SQL	На машину с сервером Microsoft SQL Server.	+	+
Базы данных и почтовые ящики Exchange	Агент для Exchange	На машину с ролью почтового ящика Microsoft Exchange Server. Если требуется резервное копирование только почтового ящика, агент может быть установлен а любой машине с ОС Windows, которая имеет сетевой доступ к машине, на которой включена роль клиентского доступа Microsoft Exchange Server.	+	+ Резервное копирование почтовых ящиков не выполняется
Почтовые ящики Microsoft Office 365	Агент для Office 365	На машину с Windows, которая подключена к Интернету.	+	+
Машины с доменными службами Active Directory	Агент для Active Directory	На контроллер домена.	+	+

Для каких объектов нужно создать резервные копии?	Какой агент следует установить?	Куда его следует установить?	Доступность агента	
			Локально	В облаке
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 машину под управлением 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 в среде Windows Azure	То же самое, что и для физических машин**	На машину, резервная копия которой будет создана.	+	+
Виртуальные машины, размещенные в Amazon EC2			+	+
Виртуальные машины на хосте Citrix XenServer			+***	+
Виртуальные машины Red Hat Virtualization (RHV/RHEV)				
Виртуальные машины на основе ядра (KVM)				
Виртуальные машины Oracle				
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		–	+

*Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Подробные инструкции см. в разделе «Резервное копирование без использования локальной сети» (стр. 231).

**Виртуальная машина считается виртуальной, если ее резервную копию создает внешний агент. 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 в облачном развертывании.

***При наличии лицензии Advanced Virtual Host для Acronis Backup эти виртуальные машины считаются виртуальными (используется лицензия для каждого хоста). При наличии лицензии Virtual Host для Acronis Backup эти виртуальные машины считаются физическими (используется лицензия для каждого хоста).

Другие компоненты

Компонент	Функция	Куда его следует установить?	Доступность	
			Локально	Облако
Сервер управления	Управляет агентами. Предоставляет пользователям веб-интерфейс.	На машине с ОС Windows или Linux.	+	–
Компоненты для удаленной установки	Сохраняет пакеты установки агента в локальную папку.	На машине Windows с сервером управления.	+	–
Служба мониторинга	Предоставляет функции панели мониторинга и составления отчетов.	На машине, где работает сервер управления.	+	–
Мастер создания загрузочных носителей	Создает загрузочный носитель.	На машине с ОС Windows или Linux.	+	–
Программа командной строки	Предоставляет интерфейс командной строки.	На машине с ОС Windows или Linux.	+	+
Монитор резервного копирования	Позволяет пользователям отслеживать резервные копии вне веб-интерфейса.	На машине с ОС Windows или macOS.	+	+
Узел хранения	Хранение резервных копий. Требуется для каталогизация и дедупликации.	На машине под управлением ОС Windows.	+	–
Служба каталога	Выполняет каталогизации резервных копий на узлах хранения.	На машине под управлением ОС Windows.	+	–
PXE-сервер	Активирует загрузку машин на загрузочный носитель по сети.	На машине под управлением ОС Windows.	+	–

2.3 Требования к программному обеспечению

2.3.1 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 10 или более поздней версии
- Microsoft Edge 25 более поздней версии
- Safari 8 или более поздней версии в операционных системах OS X и iOS

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

2.3.2 Поддерживаемые операционные системы и среды

2.3.2.1 Агенты

Агент для Windows

Windows XP Professional с пакетом обновления 3 (SP3) (x86, x64)

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 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 2003/2008/2008 R2/2012/2012 R2/2016

Windows 10 — выпуски Home, Pro, Education, Enterprise, и IoT Enterprise

Windows Server 2016 — все варианты установки, кроме Nano Server

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

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

Агент для Exchange (для резервного копирования почтового ящика)

Этот агент можно установить на машине с или без Microsoft Exchange Server.

Windows Server 2008 — выпуски Standard, Enterprise, Datacenter 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

Агент для Office 365

Windows Server 2008 — выпуски Standard, Enterprise, Datacenter и Web (только x64)

Windows Small Business Server 2008

Windows Server 2008 R2 — выпуски Standard, Enterprise, Datacenter, Foundation и Web

Windows Small Business Server 2011 — все выпуски

Windows 8/8.1 — все выпуски (только x64), кроме выпусков Windows RT

Windows Server 2012/2012 R2 — все выпуски

Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (только x64)

Windows 10 — выпуски Home, Pro, Education и Enterprise (только x64)

Windows Server 2016 — все варианты установки (только x64), кроме Nano Server

Агент для Oracle

Windows Server 2008 — выпуски Standard, Enterprise, Datacenter и Web (x86, x64)

Windows Server 2012 — выпуски Standard, Enterprise, Datacenter и Web (x86, x64)

Агент для Linux

Linux с версией ядра от 2.6.9 до 4.9 и glibc версии 2.3.4 или более поздней

Различные дистрибутивы Linux x86 и x86_64, включая:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4
- 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
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
- 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, 9.0, 9.1, 9.2
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1

ClearOS 5.x, 6.x, 7, 7.1

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 суперпользователя: **`apt-get install rpm`**

Агент для Mac

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

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 и 6.5

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.

Агент для Hyper-V

Windows Server 2008 (только 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 (только x64) с Hyper-V

Windows 10 — выпуски Pro, Education и Enterprise с Hyper-V

Windows Server 2016 с Hyper-V — все варианты установки, кроме Nano Server

Microsoft Hyper-V Server 2016

2.3.2.2 Сервер управления (только в локальных развертываниях)

В Windows

Windows Server 2008 — выпуски Standard, Enterprise и Datacenter (x86, x64)

Windows Small Business Server 2008

Windows 7 — все выпуски (x86, x64)

Windows Server 2008 R2 — выпуски Standard, Enterprise, Datacenter и Foundation

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 R2/2016

Windows 10 — выпуски Home, Pro, Education, Enterprise, и IoT Enterprise

Windows Server 2016 — все варианты установки, кроме Nano Server

В ОС Linux

Linux с версией ядра от 2.6.18 до 4.9 и glibc версии 2.3.4 или более поздней

Различные дистрибутивы Linux x86_64, включая:

Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3, 7.4

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

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24

SUSE Linux Enterprise Server 10, 11, 12

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, 9.0, 9.1, 9.2

CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3, 7.4

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3 — Unbreakable Enterprise Kernel и Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7, 7.1

ALT Linux 7.0

2.3.2.3 Узел хранения (только в локальных развертываниях)

Windows Server 2008 — выпуски Standard, Enterprise и Datacenter (только x64)

Windows Small Business Server 2008

Windows 7, все версии (только x64)

Windows Server 2008 R2 — выпуски Standard, Enterprise, Datacenter и Foundation

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 — все выпуски

Windows 8/8.1 — все выпуски (только x64), кроме выпусков Windows RT

Windows Server 2012/2012 R2 — все выпуски

Windows Storage Server 2008/2008 R2/2012/2012 R2/2016

Windows 10 — выпуски Home, Pro, Education и Enterprise

Windows Server 2016 — все варианты установки, кроме Nano Server

2.3.3 Поддерживаемые версии Microsoft SQL Server

- 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

2.3.4 Поддерживаемые версии Microsoft Exchange Server

- **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.

2.3.5 Поддерживаемые версии Microsoft SharePoint

Acronis Backup 12.5 поддерживает следующие версии Microsoft SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

* Чтобы использовать SharePoint Explorer с этими версиями, необходима ферма восстановления SharePoint для прикрепления баз данных.

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

2.3.6 Поддерживаемые версии Oracle Database

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

Поддерживаются только конфигурации с одним экземпляром.

2.3.7 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		

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
Версии VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5 **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	+	+
Microsoft Virtual PC 2004 и 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2		Только полностью виртуализированные (известные также как HVM) гостевые системы

Платформа	Резервное копирование на уровне гипервизора (резервное копирование без агента)	Резервное копирование изнутри гостевой ОС
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		+
Виртуальные машины на основе ядра (KVM)		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0 и 3.3		+
Oracle VM VirtualBox 4.x		+
Amazon		
Экземпляры Amazon EC2		+
Microsoft Azure		
Виртуальные машины Azure		+

* 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.

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 независимые диски и RDM-диски в режиме физической совместимости из плана резервного копирования. 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 диски прямого доступа из плана резервного копирования. Если необходимо выполнить резервное копирование этих дисков или данных на этих дисках, установите агент в гостевой операционной системе.

- **Зашифрованные виртуальные машины** (эта функциональная возможность представлена в VMware vSphere 6.5)
  - Резервное копирование зашифрованных виртуальных машин выполняется в незашифрованном состоянии. Если шифрования является критически важным, включите шифрование резервных копий при создании плана резервного копирования (стр. 99).
  - 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** (эта функциональная возможность представлена в VMware vSphere 6.5)

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

2.3.8 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.

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.

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 в том, что команда возвращает ту же версию, что и в параметре **gcc version** 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.

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**	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**	Программа установки загрузит и установит пакеты автоматически.
	perl	Выполните следующую команду: `yum install perl`
Ubuntu	**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`

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.

Установка пакетов вручную

Установка пакетов **вручную** может потребоваться в следующих случаях:

- У машины нет активной подписки на Red Hat или подключения к Интернету.
- Программа установки не может найти версию **kernel-devel** и **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 PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```

- В Ubuntu выполните следующую команду:

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

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 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.

2.3.9 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 ее доступа к разделу 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.

Типичные правила установки

Настоятельно рекомендуется установить программу шифрования перед установкой агентов резервного копирования.

Способ использования раздела Зона безопасности

Раздел Зона безопасности не должен быть зашифрована на уровне дисков. Это единственный способ использования раздела Зона безопасности:

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

Общее правило резервного копирования

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

Процедуры восстановления для конкретных программ

Шифрование дисков Microsoft BitLocker

Как восстановить систему, зашифрованную функцией BitLocker

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

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

McAfee Endpoint Encryption и PGP Whole Disk Encryption

Можно восстановить шифрованный системный раздел, используя только загрузочный носитель.

Если восстановленную систему не удастся загрузить, восстановите основную загрузочную запись, как описано в статье базы знаний Майкрософт по ссылке https://support.microsoft.com/kb/2622803

2.4 Требования к системе

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

Устанавливаемые компоненты	Занятое пространство	Минимальный используемый объем памяти
Агент для Windows	850 МБ	150 МБ
Агент для Windows и один из следующих агентов: ▪ Агент для SQL ▪ Агент для Exchange	950 МБ	170 МБ
Агент для Windows и один из следующих агентов: ▪ Агент для VMware (Windows) ▪ Агент для Hyper-V	1170 МБ	180 МБ
Агент для Office 365	500 МБ	170 МБ
Агент для Linux	720 МБ	130 МБ
Агент для Mac	500 МБ	150 МБ
Только для локальных развертываний		
Сервер управления в Windows	1,7 ГБ	200 МБ
Сервер управления в Linux	0,6 ГБ	200 МБ
Сервер управления и агент для Windows	2,4 ГБ	360 МБ
Сервер управления и агенты на машине с ОС Windows, Microsoft SQL Server, Microsoft Exchange Server и доменными службами Active Directory	3,35 ГБ	400 МБ
Сервер управления и агент для Linux	1,2 ГБ	340 МБ
Узел хранения и агент для Windows ▪ только 64-разрядная платформа ▪ Для использования функции дедупликации требуется минимум 8 ГБ ОЗУ. Дополнительные сведения см. в разделе «Рекомендации по дедупликации» (стр. 279).	1,1 ГБ	330 МБ

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

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

Сервер управления с одной зарегистрированной машиной занимает 200 МБ памяти. При регистрации каждой дополнительной машины используется еще 4 МБ. Таким образом, сервер со 100 зарегистрированными машинами занимает примерно 600 МБ, помимо операционной системы и запущенных приложений. Максимальное число зарегистрированных машин составляет 900–1000. Это ограничение налагается встроенной в сервер управления базой данных SQLite.

Обойти это ограничение можно, указав внешний экземпляр Microsoft SQL Server во время установки сервера управления. С помощью внешней базы данных SQL можно зарегистрировать до 2000 машин без значительного снижения производительности.

2.5 Поддерживаемые файловые системы

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

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

<table>
<tr><th rowspan="2">Файловая система</th><th colspan="4">Поддержка</th><th rowspan="2">Ограничения</th></tr>
<tr><th>Агенты</th><th>Загрузочный носитель Win-PE</th><th>Загрузочные носители на основе Linux</th><th>Загрузочные носители Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Все агенты</td><td>+</td><td>+</td><td>+</td><td rowspan="4">Без ограничений</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>+</td><td>–</td></tr>
<tr><td>HFS+</td><td rowspan="2">Агент для Mac</td><td>-</td><td>–</td><td>+</td></tr>
<tr><td>APFS</td><td>–</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="3">Агент для Linux</td><td>-</td><td>+</td><td>-</td><td rowspan="2">Файлы невозможно исключить из резервной копии диска</td></tr>
<tr><td>ReiserFS3</td><td>-</td><td>+</td><td>-</td></tr>
<tr><td>ReiserFS4</td><td>-</td><td>+</td><td>-</td><td rowspan="2">▪ Файлы невозможно исключить из резервной копии диска</td></tr>
<tr><td>ReFS</td><td>Все агенты</td><td>+</td><td>+</td><td>+</td></tr>
</table>

Файловая система	Поддержка				Ограничения
	Агенты	Загрузочный носитель Win-PE	Загрузочные носители на основе Linux	Загрузочные носители Mac	
XFS		+	+	+	▪ Невозможно изменить размер томов при выполнении восстановления
Linux SWAP	Агент для Linux	-	+	-	Без ограничений

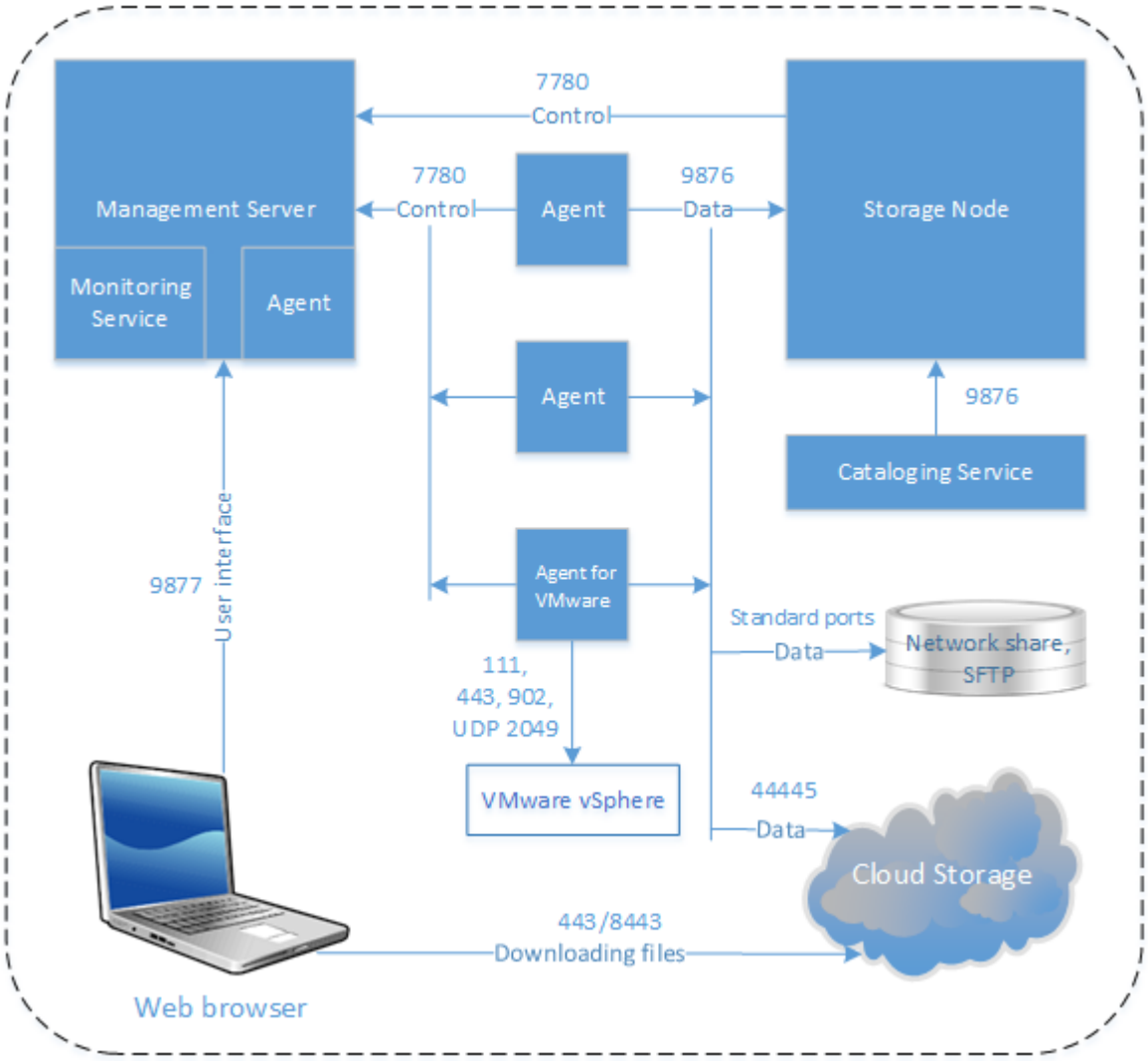
Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами. Посекторное резервное копирование возможно для любой файловой системы, которая:

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

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

2.6 Локальное развертывание

Локальное развертывание включает в себя ряд программных компонентов, которые описаны в разделе «Компоненты» (стр. 14). На указанной ниже диаграмме показано взаимодействие компонентов и портов, которые требуются для этого взаимодействия. Стрелки направлены от тех компонентов, которые инициируют подключение.



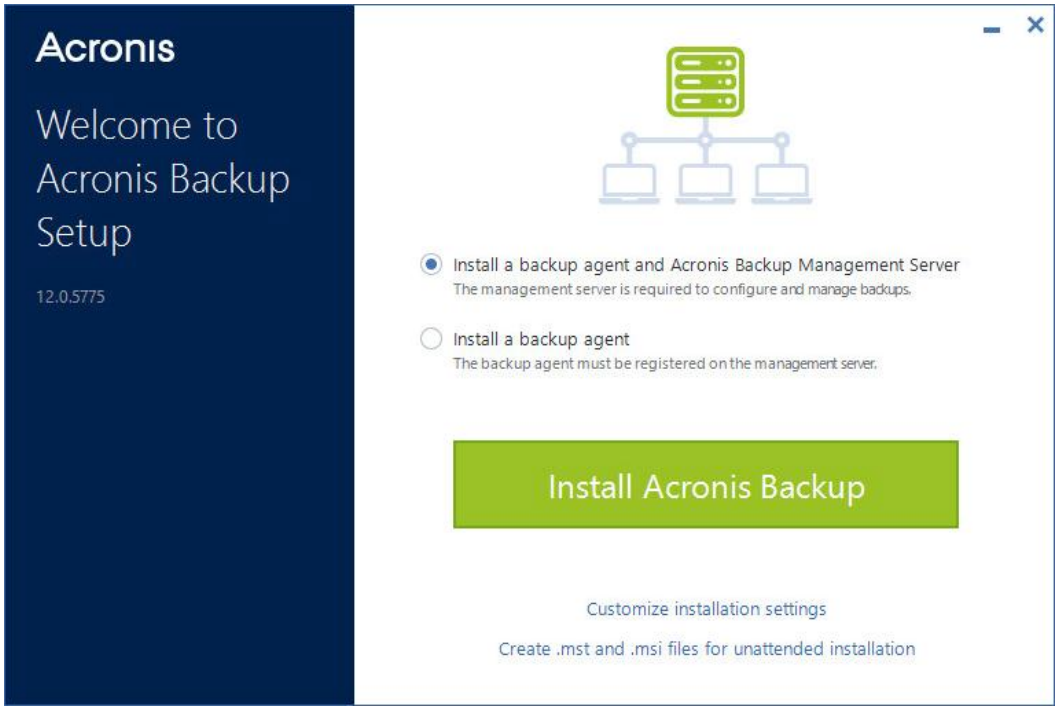
2.6.1 Установка сервера управления

2.6.1.1 Установка в ОС Windows

Установка сервера управления

1. Войдите как администратор и запустите программу установки Acronis Backup Advanced.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Установка языка**.
3. Примите условия лицензионного соглашения и укажите, будет ли машина участвовать в программе улучшения качества Acronis Customer Experience Program (CEP).

4. Оставьте настройку по умолчанию **Установить агент резервного копирования и сервер управления Acronis Backup**.



5. Выполните любое из следующих действий:
   - Выберите пункт **Установить Acronis Backup**.

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

     По умолчанию устанавливаются следующие компоненты:
     - Management Server
     - Компоненты для удаленной установки
     - Служба мониторинга
     - Агент для Windows
     - Другие агенты (агент для Hyper-V, агент для Exchange, агент для SQL и агент для Active Directory), если на машине обнаружен соответствующий гипервизор или приложение
     - Мастер создания загрузочных носителей
     - Программа командной строки
     - Монитор резервного копирования
   - Щелкните **Настройка параметров установки**, чтобы настроить программу установки.

     Можно будет выбрать компоненты для установки и указать дополнительные параметры. Дополнительную информацию см. в разделе «Настройка параметров установки» (стр. 33).
   - Щелкните **Создать MST- и MSI-файлы для автоматической установки**, чтобы извлечь пакеты установки. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **Создать**. Для этой процедуры не требуется никаких дополнительных шагов.

     Чтобы развернуть агенты через групповую политику, см. раздел «Развертывание агентов с использованием групповой политики» (стр. 59).
6. Приступите к установке.

7. После завершения установки нажмите кнопку **Закрыть**.

Настройка параметров установки

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

Общие параметры

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

  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** (по умолчанию для службы сервера управления и службы узла хранения)

    Учетные записи будут иметь имена **Acronis Agent User**, **AMS User** и **ASN User** для агента, сервера управления и служб узла хранения соответственно.
  - **Использовать следующую учетную запись**

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

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

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

Установка сервера управления

- База данных, которая должна использоваться сервером управления.

  По умолчанию используется встроенная база данных SQLite. Можно выбрать любую версию Microsoft SQL Server 2012, Microsoft SQL Server 2014 или Microsoft SQL Server 2016. Выбранный экземпляр может использоваться и другими программами.

  Перед выбором установленного на другой машине экземпляра убедитесь, что на этой машине включены служба обозревателя SQL Server и протокол TCP/IP. Инструкции по запуску службы обозревателя SQL Server см. на странице http://msdn.microsoft.com/en-us/library/ms189093.aspx. Включить протокол TCP/IP можно с помощью аналогичной процедуры.
- Порт, который будет использоваться веб-браузером для доступа к серверу управления (по умолчанию 9877) и порт, который будет использоваться для связи между компонентами продукта (по умолчанию 7780). Изменение последнего порта после установки потребует перерегистрации всех компонентов.

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

- Будут ли агенты и другие компоненты осуществлять доступ к серверу управления, используя его имя хоста или IP-адрес.

  По умолчанию указано имя хоста. Возможно, нужно будет изменить этот параметр, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации компонента.

Установка агента

- Этот параметр определяет, будет ли агент подключаться к Интернету через прокси-сервер HTTP при резервном копировании в облачное хранилище данных и восстановлении из него.

  Если необходимо указать прокси-сервер, укажите его имя хоста или IP-адрес и номер порта.

2.6.1.2 Установка в ОС Linux

Подготовка

1. Перед установкой продукта на системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например запустив следующую команду в качестве привилегированного пользователя: **`apt-get install rpm`**.
2. Если требуется установить агент для Linux вместе с сервером управления, убедитесь в том, что на машине установлены необходимые пакеты Linux (стр. 24).
3. Выберите базу данных, которая должна использоваться сервером управления.

   По умолчанию используется встроенная база данных SQLite. В качестве альтернативного варианта можно использовать PostgreSQL. Информацию о настройке сервера управления для использования PostgreSQL см. по ссылке http://kb.acronis.com/content/60395.

   Примечание. *Если переход к использованию PostgreSQL выполняется после того, как север управления уже работал определенное время, необходимо будет с нуля добавить устройства, настроить планы резервного копирования и задать другие настройки.*

Установка

Установка сервера управления

1. Запустите файл установки от имени суперпользователя.
2. Примите условия лицензионного соглашения.
3. [Необязательно] Выберите компоненты, которые требуется установить.

   По умолчанию устанавливаются следующие компоненты:

   - Сервер управления
   - Агент для Linux
   - Мастер создания загрузочных носителей
4. Укажите порт, который будет использоваться в веб-браузере для доступа к серверу управления. Значение по умолчанию составляет 9877.
5. Укажите порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию установлено значение 7780.
6. Нажмите кнопку **Далее**, чтобы продолжить установку.

7. По окончании установки выберите **Открыть веб-консоль**, затем нажмите кнопку **Выход**. Консоль резервного копирования откроется в веб-браузере по умолчанию.

2.6.1.3 Устройство Acronis Backup

Используя устройство Acronis Backup, можно легко получить виртуальную машину с указанным ниже программным обеспечением:

- CentOS
- Компоненты Acronis Backup:
  - Management Server
  - Агент для Linux
  - Агент для VMware (Linux)

Устройство комплекс предоставляется в виде ZIP-архива. Архив содержит файлы OVF и ISO. Можно развернуть файл OVF на хосте ESXi или использовать файл ISO для загрузки существующей виртуальной машины. В архиве также есть файл VMDK, который необходимо поместить в один каталог с файлом OVF.

Примечание *VMware Host Client (веб-клиент, который используется для управления автономным ESXi 6.0+) не разрешает развертывание шаблонов OVF с образом ISO внутри. В таком случае создайте виртуальную машину, которая соответствует указанным ниже системным требованиям и используйте файл ISO для установки программного обеспечения.*

Минимальные системные требования для виртуального устройства приведены ниже.

- 2 ЦП
- 4 ГБ ОЗУ
- Один виртуальный диск 10 ГБ (рекомендуется 40 ГБ)

Установка программного обеспечения

1. Выполните одно из следующих действий:
   - Развертывание устройства из шаблона OVF, как описано в теме «Развертывание агента для VMware (виртуальное устройство) из шаблона OVF» (стр. 45) раздела «Развертывание шаблона OVF». По окончании развертывания включите развернутую машину.
   - Загрузите существующую виртуальную машину с файла ISO.
2. Выберите **Установить или обновить Acronis Backup** и нажмите кнопку **ВВОД**. Дождитесь появления начального окна настройки.
3. [Необязательно] Чтобы изменить настройки установки, выберите **Изменить настройки** и нажмите клавишу **ВВОД**. Можно указать следующие настройки:
   - Имя хоста устройства (по умолчанию **AcronisAppliance-**<случайная часть>).
   - Пароль для пользователя «root», который будет использоваться для входа на консоль резервного копирования (по умолчанию, **не указан**).

     Если оставить значение по умолчанию, после установки Acronis Backup поступит запрос указать пароль. Без этого пароля у вас не будет возможности войти в консоль резервного копирования и веб-консоль Cockpit.
   - Настройки сети сетевого адаптера:
     - **Использвоать DHCP** (по умолчанию)
     - **Задать статический IP-адрес**

Если в машине несколько сетевых адаптеров программное обеспечение выберет один из них случайно и применит к нему эти настройки.

4. Выберите **Установить текущие настройки**.

В результате CentOS и Acronis Backup будут установлены на машине.

Дальнейшие действия

По окончании установки программное обеспечение покажет ссылки на консоль резервного копирования и веб-консоль Cockpit. Подключитесь к консоли резервного копирования, чтобы начать использовать Acronis Backup: добавляйте больше устройств, создавайте планы резервного копирования и т. д.

Чтобы добавить виртуальные машины ESXi, щелкните **Добавить** > **VMware ESXi**, затем укажите адрес и учетные данные для vCenter Server или автономного хоста ESXi.

Нет настроек Acronis Backup, настроенных в веб-консоли Cockpit. Консоль предоставлена для удобства и поиска и устранения неисправностей.

Обновление программного обеспечения

1. Загрузка и распаковка ZIP-архива с новой версией устройства.
2. Загрузите машину с нераспакованным образом ISO в предыдущем шаге.
3. Выберите **Установить или обновить Acronis Backup** и нажмите кнопку **ВВОД**.
4. Выберите **Обновить** и нажмите кнопку **ВВОД**.

В результате Acronis Backup будет обновлено. Если CentOS в образе ISO имеет версию более позднюю, чем версия на диске, операционная система будет обновлена после обновления Acronis Backup.

2.6.2 Добавление машин через веб-интерфейс

Чтобы начать добавлять машины на сервер управления, последовательно выберите пункты **Все устройства** > **Добавить**.

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

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

2.6.2.1 Добавление машины с ОС Windows

Подготовка

1. Для успешной установки на удаленной машине под управлением ОС Windows XP параметр **Панель управления > Свойства папки > Вид> Использовать простой общий доступ к файлам** должен быть *отключен* на этой машине.

   Для успешной установки на удаленной машине под управлением ОС Windows Vista или более поздней версии параметр **Панель управления > Свойства папки > Вид > Использовать мастер общего доступа** должен быть *отключен* на этой машине.
2. Для успешной установки на удаленной машине, *не* входящей в домен Active Directory, контроль учетных записей (UAC) должен быть *отключен* (стр. 38).

3. Общий доступ к файлам и принтерам на удаленной машине должен быть *включен*. Получение доступа к этому параметру
   - На машине под управлением Windows XP с пакетом обновления 2 (SP2) или 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**.
4. Acronis Backup использует TCP-порты 445, 25001 и 9876 для удаленной установки.

   Порт 445 открывается автоматически при выборе параметра «Общий доступ к файлам и принтерам». С брандмауэром Windows порты 9876 и 25001 открываются 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 9876 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.

Пакеты установки

Агенты устанавливаются из пакетов установки. Сервер управления берет пакеты установки из локальной папки, указанной в следующем разделе реестра: **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\RemoteInstallationFiles**<номер сборки продукта>. Хранилище по умолчанию: **%ProgramFiles%\Acronis\RemoteInstallationFiles**<номер сборки продукта>.

Вам может потребоваться загрузить пакет установки с следующих ситуациях:

- Компоненты для удаленной установки не были установлены при установке сервера управления.
- Пакеты установки вручную удалены из расположения, указанного в разделе реестра.
- Необходимо добавить 32-разрядную машину на 64-разрядный сервер управления или наоборот.
- На вкладке **Агенты** необходимо обновить агенты на 32-разрядной машине с 64-разрядного сервера управления или наоборот.

Порядок получения пакетов установки

1. На консоли резервного копирования щелкните значок учетной записи в правом верхнем углу и выберите > **Загрузки**.
2. Выберите **Автономный установщик для Windows**. Обратите внимание на требуемую разрядность: 32 бита или 64 бита.
3. Сохраните установщик в папку для пакетов.

Добавление машины

1. Щелкните **Все устройства** > **Добавить**.
2. Щелкните **Windows** или кнопку, соответствующую приложению, которое необходимо защитить. В зависимости от того, какая кнопка нажата, будет выбран один из следующих вариантов:
   - Агент для Windows

- Агент для Hyper-V
- Агент для SQL + агент для Windows
- Агент для Exchange + агент для Windows

  Если при наличии хотя бы одного зарегистрированного агента для Exchange щелкнуть **Microsoft Exchange Server** > **Почтовые ящики Exchange**, будет выполнен переход непосредственно к шагу 5.
- Агент для Active Directory + агент для Windows
- Агент для Office 365

3. Укажите имя хоста или IP-адрес машины и данные учетной записи с правами администратора на этой машине.
4. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
5. Нажмите кнопку **Добавить**.
6. Если на шаге 2 вы выбрали **Microsoft Exchange Server** > **Почтовые ящики Exchange**, укажите машину, на которой включена роль сервера **Client Access** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе «Резервное копирование почтовых ящиков» (стр. 204).

Требования к контролю учетных записей пользователей (UAC)

На машине с ОС Windows Vista или более поздней версии, которая не является членом домена Active Directory, для операций централизованного управления (включая удаленную установку) необходимо, чтобы контроль учетных записей пользователей (UAC) был отключен.

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: Мелкие значки > Учетные записи пользователей > Изменение параметров контроля учетных записей** и передвиньте бегунок на **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.

2.6.2.2 Добавление машины с ОС Linux

1. Выберите **Все устройства** > **Добавить**.
2. Выберите пункт **Linux**. Будет загружен файл установки.
3. На машине, которую нужно защитить, запустите программу установки локально (стр. 44).

2.6.2.3 Добавление машины с ОС OS X

1. Выберите **Все устройства** > **Добавить**.

2. Выберите пункт **Mac**. Будет загружен файл установки.
3. На машине, которую нужно защитить, запустите программу установки локально (стр. 44).

2.6.2.4 Добавление vCenter или хоста ESXi

В этом разделе описаны методы добавления vCenter или отдельного хоста ESXi на сервер управления:

- Развертывание агента для VMware (виртуальное устройство) (стр. 39)

  Этот способ рекомендуется в большинстве случаев. Виртуальное устройство будет автоматически развернуто на каждом хосте, находящемся под управлением указанной системы vCenter. Можно выбрать хосты и настроить параметры виртуальных устройств.
- Установка агента для VMware (Windows) (стр. 40)

  Этот метод доступен только в случае, если сервер управления установлен на машине, работающей под управлением ОС Windows.

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

  - **Резервное копирование с помощью третьей машины**

    Используйте в том случае, если нагрузка на рабочие хосты ESXi так велика, что запускать на них виртуальные устройства нежелательно.
  - **Резервное копирование без использования локальной сети**

    Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Подробные инструкции см. в разделе «Резервное копирование без использования локальной сети» (стр. 231).
- Регистрация установленного агента для VMware (стр. 40)

  Используйте этот способ, если агент для VMware (виртуальное устройство) развернут из шаблона OVF (стр. 45) или если потребовалось повторно установить сервер управления.
- Настройка уже зарегистрированного агента для VMware (стр. 41)

  Используйте этот способ, если агент для VMware (Windows) установлен вручную или нужно связать агент для VMware с другим vCenter или отдельно стоящим хостом ESXi.

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

1. Щелкните **Все устройства** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Разверните виртуальное устройство на каждом хосте vCenter**.
4. Укажите адрес и учетные данные для доступа к vCenter Server или автономному хосту ESXi. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 242) на vCenter Server или ESXi.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. [Необязательно] Щелкните **Настройки**, чтобы настроить параметры развертывания:

- хосты ESXi, на которых необходимо развернуть агент (только если на предыдущем шаге был указан сервер vCenter Server);
- имя виртуального устройства;
- хранилище данных, в котором будет находиться устройство;
- пул ресурсов или контейнер vApp, в котором будет содержаться устройство;
- сеть, к которой будет подключен сетевой адаптер виртуального устройства;
- настройки сети виртуального устройства. Можно выбрать автоматическую настройку DHCP или вручную указать значения, включая статический IP-адрес.

7. Щелкните **Развернуть**.

Установка агента для VMware (Windows)

Подготовка

Выполните инструкции по подготовке, описанные в разделе «Добавление машины с Windows» (стр. 36).

Установка

1. Щелкните **Все устройства** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Удаленно установить на машине под управлением Windows**.
4. Укажите имя хоста или IP-адрес машины и данные учетной записи с правами администратора на этой машине.
5. Выберите имя или IP-адрес, которые будут использоваться агентом для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. Щелкните **Подключиться**.
7. Укажите адрес и учетные данные для vCenter Server или автономного хоста ESXi, а затем щелкните **Подключиться**. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 242) на vCenter Server или ESXi.
8. Щелкните **Установить**, чтобы установить агент.

Регистрация установленного агента для VMware

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

В качестве альтернативного варианта можно зарегистрировать агент для VMware (виртуальное устройство), указав сервер управления в интерфейсе виртуального устройства. См. шаг 3 в подразделе «Настройка виртуального устройства» раздела «Развертывание агента для VMware (виртуальное устройство) из шаблона OVF» (стр. 45).

Регистрация агента для VMware

1. Щелкните **Все устройства** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Выберите **Зарегистрировать уже установленный агент**.

4. При регистрации *агента для VMware (Windows)* укажите имя хоста или IP-адрес машины, на которой установлен агент, и данные учетной записи с правами администратора на этой машине.

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

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации агента.
6. Щелкните **Подключиться**.
7. Укажите имя хоста либо IP-адрес сервера vCenter Server или хоста ESXi и учетные данные для доступа к нему, а затем щелкните **Подключение**. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 242) на vCenter Server или ESXi.
8. Щелкните **Зарегистрировать**, чтобы зарегистрировать агент.

Настройка уже зарегистрированного агента для VMware

В этом разделе описана настройка агента для VMware в веб-интерфейсе, т. е. подключение агента к vCenter Server или автономному хосту ESXi, для виртуальных машин которого этот агент будет создавать резервные копии.

Настройка агента для VMware

1. Щелкните **Все устройства** > **Добавить**.
2. Щелкните **VMware ESXi**.
3. Программное обеспечение определяет агенты для VMware, зарегистрированные на сервере управления, и показывает в алфавитном порядке первый агент, который еще не настроен.

   При необходимости щелкните **Машина с агентом** и выберите агент для настройки. Этот шаг необходим в указанных ниже случаях:

   - На сервере управления зарегистрировано несколько ненастроенных агентов, и при этом вам необходимо настроить один из них, который не является первым по алфавиту.
   - Необходимо заново подключить уже настроенный агент к другому серверу vCenter или автономному хосту ESXi. В качестве альтернативного варианта последовательно выберите пункты **Настройки** > **Агенты** > агент > **Подробнее** > **vCenter/ESXi**.
4. Укажите или измените имя хоста либо IP-адрес сервера vCenter Server или хоста ESXi и учетные данные для доступа к ним. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 242) на vCenter Server или ESXi.

   Если выбранный агент уже настроен, эти поля заполнены.
5. [Необязательно] Щелкните **Проверить подключение**, чтобы проверить подключение к указанному vCenter Server или автономному хосту ESXi.
6. Щелкните **Настроить**, чтобы сохранить изменения.

2.6.3 Локальная установка агентов

2.6.3.1 Установка в ОС Windows

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

1. Войдите как администратор и запустите программу установки Acronis Backup Advanced.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Установка языка**.
3. Примите условия лицензионного соглашения и укажите, будет ли машина участвовать в программе улучшения качества Acronis Customer Experience Program (CEP).
4. Выберите **Установить агент резервного копирования**.
5. Выполните любое из следующих действий:
   - Выберите пункт **Установить Acronis Backup**.

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

     По умолчанию устанавливаются следующие компоненты:

     - Агент для Windows
     - Другие агенты (агент для Hyper-V, агент для Exchange, агент для SQL и агент для Active Directory), если на машине обнаружен соответствующий гипервизор или приложение
     - Мастер создания загрузочных носителей
     - Программа командной строки
     - Монитор резервного копирования
   - Щелкните **Настройка параметров установки**, чтобы настроить программу установки.

     Можно будет выбрать компоненты для установки и указать дополнительные параметры. Дополнительную информацию см. в разделе «Настройка параметров установки» (стр. 33).
   - Щелкните **Создать MST- и MSI-файлы для автоматической установки**, чтобы извлечь пакеты установки. Проверьте и при необходимости измените настройки установки, которые будут добавлены в MST-файл, затем нажмите кнопку **Создать**. Для этой процедуры не требуется никаких дополнительных шагов.

     Чтобы развернуть агенты через групповую политику, выполните действия, указанные в разделе «Развертывание агентов с использованием групповой политики» (стр. 59).
6. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   b. Укажите учетные данные администратора сервера управления. Можно использовать текущие учетные данные сеанса Windows или явно указать имя пользователя и пароль.

      Если вы вошли не как администратор сервера управления, машину можно зарегистрировать, оставив значение параметра **Подключиться к серверу управления как** по умолчанию.
   c. Нажмите кнопку **Готово**.
7. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена

в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).

8. Приступите к установке.
9. После завершения установки нажмите кнопку **Закрыть**.
10. Если установлен агент для Exchange, можно будет выполнять резервное копирование баз данных Exchange. Чтобы создать резервную копию почтовых ящиков Exchange, откройте консоль резервного копирования, щелкните **Добавить** > **Microsoft Exchange Server** > **Почтовые ящики Exchange** и укажите машину, на которой включена роль сервера **Client Access** (CAS) Microsoft Exchange Server. Дополнительную информацию см. в разделе «Резервное копирование почтовых ящиков» (стр. 204).

Порядок установки агента для VMware (Windows), агента для Office 365, агента для Oracle или агента для Exchange на машину без сервера Microsoft Exchange Server

1. Войдите как администратор и запустите программу установки Acronis Backup Advanced.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Установка языка**.
3. Примите условия лицензионного соглашения и укажите, будет ли машина участвовать в программе улучшения качества Acronis Customer Experience Program (CEP).
4. Выберите **Установить агент резервного копирования**, затем щелкните **Настройка параметров установки**.
5. Рядом с пунктом **Устанавливаемые компоненты** щелкните **Изменить**.
6. Установите флажок, соответствующий агенту, который необходимо установить. Снимите флажки для компонентов, которые не нужно устанавливать. Чтобы продолжить, нажмите кнопку **Готово**.
7. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Перейдите на **Сервер управления Acronis Backup**, нажмите**Указать**.
   b. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   c. Укажите учетные данные администратора сервера управления. Можно использовать текущие учетные данные сеанса Windows или явно указать имя пользователя и пароль.

      Если вы вошли не как администратор сервера управления, машину можно зарегистрировать, оставив значение параметра **Подключиться к серверу управления как** по умолчанию.
   d. Нажмите кнопку **Готово**.
8. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).
9. [Необязательно] Измените другие настройки установки, как описано в разделе «Настройка параметров установки» (стр. 33).
10. Нажмите **Установить**, чтобы продолжить установку.
11. После завершения установки нажмите кнопку **Закрыть**.
12. [Только при установке агента для VMware (Windows)] Выполните процедуру, которая описана в разделе «Регистрация установленного агента для VMware» (стр. 40).
13. [Только при установке агента для Exchange] Откройте консоль резервного копирования, щелкните **Добавить** > **Microsoft Exchange Server** > **Почтовые ящики Exchange** и укажите машину, на которой включена роль сервера **Client Access** (CAS) Microsoft Exchange Server.

Дополнительную информацию см. в разделе «Резервное копирование почтовых ящиков» (стр. 204).

2.6.3.2 Установка в ОС Linux

Подготовка

1. Перед установкой продукта на системе, в которой не используется диспетчер пакетов RPM, такой как Ubuntu, необходимо установить этот диспетчер вручную, например запустив следующую команду в качестве привилегированного пользователя: **`apt-get install rpm`**.
2. Убедитесь в том, что на машине установлены необходимые пакеты Linux (стр. 24).

Установка

Установка агента для Linux

1. Запустите соответствующий файл установки (файл .i686 или .x86_64) как привилегированный пользователь.
2. Примите условия лицензионного соглашения.
3. Снимите флажок **Сервер управления Acronis Backup** и нажмите кнопку **Далее**.
4. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   b. Укажите имя пользователя и пароль администратора сервера управления или выберите анонимную регистрацию.

      Если в вашей организации есть отделы, установка учетных данных может понадобиться, чтобы добавить машину в отдел, которым управляет указанный администратор. При анонимной регистрации машина всегда добавляется в организацию. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).
   c. Нажмите кнопку **Далее**.
5. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов, затем нажмите клавишу **ВВОД**.

   Этот запрос появляется, если учетная запись, указанная в предыдущем шаге, является администратором одного отдела или организации как минимум с одним отделом.
6. После завершения установки нажмите кнопку **Выход**.

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

2.6.3.3 Установка в macOS

Установка агента для Mac

1. Дважды щелкните DMG-файл установки.
2. Дождитесь, пока операционная система подключит образ установочного диска.
3. Дважды щелкните **Установить**, затем щелкните **Продолжить**.
4. [Необязательно] Щелкните **Изменить расположение установки**, чтобы изменить диск, на котором будет установлено программное обеспечение. По умолчанию выбирается диск, с которого запускается система.
5. Нажмите **Установить**. При поступлении соответствующего запроса введите имя и пароль администратора.
6. Укажите сервер управления, на котором будет зарегистрирована машина с агентом:
   a. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.

b. Укажите имя пользователя и пароль администратора сервера управления или выберите анонимную регистрацию.

   Если в вашей организации есть отделы, установка учетных данных может понадобиться, чтобы добавить машину в отдел, которым управляет указанный администратор. При анонимной регистрации машина всегда добавляется в организацию. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).

c. Щелкните **Зарегистрироваться**.

7. При поступлении запроса выберите, добавлять ли машину с агентом в организацию или в один из отделов, затем нажмите кнопку **Готово**.

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

8. После завершения установки нажмите кнопку **Закрыть**.

2.6.3.4 Развертывание агента для VMware (виртуальное устройство) из шаблона OVF

После установки сервера управления пакет виртуального устройства OVF располагается в папке **%ProgramFiles%\Acronis\ESXAppliance** (в Windows) или **/usr/lib/Acronis/ESXAppliance** (в Linux).

Папка содержит один OVF-файл и два VMDK-файла. Убедитесь в том, что эти файлы доступны с машины с клиентом vSphere.

Развертывание шаблона OVF

1. Запустите клиент vSphere и выполните вход на сервер vCenter Server.
2. В меню **Файл** выберите пункт **Развернуть шаблон OVF**.
3. В разделе **Источник** укажите путь к OVF-пакету виртуального устройства.
4. Ознакомьтесь с разделом **Подробные сведения об OVF-шаблоне** и нажмите кнопку **Далее**.
5. В поле **Имя и расположение** введите имя устройства или оставьте имя по умолчанию **AcronisESXAppliance**.
6. В поле **Хост/кластер** выберите хост ESXi, на котором будет развернуто устройство.
7. [Необязательно] В поле **Пул ресурсов** выберите пул ресурсов, в котором будет содержаться устройство.
8. В поле **Хранилище данных** оставьте хранилище данных по умолчанию, если в нем достаточно места для виртуального устройства. Если места недостаточно, выберите другое хранилище данных. Пропустите этот шаг, если на сервере имеется только одно хранилище данных.
9. В поле **Формат диска** выберите требуемое значение. Формат диска не влияет на производительность устройства.
10. В разделе **Отображение сетей** выберите для сетевого адаптера режим моста.
11. Ознакомьтесь со сводкой и нажмите кнопку **Готово**. После сообщения об успешном развертывании закройте индикатор выполнения.

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**. На экране приветствия нажмите кнопку **Закрыть**.

2. **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. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 242) на vCenter Server или ESXi.

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

3. **Сервер управления Acronis Backup**

   В разделе **Параметры агента** в подразделе **Сервер управления Acronis Backup** нажмите кнопку **Изменить**.

   Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления, а также учетные данные для доступа к этой машине.

4. **Часовой пояс**

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

Виртуальное устройство готово к работе. Кроме того, можно изменить следующие параметры.

- **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.

- **Локальные хранилища данных**

  К виртуальному устройству можно присоединить дополнительный диск, чтобы агент для VMware мог сохранять резервные копии на этом локально присоединенном хранилище. Резервное копирование этого типа обычно выполняется быстрее, чем резервное копирование через локальную сеть, а также не занимает полосу пропускания сети.

  Размер виртуального диска должен составлять по меньшей мере 10 ГБ. 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.

  Необходимо соблюдать осторожность при добавлении уже существующего диска. После создания хранилища все данные, содержавшиеся ранее на этом диске, будут потеряны.

2.6.4 Автоматическое установка или автоматическое удаление

2.6.4.1 Автоматическое установка или автоматическое удаление в Windows

В этом разделе показано, как установить или удалить Acronis Backup 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» (стр. 59).

При установке можно использовать файл, называемый **преобразованием** (MST-файл). Преобразование — это файл с параметрами установки. Он используется для массового развертывания посредством групповой политики или сторонних инструментов развертывания. При установке через Windows Installer использование преобразования упрощает установку, поскольку требуемые параметры установки предварительно настроены в этом файле. В качестве альтернативного варианта можно указать параметры прямо в командной строке.

Создание MST-преобразования и извлечение пакета установки

1. Войдите как администратор и запустите программу установки.
2. Щелкните **Создать MST- и MSI-файлы для автоматической установки**.
3. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл.
4. Нажмите кнопку **Создать**.

В результате создается MST-файл, а установочные MSI-пакеты и CAB-пакеты извлекаются в указанную папку.

Установка продукта с использованием преобразования MST

Выполните следующую команду:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

В этой формуле:

- `<package name>` — это имя MSI-файла, извлеченного ранее. Этот файл имеет имя **AB.msi** или **AB64.msi** в зависимости от разрядности операционной системы.
- `<transform name>` — это имя преобразования, созданного ранее. Этот файл имеет имя **AB.msi.mst** или **AB64.msi.mst** в зависимости от разрядности операционной системы.

Например, **`msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`**

Установка или удаление продукта с указанием параметров вручную

Выполните следующую команду:

```
msiexec /i <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Здесь `<package name>` — это имя MSI-файла, извлеченного ранее. Этот файл имеет имя **AB.msi** или **AB64.msi** в зависимости от разрядности операционной системы.

Доступнуы параметры и их значения описаны в разделе «Параметры автоматической установки или автоматического удаления» (стр. 48).

Примеры

- Установка сервера управления и компонентов для удаленной установки.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=ru
ACEP_AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1 AMS_PUBLIC_ADDRESS=10.10.1.1
```

- Установка агента для Windows, компонентов для удаленной установки, инструмента командной строки и индикатора в области уведомлений. Регистрация компонентов, которые устанавливаются на ранее установленный сервер управления.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,ComponentRegisterFeature,C
ommandLineTool,TrayMonitor TARGETDIR="C:\Program Files\Acronis"
REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_AGREEMENT=1
MMS_CREATE_NEW_ACCOUNT=1 MANAGEMENT_SERVER_ADDRESS=10.10.1.1
```

Параметры автоматической установки или автоматического удаления

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

Кроме этих параметров можно использовать другие параметры **msiexec**, как описано по ссылке https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Параметры установки

Стандартные параметры

ADDLOCAL=<список компонентов>

Устанавливаемые компоненты Компоненты разделены запятыми без символов пробела.

Для установки доступны указанные ниже компоненты:

Компонент	Необходимо установить вместе с	Разрядность	Имя / описание компонента
AcronisCentralizedManagementServer	WebConsole	x32/x64	Management Server
WebConsole	AcronisCentralizedManagementServer	x32/x64	Веб-консоль
MonitoringServer	AcronisCentralizedManagementServer	x32/x64	Служба мониторинга
ComponentRegisterFeature	AcronisCentralizedManagementServer	x32/x64	Компоненты для удаленной установки
AgentsCoreComponents		x32/x64	Компоненты Core для агентов
BackupAndRecoveryAgent;	AgentsCoreComponents	x32/x64	Агент для Windows
ArxAgentFeature	BackupAndRecoveryAgent;	x32/x64	Агент для Exchange
ArsAgentFeature	BackupAndRecoveryAgent;	x32/x64	Агент для SQL
ARADAgentFeature	BackupAndRecoveryAgent;	x32/x64	Агент для Active Directory
OracleAgentFeature	BackupAndRecoveryAgent;	x32/x64	Агент для Oracle

Компонент	Необходимо установить вместе с	Разрядность	Имя / описание компонента
ArxOnlineAgentFeature	AgentsCoreComponents	x32/x64	Агент для Office 365
AcronisESXSupport	AgentsCoreComponents	x32/x64	Агент для VMware (Windows)
HyperVAgent	AgentsCoreComponents	x32/x64	Агент для Hyper-V
ESXVirtualAppliance		x32/x64	Агент для VMware (виртуальное устройство)
CommandLineTool		x32/x64	Программа командной строки
TrayMonitor	BackupAndRecoveryAgent;	x32/x64	Монитор резервного копирования
BackupAndRecoveryBootableComponents;		x32/x64	Мастер создания загрузочных носителей
PXEServer		x32/x64	PXE-сервер
StorageServer	BackupAndRecoveryAgent;	x64	Узел хранения
CatalogBrowser	Обновление 111 для JRE 8	x64	Служба каталога

TARGETDIR=<путь>

Папка, в которую будет установлен продукт.

REBOOT=ReallySuppress

Если указан данный параметр, перезапуск машины запрещен.

CURRENT_LANGUAGE=<идентификатор языка>

Язык продукта. Доступны следующие значения: **en**, **en_GB**, **cs**, **da**, **de**, **es_ES**, **fr**, **ko**, **it**, **hu**, **nl**, **ja**, **pl**, **pt**, **pt_BR**, **ru**, **tr**, **zh**, **zh_TW**.

ACEP_AGREEMENT={0,1}

Если задано значение **1**, машина будет участвовать в программе улучшения качества продуктов Acronis.

MANAGEMENT_SERVER_ADDRESS=<имя хоста или IP-адрес>

Имя хоста или IP-адрес машины, на которой установлен сервер управления. Все компоненты (агенты, узел хранения и служба каталогизации), указанные в параметре **ADDLOCAL**, будут зарегистрированы на сервере управления.

TENANT=<имя отдела>

Отдел в организации. Все компоненты (агенты, узел хранения и служба каталогизации), указанные в параметре **ADDLOCAL**, будут добавлены в этот отдел.

Если данный параметр не указан, компоненты будут добавлены в организацию.

/l*v <файл журнала>

Если данный параметр не указан, журнал установки в режиме подробного протоколирования сохраняется в указанный файл. Файл журнала используется для анализа проблем с установкой.

Установка сервера управления

WEB_SERVER_PORT=<номер порта>

Порт, который будет использоваться в веб-браузере для доступа к серверу управления. По умолчанию это порт 9877.

AMS_ZMQ_PORT=<номер порта>

Порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию это порт 7780.

AMS_PUBLIC_ADDRESS=<IP-адрес>

Общедоступный IP-адрес сервера управления. Агенты получат доступ к серверу управления, используя этот IP-адрес.

SQL_INSTANCE=<экземпляр>

База данных, которая должна использоваться сервером управления. Можно выбрать любую версию Microsoft SQL Server 2012, Microsoft SQL Server 2014 или Microsoft SQL Server 2016. Выбранный экземпляр может использоваться и другими программами.

Без этого параметра будет использоваться встроенная база данных SQLite.

SQL_USER_NAME=<имя пользователя> и **SQL_PASSWORD=**<пароль>

Учетные данные для выбранного экземпляра Microsoft SQL Server. Если эти параметры не заданы, будет использоваться проверка подлинности Windows (учетная запись службы сервера управления).

Учетная запись, под которой запущена служба сервера управления

Укажите один из следующих параметров:

- **AMS_USE_SYSTEM_ACCOUNT={0,1}**

  Если задано значение **1**, будет использоваться системная учетная запись.
- **AMS_CREATE_NEW_ACCOUNT={0,1}**

  Если задано значение **1**, будет создана новая учетная запись.
- **AMS_SERVICE_USERNAME=**<имя пользователя> и **AMS_SERVICE_PASSWORD=**<пароль>

  Учетные данные существующей учетной записи, которые будут использоваться.

Установка агента

HTTP_PROXY_ADDRESS=<IP-адрес> и **HTTP_PROXY_PORT=**<порт>

При резервном копировании в облачное хранилище данных и восстановлении из него агент будет использовать прокси-сервер HTTP для подключения к Интернету. Если эти параметры не заданы, не будет использовано ни одного прокси-сервера.

SET_ESX_SERVER={0,1}

Если задано значение **0**, устанавливаемый агент для VMware не будет подключаться к vCenter Server или хосту ESXi. Позже необходимо будет выполнить процедуру, описанную в разделе «Регистрация установленного агента для VMware» (стр. 40).

Если задано значение **1**, укажите следующие параметры:

ESX_HOST=<имя хоста или IP-адрес>

Имя хоста или IP-адрес vCenter Server или хоста ESXi.

ESX_USER=<имя пользователя> и **ESX_PASSWORD=**<пароль>

Учетные данные для доступа к vCenter Server или хосту ESXi.

Учетная запись, с которой будет запускаться служба агента

Укажите один из следующих параметров:

- **MMS_USE_SYSTEM_ACCOUNT={0,1}**

  Если задано значение **1**, будет использоваться системная учетная запись.
- **MMS_CREATE_NEW_ACCOUNT={0,1}**

  Если задано значение **1**, будет создана новая учетная запись.
- **MMS_SERVICE_USERNAME=**<имя пользователя> и **MMS_SERVICE_PASSWORD=**<пароль>

  Учетные данные существующей учетной записи, которые будут использоваться.

Установка узла хранения

Учетная запись, с которой будет запускаться служба узла агента

Укажите один из следующих параметров:

- **ASN_USE_SYSTEM_ACCOUNT={0,1}**

  Если задано значение **1**, будет использоваться системная учетная запись.
- **ASN_CREATE_NEW_ACCOUNT={0,1}**

  Если задано значение **1**, будет создана новая учетная запись.
- **ASN_SERVICE_USERNAME=**<имя пользователя> и **ASN_SERVICE_PASSWORD=**<пароль>

  Учетные данные существующей учетной записи, которые будут использоваться.

Параметры удаления

REMOVE={<список компонентов>**|ALL}**

Компоненты для удаления. Компоненты разделены запятыми без символов пробела.

Доступные компоненты описаны ранее в этом разделе.

Если задано значение **ALL**, все компоненты, установленные на этой машине, 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.

2.6.4.2 Автоматическое установка или автоматическое удаление в Linux

В этом разделе показано, как установить или удалить Acronis Backup в автоматическом режиме на машине с Linux, используя командную строку.

Порядок установки или удаления продукта

1. Откройте приложение терминала.
2. Выполните следующую команду:

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   Здесь <package name> — это имя пакета установки (файла .i686 или .x86_64).

Параметры информации

{-?|--help}

Показано описание параметров.

--usage

Показывает краткое описание использования команды.

{-v|--version}

Показана версия продукта пакета установки.

--product-info

Показана информация о продукте пакета установки.

Параметры установки

Стандартные параметры

{-i|--id}=<список компонентов>

Устанавливаемые компоненты Компоненты разделены запятыми без символов пробела.

Для установки доступны указанные ниже компоненты:

Компонент	Описание компонента
AcronisCentralizedManagementServer	Management Server
BackupAndRecoveryAgent;	Агент для Linux
BackupAndRecoveryBootableComponents;	Мастер создания загрузочных носителей
MonitoringServer	Служба мониторинга

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

--language=<идентификатор языка>

Язык продукта. Доступны следующие значения: **en**, **en_GB**, **cs**, **da**, **de**, **es_ES**, **fr**, **ko**, **it**, **hu**, **nl**, **ja**, **pl**, **pt**, **pt_BR**, **ru**, **tr**, **zh**, **zh_TW**.

{-d|--debug}

Если данный параметр указан, журнал установки записывается в режиме подробного протоколирования. Файл журнала используется для анализа проблем с установкой.

{-t|--strict}

Если данный параметр указан, любое предупреждение при установке приведет к сбою установки. Если данный параметр не указан, установка успешно выполняется, даже при наличии предупреждений.

{-n|--nodeps}

Если параметр указан, отсутствие требуемых пакетов Linux не будет принято во внимание при установке.

Установка сервера управления

{-W|--web-server-port}=<номер порта>

Порт, который будет использоваться в веб-браузере для доступа к серверу управления. По умолчанию это порт 9877.

--ams-tcp-port=<номер порта>

Порт, который будет использоваться для обмена данными между компонентами продукта. По умолчанию это порт 7780.

Установка агента

Укажите один из следующих параметров:

- **--skip-registration**

  Не регистрируйте агент на сервере управления.

- **{-C|--ams}**=<имя хоста или IP-адрес>

  Имя хоста или IP-адрес машины, на которой установлен сервер управления. Агент будет зарегистрирован на этом сервере управления.

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

  Учетные данные для машины, на которой установлен сервер управления.

  --unit=<ИД отдела>

  Идентификатор отдела в организации. Агент будет добавлен в этот отдел.

  Чтобы узнать идентификатор отдела, на консоли резервного копирования щелкните **Настройки** > **Администраторы** > требуемый отдел. Идентификатор отдела — это часть URL-адреса (параметр **unit_id**).

  Если данный параметр не указан, агент будет добавлен в организацию.

Параметры удаления

{-u|--uninstall}

Удаляет продукт.

--purge

Удаляет журналы продукта, задачи и настройки конфигурации.

Примеры

- Установка сервера управления.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Установка сервера управления и службы управления. Определение настраиваемых портов.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i
AcronisCentralizedManagementServer,MonitoringServer --web-server-port 6543
--ams-tcp-port 8123
```

- Установка агента для Linux и его регистрация на удаленном сервере управления.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1
--login root --password 123456
```

- Установка агента для Linux. Регистрация агента на удаленном сервере управления сервер и его добавление в заданный отдел.

```
./AcronisBackup_12.5_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1
--login root --password 123456 –unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

2.6.5 Проверка наличия обновлений программного обеспечения

Эта функциональность доступна только для администраторов организации (стр. 286).

При каждом запуске консоли резервного копирования Acronis Backup проверяет, доступна ли новая версия на веб-сайте Acronis. В таком случае на консоли резервного копирования отображается ссылка на загрузку новой версии в нижней части каждой страницы на вкладках

Устройства, **Планы** и **Резервные копии**. Ссылка также доступна на странице **Настройки** > **Агенты**.

Чтобы включить или отключить автоматические проверки наличия обновлений, измените системную настройку **Обновления** (стр. 285).

Чтобы проверить обновления вручную, щелкните значок вопроса в верхнем правом углу > **О программе** > **Проверить обновления** или значок вопроса > **Проверить обновления**.

2.6.6 Управление лицензиями

Лицензирование Acronis Backup основано на количестве физических машин и хостов виртуализации, подлежащих резервному копированию. Можно использовать как подписки, так и бессрочные лицензии. Период действия подписки начинается с момента ее регистрации на сайте Acronis.

Чтобы приступить к использованию Acronis Backup, необходимо добавить на сервер управления хотя бы один лицензионный ключ. Лицензия автоматически назначается машине при применении плана резервного копирования.

Кроме того, лицензии можно назначить и отозвать вручную. Ручные операции с лицензиями доступны только для администраторов организации (стр. 286).

Порядок доступа к странице «Лицензии»

1. Выполните одно из следующих действий:
   - Щелкните **Настройки**.
   - Щелкните значок учетной записи в правом верхнем углу.
2. Щелкните **Лицензии**.

Добавление лицензионного ключа

1. Щелкните **Добавить ключи**.
2. Введите лицензионные ключи.
3. Нажмите кнопку **Добавить**.
4. Чтобы активировать подписку, необходимо выполнить вход. Если вы ввели хотя бы один ключ подписки, введите адрес электронной почты и пароль своей учетной записи Acronis, а затем нажмите кнопку **Вход**. Если вы ввели только бессрочные ключи, пропустите это действие.
5. Нажмите кнопку **Готово**.

Подсказка *Если вы уже зарегистрировали ключи подписки, сервер управления может импортировать их из вашей учетной записи Acronis. Чтобы синхронизировать ключи подписки, щелкните* ***Синхронизация*** *и выполните вход.*

Управление бессрочными лицензиями

Назначение бессрочной лицензии машине

1. Выберите бессрочную лицензию.

   В программе отобразятся лицензионные ключи, соответствующие выбранной лицензии.
2. Выберите ключ, который нужно назначить.
3. Щелкните **Назначить**.

   В программе отобразятся машины, которым можно назначить выбранный ключ.
4. Выберите машину и нажмите кнопку **Готово**.

Отзыв бессрочной лицензии для машины

1. Выберите бессрочную лицензию.

   В программе отобразятся лицензионные ключи, соответствующие выбранной лицензии. Машина, которой назначен ключ, указана в столбце **Кому назначено**.
2. Выберите лицензионный ключ, который нужно отозвать.
3. Щелкните **Отозвать**.
4. Подтвердите операцию.

   Отозванный ключ останется в списке лицензионных ключей. Его можно назначить другой машине.

Управление лицензиями по подписке

Назначение лицензии по подписке машине

1. Выберите лицензию по подписке.

   В программе отобразятся машины, которым уже назначена выбранная лицензия.
2. Щелкните **Назначить**.

   В программе отобразятся машины, которым можно назначить выбранную лицензию.
3. Выберите машину и нажмите кнопку **Готово**.

Отзыв лицензии по подписке для машины

1. Выберите лицензию по подписке.

   В программе отобразятся машины, которым уже назначена выбранная лицензия.
2. Выберите машину, для которой необходимо отозвать лицензию.
3. Щелкните **Отозвать лицензию**.
4. Подтвердите операцию.

2.7 Облачное развертывание

2.7.1 Подготовка

Шаг 1

Выберите агент в зависимости от того, для какого именно объекта вы хотите создать резервную копию. Сведения об агентах см. в разделе Компоненты (стр. 14).

Шаг 2

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 — небольшой исполняемый файл, который загружает основную программу установки из Интернета и сохраняет ее как временный файл. 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 (стр. 59).

Установка в ОС Linux и OS X выполняется с помощью обычных программ установки.

Всем программам установки необходимо подключение к Интернету для регистрации машины в сервисе резервного копирования. Если подключение отсутствует, выполнить установку не удастся.

Шаг 3

Перед установкой убедитесь в том, 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 резервного копирования, регистрации агентов, загрузки сертификатов, авторизации пользователей, а также скачивания файлов из облачного хранилища;
- **7770...7800** — агенты используют эти порты для обмена данными с сервером управления резервным копированием;
- **44445** — агенты используют этот порт для передачи данных во время резервного копирования и восстановления.

Если в вашей сети включен прокси-сервер, см. раздел «Настройки прокси-сервера» (стр. 56), который поможет понять, нужно ли конфигурировать эти настройки на каждой машине с запущенным агентом резервного копирования.

2.7.2 Настройки прокси-сервера

Агенты резервного копирования могут передавать данные через прокси-сервер HTTP.

Для установки агента требуется подключение к Интернету. Если прокси-сервер настроен в Windows (**Панель управления** > **Свойства браузера** > **Подключения**), то программа установки считает настройки прокси-сервера из реестра и использует их автоматически. В Linux и OS X необходимо указать настройки прокси-сервера до установки.

Чтобы указать настройки прокси-сервера перед установкой агента или изменить их после этого, воспользуйтесь процедурами, которыми описаны ниже.

В ОС Linux

1. Создайте файл **/etc/Acronis/Global.config** и откройте его в текстовом редакторе.
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>
    </key>
</registry>
```

3. Замените `proxy.company.com` именем хоста или IP-адресом прокси-сервера, а `443` — номером порта в десятичном формате.
4. Сохраните файл.
5. Если агент резервного копирования еще не установлен, то можно установить его сейчас. В противном случае перезапустите агент, выполнив следующую команду в любом каталоге:

```
sudo service acronis_mms restart
```

In OS X

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>
    </key>
</registry>
```

3. Замените `proxy.company.com` именем хоста или IP-адресом прокси-сервера, а `443` — номером порта в десятичном формате.
4. Сохраните файл.
5. Если агент резервного копирования еще не установлен, то можно установить его сейчас. В противном случае выполните следующие действия, чтобы перезапустить агент:
   a. Откройте **Приложения** > **Утилиты** > **Терминал**
   b. Выполните следующие команды:

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

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
```

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. Сохраните документ с именем **proxy.reg**.
5. Запустите файл от имени администратора.
6. Подтвердите изменение реестра Windows.
7. Если агент резервного копирования еще не установлен, то можно установить его сейчас. В противном случае выполните следующие действия, чтобы перезапустить агент:
   a. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
   b. Нажмите кнопку **ОК**.
   c. Выполните следующие команды:

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

2.7.3 Установка агентов

В Windows

1. Убедитесь в том, что машина подключена к Интернету.
2. Войдите как администратор и запустите программу установки.
3. Нажмите **Установить**.
4. Укажите учетные данные учетной записи, которой необходимо назначить машину.
5. Щелкните **Показать настройки прокси-сервера**, чтобы проверить или изменить имя/IP-адрес и порт хоста прокси-сервера. В противном случае пропустите этот шаг. Если прокси-сервер включен в Windows, он определяется и используется автоматически.
6. [Только при установке агента для VMware] Укажите адрес и учетные данные доступа для сервера vCenter Server или автономного хоста ESXi, для которых агент будет выполнять резервное копирование виртуальных машин. Рекомендуется использовать учетную запись, которой назначена роль **Администратор**. В противном случае укажите учетную запись с необходимыми привилегиями (стр. 242) на vCenter Server или ESXi.
7. Только при установке на контроллер домена: укажите учетную запись пользователя, под которой будет работать служба агента. В целях безопасности программа установки не может автоматически создавать учетные записи на контроллере домена.
8. Нажмите **Начать установку**.

Чтобы изменить путь установки и учетную запись службы агента, щелкните **Настройка параметров установки** на первом этапе мастера установки.

В ОС Linux

1. Убедитесь в том, что машина подключена к Интернету.
2. Запустите файл установки от имени суперпользователя.
3. Укажите учетные данные учетной записи, которой необходимо назначить машину.
4. Установите флажки для агентов, которые необходимо установить. Доступны следующие агенты:
   - **Агент для Linux**
   - **Агент для Virtuozzo**

   Агент для Virtuozzo невозможно установить без агента для Linux.
5. Завершите процедуру установки.

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

In OS X

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. При необходимости введите учетные данные администратора.
6. Укажите учетные данные учетной записи, которой необходимо назначить машину.
7. Завершите процедуру установки.

2.7.4 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:

- **Ссылка на активацию учетной записи.** Щелкните эту ссылку и задайте пароль для данной учетной записи. Запомните свое имя для входа, которое отображается на странице активации учетной записи.
- **Ссылка на страницу входа в консоль администратора.** Используйте эту ссылку для доступа к консоли в будущем. При этом потребуется указать имя для входа и пароль из предыдущего шага.

2.8 Развертывание агентов с использованием групповой политики

Агент для Windows можно централизованно устанавливать (или развертывать) на машинах в составе домена Active Directory с помощью групповой политики.

В этом разделе описывается настройка объекта групповой политики для развертывания агентов на машинах во всем домене или в его организационной единице.

Каждый раз при входе машины в домен результирующий объект групповой политики проверяет, установлен и зарегистрирован ли на ней агент.

Предварительные требования

Перед развертыванием агента убедитесь в том, что выполнены перечисленные ниже условия.

- Имеется домен Active Directory, контроллер которого работает под управлением Microsoft Windows Server 2003 или более позднего выпуска.
- Вы входите в состав группы **Администраторы домена**.
- Вы загрузили программу установки **Все агенты для установки в Windows**. Ссылка для загрузки доступна на странице **Добавить устройства** на консоли резервного копирования.

Шаг 1. 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. Скопируйте программу установки в созданную папку.
4. Запустите программу установки.
5. Щелкните **Создать MST- и MSI-файлы для автоматической установки**.
6. При поступлении соответствующего запроса укажите данные учетной записи, которой необходимо назначить машины.
7. Проверьте и при необходимости измените параметры установки, которые будут добавлены в MST-файл.
8. Нажмите кнопку **Создать**.

В результате будет сформировано MST-преобразование, а установочные MSI-пакеты и CAB-пакеты будут извлечены в созданную вами папку. Теперь EXE-файл программы установки можно перенести или удалить.

Шаг 2. 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 **Администрирование**, затем щелкните **Пользователи и компьютеры Active Directory** (в Windows Server 2003) или **Управление групповой политикой** (в Windows Server 2008 и Windows Server 2012).
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 и Windows Server 2012:
   - 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** с помощью описанных ниже действий.
   - В Windows Server 2003 щелкните объект групповой политики, а затем выберите **Изменить**.
   - В Windows Server 2008 и Windows Server 2012 в разделе **Объекты групповой политики** щелкните правой кнопкой мыши объект групповой политики, а затем выберите **Изменить**.
7. В оснастке «Редактор объектов групповой политики» разверните узел **Конфигурация компьютера**.
8. В Windows Server 2003 и Windows Server 2008:
   - Разверните узел **Настройки программ**.

   В Windows Server 2012:
   - 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 **Расширенное**, затем нажмите кнопку **ОК**.
12. На вкладке **Изменения** нажмите кнопку **Добавить** и выберите созданное ранее MST-преобразование.
13. Нажмите кнопку **ОК**, чтобы закрыть диалоговое окно **Развертывание программ**.

2.9 Обновление агентов

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

Можно обновить агенты, повторив их установку любым способом. Чтобы одновременно обновить несколько агентов, используйте указанную ниже процедуру.

Порядок обновления агентов с использованием вкладки «Агенты»

1. [Только в локальных развертываниях] Обновите сервер управления.
2. [Только в локальных развертываниях] Убедитесь, что на машине с сервером управления есть пакеты установки. Чтобы узнать о конкретных действиях, выберите «Добавление машины с ОС Windows» (стр. 36) > «Пакеты установки».
3. Щелкните **Настройки** > **Агенты**.

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

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

2.10 Удаление продукта

Чтобы удалить с машины отдельные компоненты продукта, запустите программу установки, перейдите к изменению продукта и отмените выбор компонентов, которые больше не нужны. Ссылки на программы установки доступны на странице **Загрузки** (щелкните значок учетной записи в правом верхнем углу и выберите пункт > **Загрузки**).

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

Предупреждение. *В локальных развертываниях не удалите по ошибке сервер управления. Консоль резервного копирования станет недоступна. Вы больше не сможете выполнять резервное копирование и восстановление машин, зарегистрированных на сервере управления.*

В Windows

1. Войдите как администратор.
2. Откройте **Панель управления** и выберите **Программы и компоненты** (**Установка и удаление программ** в Windows XP) > **Acronis Backup** > **Удалить**.
3. [Необязательно] Установите флажок **Удалить журналы и параметры конфигурации**.

   Не устанавливайте этот флажок, если удаляете агент и планируете установить его снова. Если установить флажок, машина может быть дуплицирована на консоли резервного копирования. При этом резервные копии старой машины могут быть не связаны с новой машиной.
4. Подтвердите операцию.
5. Если планируется установить агент снова, пропустите этот шаг. В противном случае на консоли резервного копирования щелкните **Настройки** > **Агенты**, выберите машину, на которой был установлен агент, а затем щелкните **Удалить**.

В ОС Linux

1. В качестве привилегированного пользователя выполните **.гык.дши.Фскщтшы.ИфслгзФтвКусщмукн.гтштыефдд.гтштыефдд**ю
2. [Необязательно] Установите флажок **Удалить все элементы трассировки продукта (журналы, задания, хранилища, параметры конфигурации продукта)**.

   Не устанавливайте этот флажок, если удаляете агент и планируете установить его снова. Если установить флажок, машина может быть дуплицирована на консоли резервного копирования. При этом резервные копии старой машины могут быть не связаны с новой машиной.

3. Подтвердите операцию.
4. Если планируется установить агент снова, пропустите этот шаг. В противном случае на консоли резервного копирования щелкните **Настройки** > **Агенты**, выберите машину, на которой был установлен агент, а затем щелкните **Удалить**.

В OS X

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. Если планируется установить агент снова, пропустите этот шаг. В противном случае на консоли резервного копирования щелкните **Настройки** > **Агенты**, выберите машину, на которой был установлен агент, а затем щелкните **Удалить**.

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 ВУ правой кнопкой мыши и нажмите **Изменить настройки**.
   b. Выберите диск с хранилищем и нажмите кнопку **Удалить**. В разделе **Параметры удаления** нажмите кнопку **Удалить из виртуальной машины**.
   c. Нажмите кнопку **ОК**.

   В результате диск остается в хранилище данных. Можно подключить другой диск к другому виртуальному устройству.
4. Щелкните ВУ правой кнопкой мыши и нажмите **Удалить с диска**. Подтвердите операцию.
5. Если планируется установить агент снова, пропустите этот шаг. В противном случае на консоли резервного копирования щелкните **Настройки** > **Агенты**, выберите виртуальное устройство, а затем щелкните **Удалить**.

3 Доступ к консоли резервного копирования

Для доступа к консоли резервного копирования введите адрес страницы входа в адресной строке веб-браузера, а затем укажите имя пользователя и пароль, как описано ниже.

Локальное развертывание

Адрес страницы входа это IP-адрес или имя машины, на которой установлен сервер управления.

По умолчанию на одном TCP-порту поддерживаются оба протокола (HTTP и HTTPS). Внести изменения в эту настройку можно при установке сервера управления (стр. 33). По умолчанию используется порт 9877.

На сервере управления (стр. 69) можно настроить использование настраиваемого сертификата или запретить доступ к консоли резервного копирования через HTTP, перенаправив всех пользователей в версию HTTPS.

В ОС Windows

Если сервер управления установлен в ОС Windows, существует два способа входа в консоль резервного копирования:

- Нажмите **Войти**, чтобы войти как текущий пользователь Windows.

  Это самый простой способ входа с машины, на которой установлен сервер управления.

  Если сервер управления установлен на другой машине, этот способ работает при условии, что:

  - Машина, с которой выполняется вход, находится в одном домене Active Directory с сервером управления.
  - Вы вошли как пользователь домена.

  Рекомендуется настроить веб-браузер для выполнения встроенной проверки подлинности Windows (стр. 63). Противном случае веб-браузер запросит имя пользователя и пароль.
- Нажмите **Ввести имя пользователя и пароль**, а затем укажите имя пользователя и пароль.

В любом случае учетная запись должна находится в списке администраторов сервера управления. По умолчанию этот список содержит группу **Администраторы** на машине, где работает сервер управления. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).

В ОС Linux

Если на сервере управления установлена ОС Linux, укажите имя пользователя и пароль учетной записи, которая включена в список администраторов сервера управления. По умолчанию в этот список входит только пользователь **root** на машине с запущенным сервером управления. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).

Облачное развертывание

Адрес страницы входа https://backup.acronis.com/. Имя пользователя и пароль те же, что у учетной записи для Acronis.

Если учетная запись создана администратором резервного копирования, необходимо активировать ее и задать пароль, щелкнув ссылку в сообщении электронной почты со сведениями об активации.

Смена языка

После входа в систему можно изменить язык веб-интерфейса, щелкнув значок учетной записи в правом верхнем углу.

3.1 Настройка веб-браузера для выполнения встроенной проверки подлинности Windows

Выполнение встроенной проверки подлинности Windows возможно при наличии доступа к консоли резервного копирования из машины с запущенной Windows и любого поддерживаемого браузера (стр. 17).

Рекомендуется настроить веб-браузер для выполнения встроенной проверки подлинности Windows. В противном случае веб-браузер запросит имя пользователя и пароль.

Настройка Internet Explorer, Microsoft Edge, Opera и Google Chrome

Если машина, на которой запущен браузер, находится в одном домене Active Directory с машиной, на которой работает сервер управления, добавьте страницу входа консоли к списку веб-узлов **локальной интрасети**.

В противном случае, добавьте страницу входа консоли к списку **надежных веб-узлов** и включите параметр **Автоматический вход в систему с текущим пользователем и паролем**.

См. пошаговые инструкции далее в этом разделе. Поскольку эти браузеры используют параметры Windows, возможна их настройка с помощью групповой политики в домене Active Directory.

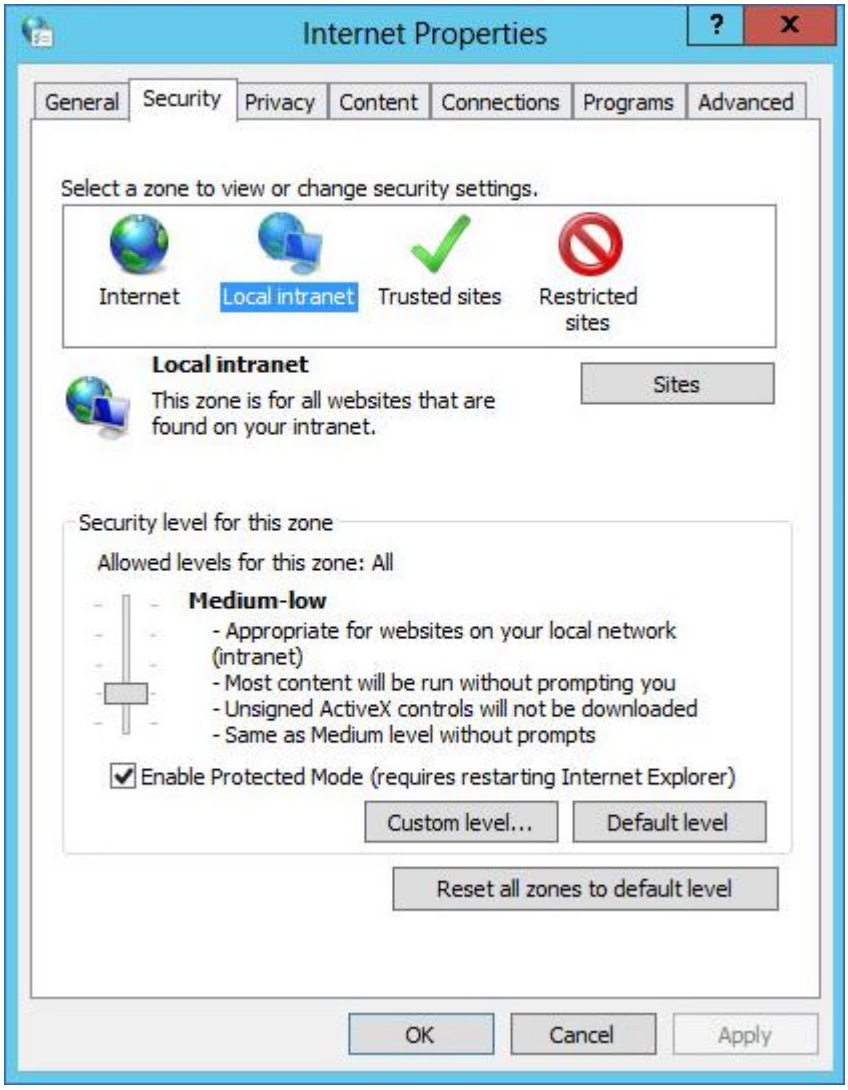
Настройка Mozilla Firefox

1. В Firefox перейдите на URL-адрес `about:config`, а затем нажмите кнопку **Я принимаю возможные риски**.
2. В поле Поиск выполните поиск настройки **network.negotiate-auth.trusted-uris**.
3. Дважды щелкните настройку, а затем введите адрес страницы входа консоли резервного копирования.
4. Повторите шаги 2-3 для настройки `network.automatic-ntlm-auth.trusted-uris`.
5. Закройте окно `about:config`.

3.1.1 Добавление консоли к списку веб-узлов локальной интрасети

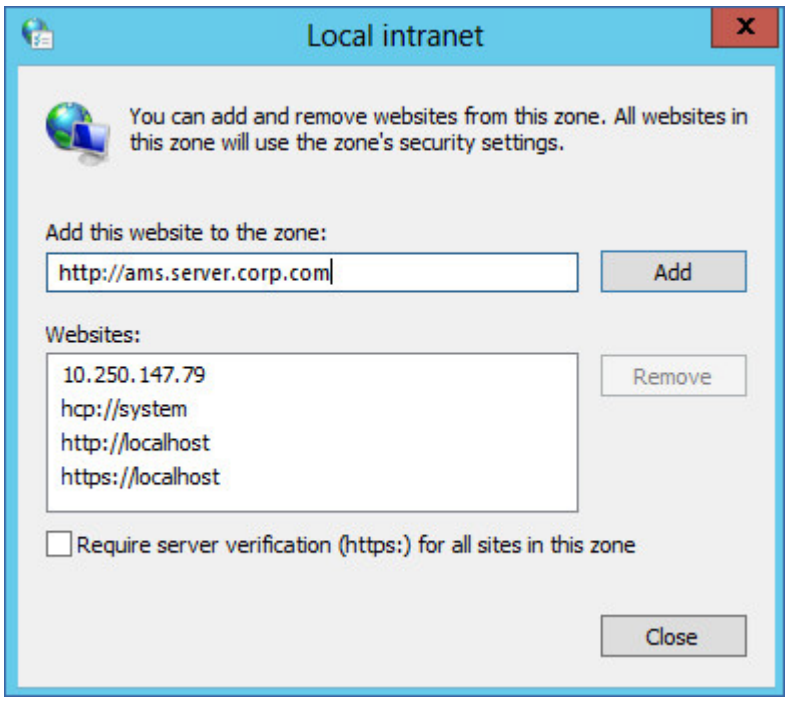
1. Выберите **Панель управления** > **Настройки Интернета**.

2. Во вкладке **Безопасность** выберите **Локальная интрасеть**.



3. Нажмите кнопку **Веб-узлы**.

4. В поле **Добавить этот веб-сайт в зону**, введите адрес страницы входа консоли резервного копирования, а затем нажмите кнопку **Добавить**.

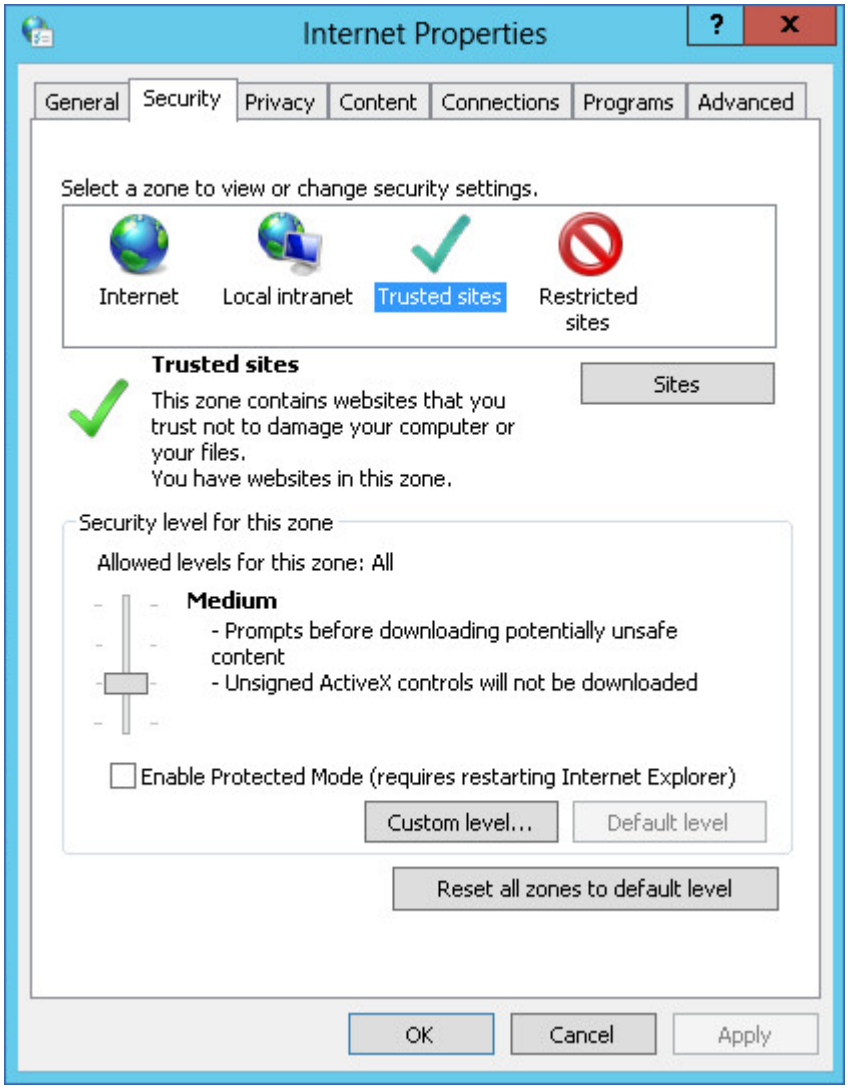


5. Нажмите кнопку **Закрыть**.
6. Нажмите кнопку **ОК**.

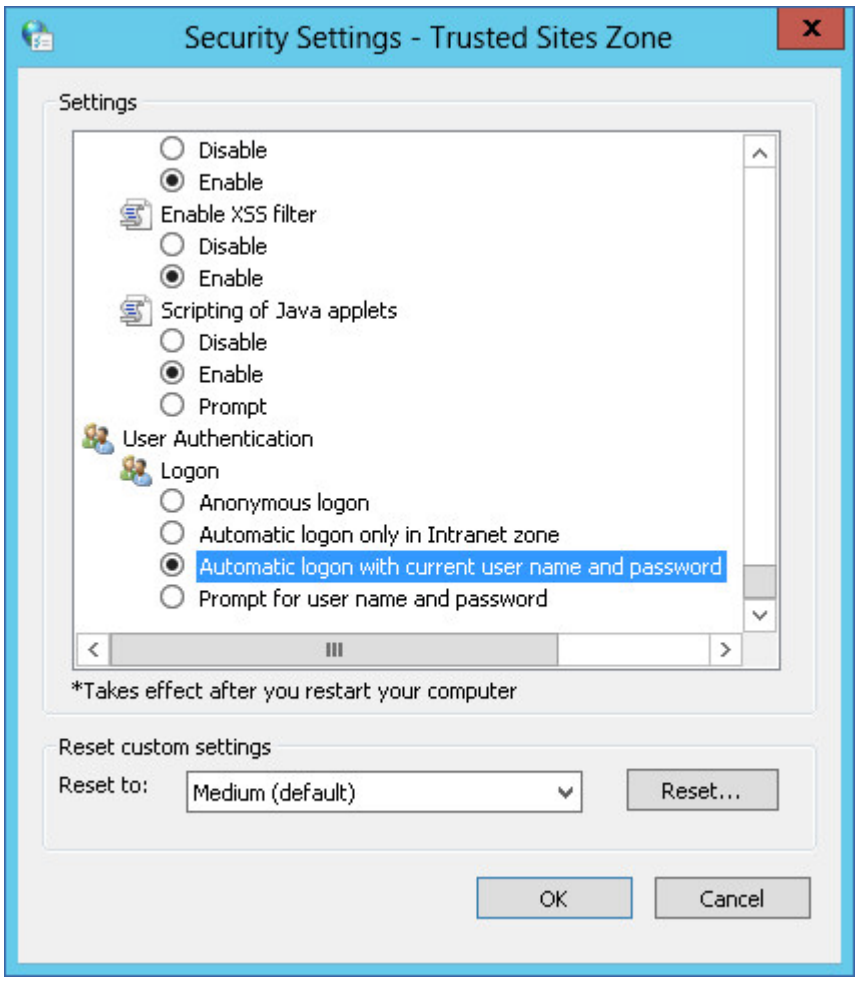
3.1.2 Добавление консоли к списку доверенных веб-узлов

1. Выберите **Панель управления** > **Настройки Интернета**.

2. Во вкладке **Безопасность** выберите **Доверенные веб-узлы**, а затем нажмите **Пользовательский уровень**.

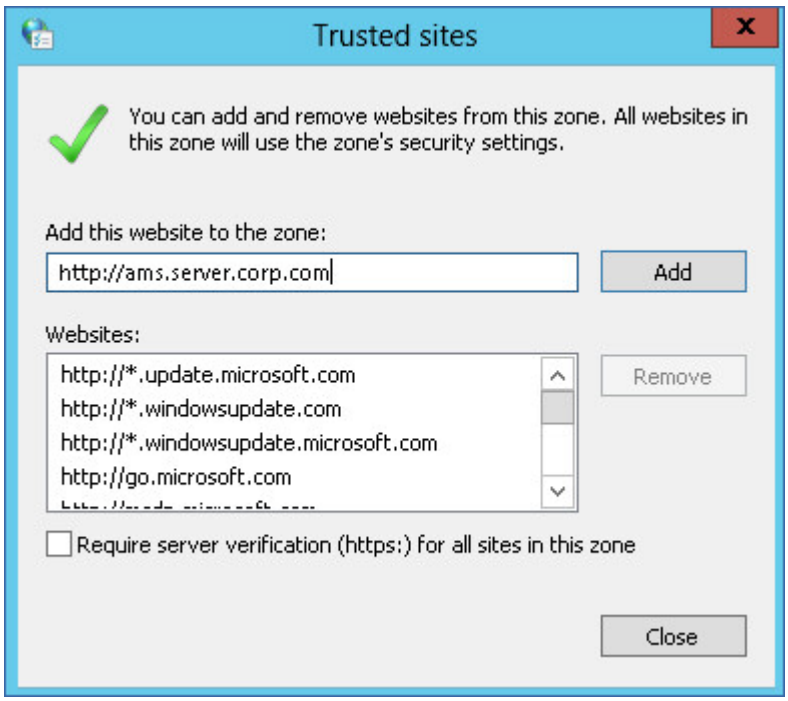


3. В группе **Ученые данные** выберите **Автоматический вход в систему с текущим именем пользователя и паролем**, а затем нажмите кнопку **OK**.



4. Во вкладке **Безопасность**, при выбранных **Доверенных веб-узлах**, нажмите **Веб-узлы**.

5. В поле **Добавить этот веб-сайт в зону**, введите адрес страницы входа консоли резервного копирования, а затем нажмите кнопку **Добавить**.



6. Нажмите кнопку **Закрыть**.
7. Нажмите кнопку **ОК**.

3.2 Изменение сертификата SSL

В этом разделе описано, как заменить самозаверяющий сертификат SSL, созданный сервером управления, сертификатом, выписанным доверенным центром сертификации, таким как GoDaddy, Comodo или GlobalSign. В этом случае сертификат, используемый сервером управления, будет доверенным на любой машине. Оповещение безопасности браузера не будет появляться при входе на консоль резервного копирования с использованием протокола HTTPS.

В качестве альтернативного варианта можно настроить сервер управления таким образом, чтобы он запретил доступ к консоли резервного копирования через HTTP, перенаправляя всех пользователей в версию HTTPS.

Порядок изменения настроек сертификата SSL/TLS

1. Убедитесь, что у вас есть:
   - Файл сертификата (.pem, .cert или в другом формате)
   - Файл с закрытым ключом для сертификата (обычно с расширением .key)
   - Парольная фраза закрытого ключа (если ключ зашифрован)
2. Скопируйте файлы на машину, на которой запущен сервер управления.
3. На этой машине откройте указанный ниже файл конфигурации с текстовым редактором:
   - В Windows: **%ProgramData%\Acronis\ApiGateway\api_gateway.json**
   - В Linux: **/var/lib/Acronis/ApiGateway/api_gateway.json**
4. Найдите следующий раздел:

```
"tls": {
    "auto_redirect" : false,
    "cert_file" : "cert.pem",
    "cipher_suites"  [
        "TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA",
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA", "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA",
        "TLS_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256",
"TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384",
"TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA", "TLS_RSA_WITH_AES_128_GCM_SHA256",
        "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384",
"TLS_RSA_WITH_AES_256_CBC_SHA", "TLS_RSA_WITH_AES_128_CBC_SHA"
    ],
    "key_file" : "key.pem",
    "min_version" : "TLS12",
    "passphrase" : ""
}
```

5. Чтобы запретить доступ к консоли резервного копирования через HTTP, перенаправив всех пользователей в версию HTTPS, измените значение **"auto_redirect"** с **false** на **true**. В противном случае пропустите этот шаг.
6. Между двойными кавычками в строке **"cert_file"** укажите полный путь к файлу сертификата. Например,
   - В Windows (обратите внимание на символы косой черты): **"cert_file": "C:/certificate/local-domain.ams.cert"**
   - В Linux: **"cert_file": "/home/user/local-domain.ams.cert"**
7. Между двойными кавычками в строке **"key_file"** укажите полный путь к файлу закрытого ключа. Например,
   - В Windows (обратите внимание на символы косой черты): **"key_file": "C:/certificate/private.key"**
   - В Linux: **"key_file": "/home/user/private.key"**
8. Если закрытый ключ зашифрован, укажите его парольную фразу между двойными кавычками в строке **"passphrase"**. Например, **"passphrase": "my secret passphrase"**
9. [Необязательно] Между двойными кавычками в строке **"min_version"** измените минимальную версию криптографического протокола, которую должен поддерживать сервер управления.

   Поддерживаются следующие значения: **SSL30**, **TLS11** и **TLS12**. По умолчанию установлено значение **TLS12**. Настоятельно рекомендуем использовать значение по умолчанию, поскольку более ранние версии не являются безопасными. Измените значение по умолчанию только в том случае, если необходимо использовать старые браузеры, которые не поддерживают протокол шифрования TLS12.
10. [Необязательно] Если нормы обеспечения безопасности не позволяют использовать некоторые комплекты шрифтов TLS, удалите пакеты из раздела "cipher_suites". Настоятельно рекомендуем использовать список пакетов шрифтов по умолчанию.

    Важно! *Будьте внимательны, чтобы не удалить в файле конфигурации ни одной запятой, скобки и двойной кавычки.*
11. Сохраните файл **api_gateway.json**.
12. Перезапустите службу Acronis Service Manager, как описано ниже.

Порядок перезапуска службы Acronis Service Manager в Windows

1. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**

2. Нажмите кнопку **ОК**.
3. Выполните следующие команды:

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

Порядок перезапуска службы Acronis Service Manager в Linux

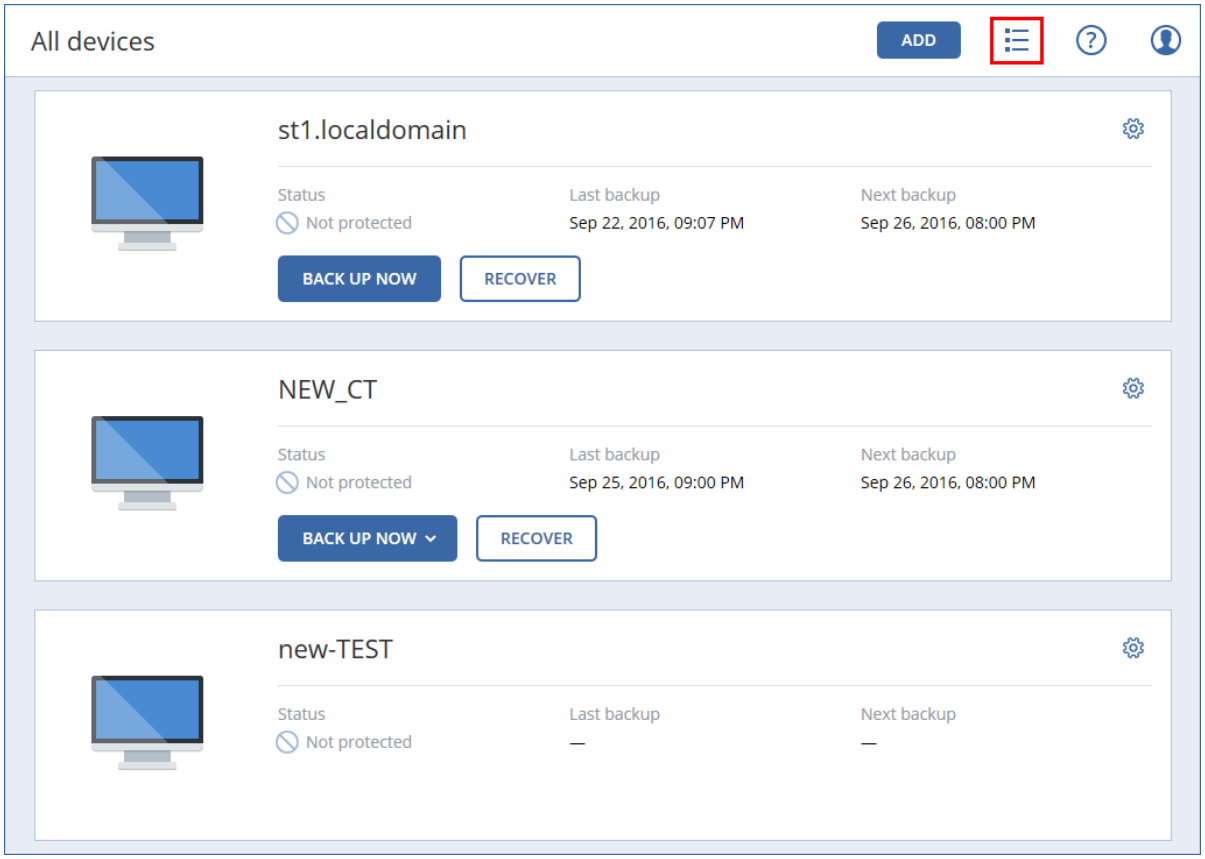
1. Откройте **приложение терминала**.
2. Выполните следующую команду в любом каталоге:

```
sudo service acronis_asm restart
```

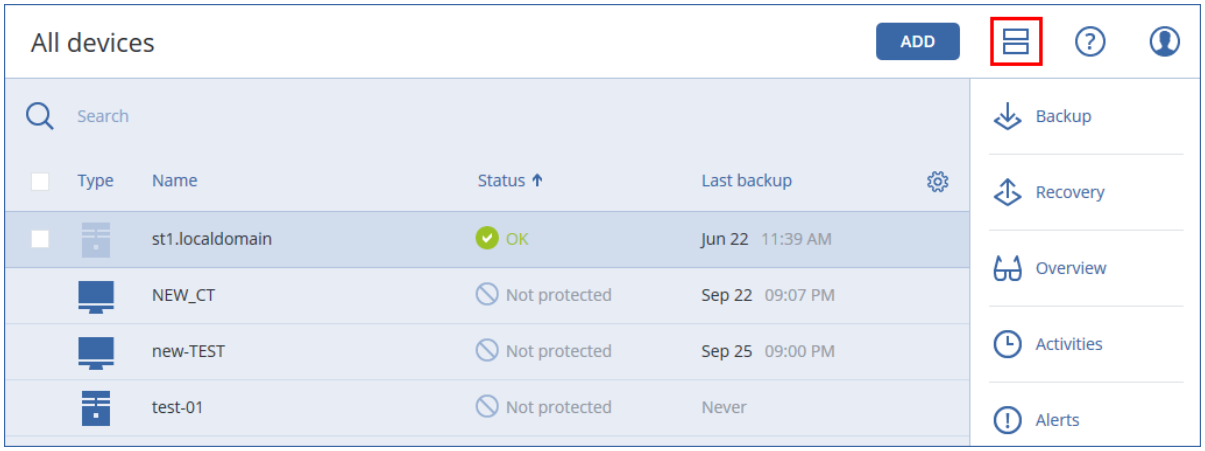
4 Представления консоли резервного копирования

В консоли резервного копирования есть два представления: простое и табличное. Для переключения между ними используется значок в правом верхнем углу.

В этом небольшом представлении поддерживается небольшое количество 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.

5 Резервная копия

План резервного копирования — это набор правил, который определяет порядок защиты данных на этой машине.

В облачных развертываниях план резервного копирования можно применить к нескольким машинам на этапе его создания или позже.

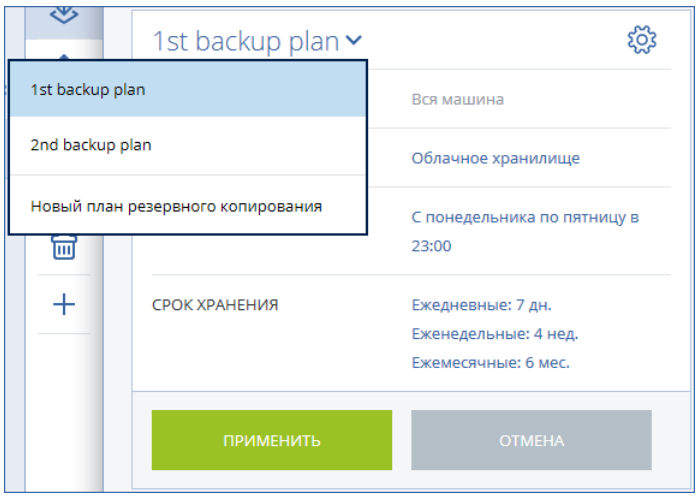
В локальных развертываниях:

- Лицензия Standard позволяет применить план резервного копирования к одной физической машине или нескольким виртуальным машинам.
- Лицензия Advanced позволяет применить план резервного копирования к нескольким физическим или виртуальным машинам во время их создания или позже.

Создание первого плана резервного копирования

1. Выберите машины, резервные копии которых необходимо создать.
2. Нажмите кнопку **Резервное копирование**.

   В программе отображается новый шаблон плана резервного копирования.

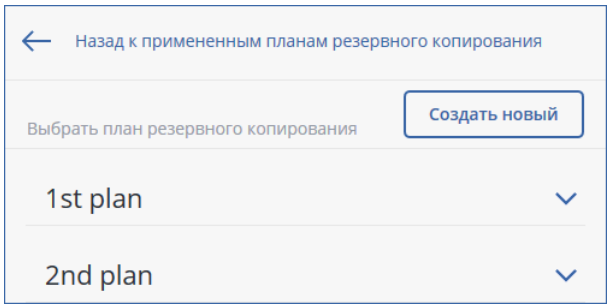


3. [Необязательно] Чтобы изменить имя плана резервного копирования, щелкните имя по умолчанию.
4. Необязательно: чтобы изменить параметры плана, щелкните соответствующий раздел на его панели.
5. [Необязательно] Чтобы изменить параметры резервного копирования, щелкните значок шестеренки.
6. Нажмите кнопку **Создать**.

Применение существующего плана резервного копирования

1. Выберите машины, резервные копии которых необходимо создать.
2. Нажмите кнопку **Резервное копирование**. Если на выбранных машинах уже используется стандартный план резервного копирования, щелкните **Добавить план резервного копирования**.

   В программе отображаются ранее созданные планы резервного копирования.



3. Выберите план резервного копирования для применения.
4. Нажмите кнопку **Применить**.

5.1 План резервного копирования: памятка

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

В таблице ниже вкратце описаны доступные параметры плана резервного копирования. 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 (не для облачной среды)	ВРЕМЯ ХРАНЕНИЯ
Диски/тома (физические машины)	Непосредственный выбор (стр. 78) Правила политики (стр. 78) Фильтры файлов (стр. 119)	Облако (стр. 82) Локальная папка (стр. 82) Сетевая папка (стр. 82) Сервер SFTP (стр. 82)* NFS (стр. 82)* Зона безопасности (стр. 82)* Управляемое хранилище (стр. 82)* Ленточное устройство (стр. 82)*	Всегда инкрементное (один файл) (стр. 88)* Всегда полное (стр. 88) Еженедельно полное, ежедневно инкрементное (стр. 88) Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) (стр. 88) Настраиваемый вариант (П-Д-И) (стр. 88)	По возрасту резервной копии (одно правило на набор резервных копий) (стр. 98) По количеству резервных копий (стр. 98) По общему размеру резервных копий (стр. 98)* Хранить бессрочно (стр. 98)
Диски/тома (виртуальные машины)	Правила политики (стр. 78) Фильтры файлов (стр. 119)	Облако (стр. 82) Локальная папка (стр. 82) Сетевая папка (стр. 82) Сервер SFTP (стр. 82)* NFS (стр. 82)* Управляемое хранилище (стр. 82)* Ленточное устройство (стр. 82)*		
Файлы (только физические машины):	Непосредственный выбор (стр. 76) Правила политики (стр. 76) Фильтры файлов (стр. 119)	Облако (стр. 82) Локальная папка (стр. 82) Сетевая папка (стр. 82) Сервер SFTP (стр. 82)* NFS (стр. 82)* Зона безопасности (стр. 82)* Управляемое хранилище (стр. 82)* Ленточное устройство (стр. 82)	Всегда полное (стр. 88) Еженедельно полное, ежедневно инкрементное (стр. 88) Ежемесячно полное, еженедельно дифференциальное, ежедневно инкрементное (GFS) (стр. 88) Настраиваемый вариант (П-Д-И) (стр. 88)	

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ Способы выбора	МЕСТО СОХРАНЕНИЯ	РАСПИСАНИЕ Схемы резервного копирования (не для облачной среды)	ВРЕМЯ ХРАНЕНИЯ
Конфигурация ESXi	Непосредственный выбор (стр. 81)	Локальная папка (стр. 82) Сетевая папка (стр. 82) Сервер SFTP (стр. 82) NFS (стр. 82)*		
Состояние системы (только в облачных развертываниях)	Непосредственный выбор (стр. 78)	Облако (стр. 82) Локальная папка (стр. 82) Сетевая папка (стр. 82)	Всегда полное (стр. 88) Еженедельно полное, ежедневно инкрементное (стр. 88) Настраиваемый вариант (П-И) (стр. 88)	
Базы данных SQL	Непосредственный выбор (стр. 198)	Облако (стр. 82) Локальная папка (стр. 82) Сетевая папка (стр. 82) Управляемое хранилище (стр. 82)* Ленточное устройство (стр. 82)		
Базы данных Exchange	Непосредственный выбор (стр. 198)			
Почтовые ящики Exchange	Непосредственный выбор (стр. 205)	Облако (стр. 82) Локальная папка (стр. 82) Сетевая папка (стр. 82) Управляемое хранилище (стр. 82)*	Всегда инкрементное (один файл) (стр. 88)	По возрасту резервной копии (одно правило на набор резервных копий) (стр. 98) По количеству резервных копий (стр. 98) Хранить бессрочно (стр. 98)
Почтовые ящики Office 365	Непосредственный выбор (стр. 218)			

* См. ограничения ниже.

Ограничения

Сервер SFTP и ленточное устройство

- Эти хранилища не могут использоваться для резервных копий машин на уровне дисков под управлением macOS.
- Эти хранилища не могут использоваться для резервных копий с поддержкой приложений.

- Схема резервного копирования **Всегда инкрементное (один файл)** недоступна при выполнении резервного копирования в эти хранилища.
- Правило хранения **По общему размеру резервных копий** недоступно для этих хранилищ.

NFS

- Резервное копирование в общие папки NFS недоступно в Windows.

Зона безопасности

- Невозможно создать Зону безопасности на компьютере Mac.

Управляемое хранилище

- Управляемое хранилище не может быть использоваться, если выбрана схема резервного копирования **Всегда инкрементное (один файл)** и в плане резервного копирования активировано шифрование.
- Управляемое хранилище с активированной функцией дедупликации или шифрования не может быть выбрано в качестве места хранения:
  - Если используется схема резервного копирования **Всегда инкрементное (один файл)**
  - Если используется формат резервной копии **Версии 12**
  - Для резервных копий машин под управлением macOS на уровне дисков
  - Для резервных копий почтовых ящиков Exchange и Office 365.
- Правило хранения **По общему размеру резервных копий** недоступно для управляемых хранилищ с активированной функцией дедупликации.

Всегда инкрементное (один файл)

- Схема резервного копирования **Всегда инкрементное (один файл)** недоступна при выполнении резервного копирования на SFTP-сервер или ленточное устройство.

По общему размеру резервных копий

- Правило хранения **По общему размеру резервных копий** недоступно:
  - Если используется схема резервного копирования **Всегда инкрементное (один файл)**
  - При выполнении резервного копирования на SFTP-сервер, ленточное устройство или управляемое хранилище с активированной функцией дедупликации.

5.2 Выбор данных для резервного копирования

5.2.1 Выбор файлов и папок

Резервное копирование на уровне файлов доступно только для физических машин.

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 (стр. 119).

Непосредственный выбор

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.

2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **Непосредственно**.
4. Для каждой машины, включенной в план резервного копирования, 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**.

Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Файлы/папки**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **С использованием правил политики**.
4. Выберите готовые правила, введите собственные или используйте оба варианта.

   Правила политики будут применены ко всем машинам, которые входят в план резервного копирования. 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 стандартных 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**.

5.2.2 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

5.2.3 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 содержит все ее диски.

Выбирать диски и тома файлы можно двумя способами: непосредственно на каждой машине или с помощью правил политики. Исключить файлы из резервной копии можно с помощью фильтров файлов (стр. 119).

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 резервного копирования, установите флажки рядом с дисками и томами, которые требуется скопировать.
5. Нажмите кнопку **Готово**.

Использование правил политики

1. В области **Элементы для резервного копирования** выберите вариант **Диски/тома**.
2. Нажмите **Элементы для резервного копирования**.
3. В области **Выберите элементы для резервного копирования** выберите вариант **С использованием правил политики**.
4. Выберите готовые правила, введите собственные или используйте оба варианта.

   Правила политики будут применены ко всем машинам, которые входят в план резервного копирования. 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 OS X

- **`[All volumes]`** обозначает все тома машин с Windows и все подключенные тома машин с Linux или OS X.

Правила для Windows

- Буква диска (например, **C:**) обозначает том с указанной буквой.
- **`[Fixed Volumes (Physical machines)]`** обозначает 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]`** обозначает системный и загрузочный тома. Это сочетание соответствует минимальному набору данных, который необходим для восстановления операционной системы из резервной копии.
- **`[Disk 1]`** обозначает 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 его имя, а также имя группы томов. Например, чтобы создать резервную копию двух логических томов **lv_root** и **lv_bin**, которые относятся к группе томов **vg_mymachine**, укажите следующие правила выбора:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Правила для OS X

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

5.2.3.1 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 (стр. 129) **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 **(стр. 133)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.

5.2.4 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.

Порядок выбора конфигурации ESXi

1. Нажмите **Устройства** > **Все машины**, после чего выберите хосты ESXi, резервную копию которых вы хотите создать.
2. Нажмите кнопку **Резервное копирование**.
3. В поле **Выбор данных**, выберите **Конфигурация ESXi**.
4. В поле **Пароль пользователя root ESXi** укажите пароль для учетной записи root на каждом выбранном хосте или примените один пароль ко всем хостам.

5.3 Выбор места назначения

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Для выбора хранилища резервных копий

1. Нажмите **Место сохранения резервной копии**.
2. Выполните одно из следующих действий:
   - Выберите использованное ранее или предопределенное хранилище резервных копий
   - Нажмите **Добавить хранилище** и затем укажите новое хранилище резервных копий.

Поддерживаемые расположения

- **Облачное хранилище**

  Резервные копии будут храниться в облачном центре обработки данных.

- **Локальная папка**

  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.

  Резервное копирование в папку с анонимным доступом не поддерживается.

- **Acronis Storage**

  Это высоконадежное программно-определяемое хранилище данных с избыточностью данных и автоматическим самовосстановлением. Это хранилище данных можно настроить как шлюз для хранения резервных копий в Microsoft Azure или в одном из ряда решений для хранения данных, совместимых с S3 или Swift. В хранилище также может использоваться сервер NFS. Дополнительную информацию о Acronis Storage см. в разделе «О Acronis Storage» (стр. 87).

- **Папка NFS** (доступна для машин под управлением Linux или macOS)

  Перейдите к требуемой папке NFS или введите путь к ней в следующем формате:

  `nfs://<имя хоста>/<экспортированная папка>:/<подпапка>`

  После этого нажмите кнопку со стрелкой.

  Невозможно выполнить резервное копирование в папку NFS, защищенную паролем.

- **Раздел Зона безопасности** (доступно, если этот раздел присутствует на каждой из выбранных машин)

  Раздел 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» (стр. 84).

- **SFTP**

  Введите имя или IP-адрес сервера SFTP Поддерживаются следующие форматы:

  ```
  sftp://<сервер>
  sftp://<сервер>/<папка>
  ```

  После ввода имени пользователя и пароля вы можете просматривать папки на сервере.

  В любом формате также можно указать порт, имя пользователя и пароль:

  ```
  sftp://<сервер>:<порт>/<папка>
  sftp://<имя пользователя>@<сервер>:<порт>/<папка>
  sftp://<имя пользователя>:<пароль>@<сервер>:<порт>/<папка>
  ```

  Если номер порта не указан, используется порт 22.

  Пользователи, для которых настроен доступ к SFTP без пароля, могут выполнять резервное копирование на SFTP.

  Резервное копирование на FTP-сервер не поддерживается.

- **Определяется сценарием** (доступно для машин под управлением Windows)

  Можно хранить резервную копию каждой машины в папке, определенной сценарием. Данное программное обеспечение поддерживает сценарии, написанные на языках JScript или VBScript. При развертывании плана резервного копирования 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. На вкладке **Резервные копии** каждая папка показана в виде отдельного хранилища резервных копий.

  В поле **Тип сценария** выберите тип сценария (**JScript** или **VBScript**), 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 архивных копий для машины в формате **\\bkpsrv**<machine name>:

  ```
  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**.

Расширенный выбор вариантов хранения

Примечание *Эта функция доступна только при наличии лицензии Advanced для Acronis Backup.*

- **Узел хранения**

  Узел хранения — это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается путем организации хранилищ и управления хранилищами, выделенными для корпоративных резервных копий (управляемыми хранилищами).

  Выберите предварительно созданное хранилище или создайте новое, нажав **Добавить хранилище** > **Узел хранения**. Информацию о настройках см. в разделе «Добавление управляемого хранилища» (стр. 277).

- **Лента**

Если ленточное устройство подключено к машине, для которой создана резервная копия или к узлу хранения, в списке хранилище указывается заданный по умолчанию пул лент. Этот пул создается автоматически.

Выберите заданный по умолчанию пул или создайте новый, нажав **Добавить хранилище** > **Лента**. Информацию о настройках пула см. в «Создание пула» (стр. 269).

5.3.1 Информация о разделе Зона безопасности

Раздел 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 раздел Зона безопасности не должен быть единственным хранилищем резервных копий. В корпоративной среде раздел Зона безопасности можно представить как вспомогательное хранилище резервных копий, когда обычное хранилище временно недоступно или подключено через медленный или загруженный канал.

Почему нужно использовать раздел Зона безопасности?

Раздел 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.

Ограничения

- Раздел Зона безопасности невозможно организовать на компьютере Mac.
- Раздел Зона безопасности — это раздел на базовом диске. Его невозможно организовать на динамическом диске или создать как логический том (управляемый LVM).
- Раздел Зона безопасности форматируется в файловую систему 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.
- Раздел Зона безопасности не поддерживает формат одного файла резервной копии (стр. 294). При изменении назначения на раздел Зона безопасности в плане резервного копирования, который имеет схему резервного копирования **Всегда инкрементное (один файл)**, данная схема заменяется схемой **Еженедельно полное, ежедневно инкрементное**.

Преобразование диска в результате создания раздела Зона безопасности

- Раздел Зона безопасности всегда создается в конце жесткого диска.
- Если в конце диска нераспределенного пространства нет или недостаточно, но существует нераспределенное пространство между томами, то эти тома будут перемещены, чтобы добавить больше нераспределенного пространства в конец диска.
- Если все незанятое пространство собрано, но его не хватает, то программа заберет свободное пространство из томов по выбору, пропорционально уменьшив их размер.

- Тем не менее на томе должно быть свободное пространство для работы операционной системы и приложений, например для создания временных файлов. Программа не будет уменьшать размер тома, на котором свободное пространство меньше или равно 25 % общего объема тома. Только если все тома на диске будут иметь 25 % или меньше свободного пространства, программа продолжит пропорциональное уменьшение томов.

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

Важно! *Для перемещения или изменения размера тома, с которого загружена операционная система, потребуется перезагрузка.*

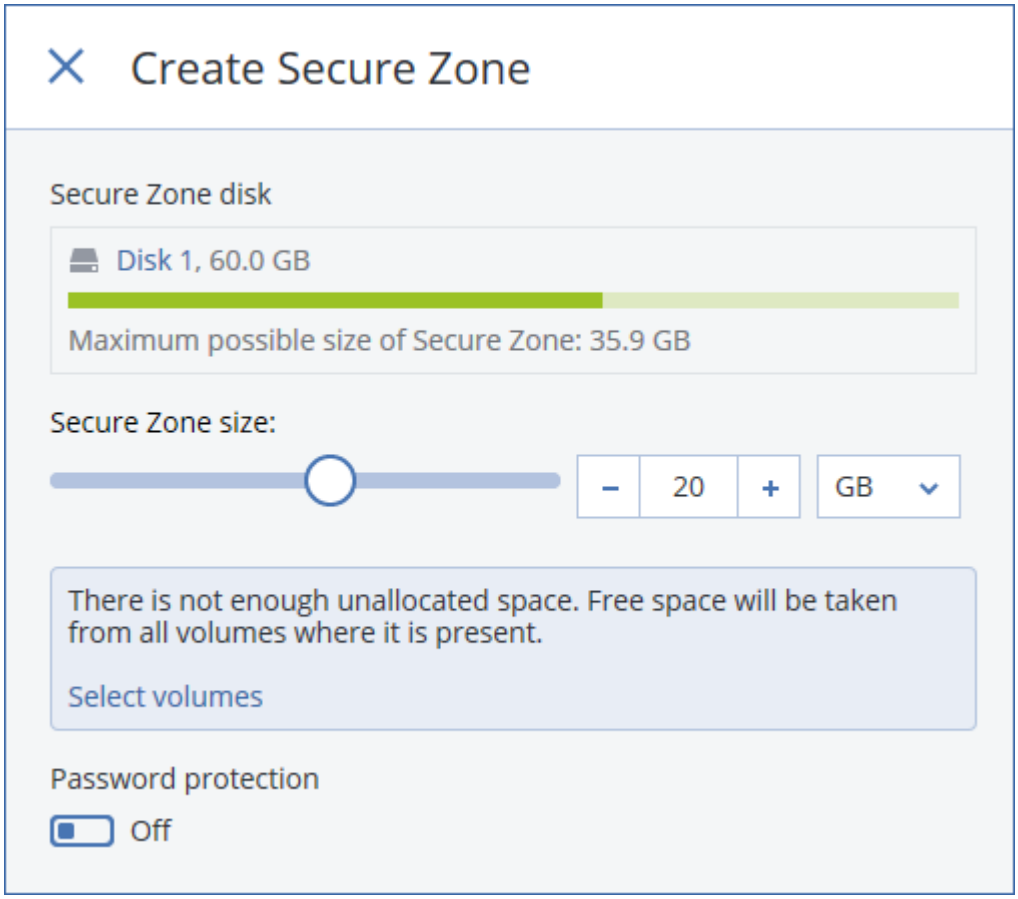
Создание раздела Зона безопасности

1. Выберите машину, на которой необходимо создать раздел Зона безопасности.
2. Выберите **Сведения** > **Создать раздел Зона безопасности**.
3. В разделе **Диск раздела 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 раздела Зона безопасности или перетащите ползунок, чтобы выбрать любой размер 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 **ОК**.
8. Подождите, пока программа создаст раздел Зона безопасности.

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

Порядок удаления раздела Зона безопасности

1. Выберите машину с разделом Зона безопасности.
2. Нажмите **Сведения**.
3. Щелкните значок шестеренки 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.

5.3.2 Информация о Acronis Storage

Развертывание

Чтобы использовать Acronis Storage, разверните его на «голом железе» в локальном месте. Чтобы воспользоваться всеми преимуществами Acronis Storage, необходимо по крайней мере пять физических серверов. Если нужна только функциональность шлюза, можно использовать один физический или виртуальный сервер либо настроить кластер шлюзов с максимально большим количеством серверов.

Убедитесь, что настройки времени синхронизированы между сервером управления и Acronis Storage. Эти настройки врмени для Acronis Storage можно настроить при развертывании. Синхронизация времени по протоколу NTP включена по умолчанию.

Можно развернуть несколько экземпляров Acronis Storage и зарегистрировать их на одном сервере управления.

Регистрация

Регистрация выполняется в веб-интерфейсе Acronis Storage. Acronis Storage может быть зарегистрировано только администраторами организации. После регистрации хранилище становится доступным всем отделам организации. Его можно добавить в качестве хранилища резервных копий в любой отдел или организацию.

Добавление хранилища резервных копий

В отдел или организацию можно добавить только по одному хранилищу резервных копий на каждый экземпляр Acronis. Хранилище, добавленное на уровне отдела, доступно в этом отделе и администраторам организации. Хранилище, добавленное на уровне организации, доступно только администраторам организации.

При добавлении хранилища вы создаете и вводите его имя. Если понадобится добавить существующее хранилище на новый или другой сервер управления, установите флажок **Использовать существующее харнилище…**, щелкните **Обзор** и выберите хранилище в списке.

Если на сервере управления зарегистрировано несколько экземпляров Acronis Storage, можно выбрать экземпляр Acronis Storage при добавлении хранилища.

Схемы резервного копирования, операции и ограничения

В плане доступных схем резервного копирования, операций с резервными копиями и ограничений, Acronis Storage подобна облачному хранилищу данных. Единственное отличие состоит в том, что можно выполнить репликацию резервных копий *с* Acronis Storage при выполнении плана резервного копирования.

Документация

Полный набор документации по Acronis Storage доступен на веб-сайте Acronis.

5.4 Расписание

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Параметры расписания зависят от того, куда будут сохраняться резервные копии.

Облачное хранилище данных

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.

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» (стр. 90).

Внимание! *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.*

При выполнении резервного копирования в другие хранилища

Можно выбрать одну из стандартных схем резервного копирования или создать собственную. Схема входит в состав плана резервного копирования и содержит расписание и методы создания резервных копий.

В разделе **Схема резервного копирования** выберите один из перечисленных ниже вариантов.

- [Только резервные копии на уровне дисков] **Всегда инкрементные (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 новый формат резервной копии в виде одного файла (стр. 294).

  Эта схема недоступна при выполнении резервного копирования на SFTP-сервер или в зону безопасности.

- **Всегда полное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска резервного копирования.

  Чтобы сменить частоту создания резервной копии, перетащите ползунок и задайте расписание резервного копирования.

  Каждый раз создаются полные резервные копии.

- **Еженедельно полное, ежедневно инкрементное**

  По умолчанию резервное копирование выполняется ежедневно с понедельника по пятницу. Дни недели и время запуска резервного копирования можно изменить.

  Раз в неделю создается полная резервная копия. Остальные копии будут инкрементными. Время создания полной резервной копии определяется параметром **Еженедельное**

резервное копирование (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 **Пользовательская** схема на панели плана резервного копирования.

- **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» (стр. 90).

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» (стр. 92).
- 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.

  Щелкните значок шестеренки, затем последовательно выберите пункты **Параметры резервного копирования** > **Планирование задач**. Установите флажок **Распределять время запуска резервного копирования по доступному времени**, затем укажите максимальную задержку. Продолжительность задержки для каждой машины определяется при применении плана резервного копирования к машине и остается неизменной до тех пор, пока в плане резервного копирования не будет изменено максимальное значение задержки.

  Примечание *В облачных развертываниях этот параметр включен по умолчанию с максимальной задержкой 30 минут. В локальных развертываниях по умолчанию все резервные копии запускаются точно по расписанию.*

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

5.4.1 Планирование по событиям

При составлении расписания для плана резервного копирования 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 резервного копирования. Укажите период времени.
- **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 (стр. 91).

В следующей таблице перечислены события, доступные для различных данных в ОС Windows и Linux. В ОС Mac планирование по событиям не поддерживается.

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	С заданной периодичностью	При входе пользователя в учетную запись	При выходе пользователя из учетной записи	При запуске системы	При завершении работы системы	По событию в журнале событий Windows
Диски/тома или файлы (физические машины)	Windows, Linux	Windows	Windows	Windows, Linux	Windows	Windows
Диски/тома (виртуальные машины)	Windows, Linux	–	–	–	–	–
Конфигурация ESXi	Windows, Linux	–	–	–	–	–
Почтовые ящики Office 365	Windows	–	–	–	–	Windows

Базы данных и почтовые ящики Exchange	Windows	–	–	–	–	Windows
Базы данных SQL	Windows	–	–	–	–	Windows

5.4.1.1 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 резервного копирования, 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. Например: **Microsoft Office Sessions**

Источник события

Указывает источник события — как правило, программу или компонент системы, который вызвал событие. Например: **диск**

Тип события

Указывает тип события: **ошибка**, **предупреждение**, **информация**, **проверка успех** или **проверка неудача**.

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 пока 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 резервного копирования, который создаст резервную копию данных жесткого диска в такой ситуации.

Если ОС Windows обнаруживает плохой блок на жестком диске, это событие записывается в журнал **Система** с источником события **диск** и номером события **7**, тип этого события — **ошибка**.

Во время создания плана введите или выберите следующее в разделе **Расписание**.

- **Имя журнала**: **Система**
- **Источник события**: **диск**
- **Тип события**: **Ошибка**
- **Идентификатор события**: **7**

Важно! *Чтобы убедиться в том, что резервное копирование будет выполнено несмотря на присутствие плохих блоков, необходимо настроить резервное копирование на пропуск плохих блоков. Для этого в разделе* ***Параметры резервного копирования*** *выберите* ***Обработка ошибок*** *и установите флажок* ***Пропуск поврежденных секторов****.*

5.4.2 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 резервного копирования.

Поведение планировщика заданий в случае, если событие происходит, а одно или несколько условий не выполнено, определяется параметром резервного копирования Условия запуска резервного копирования (стр. 115). Чтобы предусмотреть случаи, когда условия не выполняются в течение слишком долгого времени и дальнейшая отсрочка резервного копирования становится рискованной, можно установить временной промежуток, после которого задание запустится независимо от условия.

В следующей таблице перечислены условия запуска, доступные для различных данных в ОС Windows и Linux. В ОС Mac условия запуска не поддерживаются.

ЭЛЕМЕНТЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ	Диски/тома или файлы (физические машины)	Диски/тома (виртуальные машины)	Конфигурация ESXi	Почтовые ящики Office 365	Базы данных и почтовые ящики Exchange	Базы данных SQL
Пользователь неактивен (стр. 93)	Windows	–	–	–	–	–
Хост хранилища резервных копий доступен (стр. 93)	Windows, Linux	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Пользователи завершили сеанс (стр. 94)	Windows	–	–	–	–	–
В интервале времени (стр. 94)	Windows, Linux	Windows, Linux	–	–	–	–
Сэкономить заряд батареи (стр. 95)	Windows	–	–	–	–	–

Не запускать при работе на лимитном подключении (стр. 96)	Windows	–	–	–	–	–
Не запускать при подключении к следующим сетям Wi-Fi (стр. 96)	Windows	–	–	–	–	–
Проверить IP-адрес устройства (стр. 97)	Windows	–	–	–	–	–

5.4.2.1 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.

5.4.2.2 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.

5.4.2.3 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.

5.4.2.4 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.

5.4.2.5 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 (стр. 115) 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.

5.4.2.6 Не запускать при работе на лимитном подключении

Предотвращает резервное копирование (включая резервное копирование на локальный диск), если устройство подключено к Инетрнету 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.

5.4.2.7 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.

5.4.2.8 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.

5.5 Правила хранения

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

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 резервного копирования. По умолчанию правила хранения задаются отдельно для каждого набора резервных копий (стр. 293). 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.

     Данная настройка недоступна в схеме резервного копирования **Всегда инкрементное (один файл)** или при резервном копировании в облачное хранилище, на сервер SFTP или на ленточное устройство.
   - **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.
   - **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.

Что еще нужно знать

- Последняя резервная копия созданная по плану резервного копирования сохраняется в любом случае, даже если это нарушает правило хранения. Не пытайтесь удалить единственную резервную копию, применяя правила хранения перед выполнением резервного копирования.

- Резервные копии, которые хранятся на ленточном накопителе, не удаляется физически до перезаписи данных на ленте.
- Если в соответствии со схемой резервного копирования и форматом резервного копирования каждая резервная копия хранится в отдельном файле, этот файл не может быть 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» (стр. 109).

5.6 Шифрование

Рекомендуем шифровать все резервные копии, которые хранятся в облачном хранилище данных, особенно в том случае, если вашей компании необходимо обеспечить соответствие требованиям регуляторов.

Важная информация. *Если вы потеряете или забудете пароль, восстановить зашифрованные резервные копии будет невозможно.*

Шифрование в плане резервного копирования

Чтобы включить шифрование, укажите настройки шифрования при создании плана резервного копирования. После применения плана резервного копирования настройки шифрования будет невозможно изменить. Чтобы использовать другие настройки шифрования, создайте новый план резервного копирования.

Определение настроек шифрования в плане резервного копирования

1. На панели плана резервного копирования включите переключатель **Шифрование**.
2. Укажите и подтвердите пароль шифрования.
3. Выберите один из следующих алгоритмов шифрования:
   - **AES 128** — резервные копии будут зашифрованы с использованием алгоритма AES и 128-разрядного ключа.
   - **AES 192** — резервные копии будут зашифрованы с использованием алгоритма AES и 192-разрядного ключа.
   - **AES 256** — резервные копии будут зашифрованы с использованием алгоритма AES и 256-разрядного ключа.
   - **ГОСТ Р 34.12-2015** – резервные копии будут зашифрованы с использованием алгоритма, соответствующего стандарту ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».
4. Нажмите кнопку **ОК**.

Шифрование как свойство машины

Этот параметр предназначен для администраторов, которые работают с резервными копиями нескольких машин. Если необходим уникальный пароль шифрования для каждой машины или нужно принудительно шифровать резервные копии независимо от настроек шифрования плана резервного копирования, сохраните настройки шифрования на каждой машине в отдельности. Резервные копии будут зашифрованы с использованием алгоритма AES и 256-разрядного ключа.

Сохранение настроек шифрования на машине влияет на планы резервного копирования следующим образом:

- **Планы резервного копирования, которые уже применены к машине.** Если настройки шифрования в плане резервного копирования разные, процессы резервного копирования завершатся сбоем.
- **Планы резервного копирования, которые будут применены к машине позже.** Настройки шифрования, сохраненные на машине, переопределят настройки шифрования в плане резервного копирования. Любая резервная копия будет зашифрована, даже если шифрование отключено в настройках плана резервного копирования.

Эту возможность можно использовать на машине с запущенным агентом для VMware. Однако следует соблюдать осторожность, если к одному серверу vCenter Server подключено несколько агентов для VMware. Обязательное требование состоит в том, что для всех агентов настройки шифрования должны быть одинаковы, поскольку между ними имеет место процесс распределения нагрузки.

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

Важно! *Если план резервного копирования, который выполняется на этой машине, уже создал резервные копии, изменение настроек шифрования приведет к сбою этого плана. Чтобы продолжить резервное копирование, создайте новый план.*

Сохранение настроек шифрования на машине

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

     Здесь <путь_к_установке> — это путь к установленному агенту резервного копирования. По умолчанию это путь **%ProgramFiles%\BackupClient** в облачных развертываниях и путь **%ProgramFiles%\Acronis** в локальных развертываниях.
   - В Linux: **/usr/sbin/acropsh -m manage_creds --set-password** <пароль_шифрования>

Сброс настроек шифрования на машине

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

     Здесь <путь_к_установке> — это путь к установленному агенту резервного копирования. По умолчанию это путь **%ProgramFiles%\BackupClient** в облачных развертываниях и путь **%ProgramFiles%\Acronis** в локальных развертываниях.
   - В Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Для изменения настроек шифрования с помощью монитора резервного копирования

1. Войдите в систему как администратор в Windows или macOS.
2. Выберите значок **Монитора резервного копирования** в области уведомлений (в Windows) или строке меню (в macOS).
3. Выберите значок шестеренки.
4. Выберите пункт **Шифрование**.
5. Выполните одно из следующих действий:
   - Установите **пароль для этой машины**. Укажите и подтвердите пароль шифрования.

- Выберите пункт **Использовать настройки шифрования, указанные в плане резервного копирования**.

6. Нажмите кнопку **ОК**.

Порядок работы шифрования

Алгоритм шифрования AES выполняется в режиме CBC (цепочка шифроблоков) и использует сформированный случайным образом ключ указанного пользователем размера (128, 192 или 256 бит). Чем больше размер ключа, тем дольше будет выполняться шифрование резервных копий и тем выше будет безопасность данных.

Затем ключ шифрования шифруется с помощью алгоритма AES-256, используя в качестве ключа хэш пароля SHA-256. Сам пароль не сохраняется где-либо на диске или в резервных копиях. В целях проверки используется хэш пароля. Такая двухуровневая схема защиты позволяет обезопасить данные резервной копии от несанкционированного доступа, но восстановление утраченного пароля невозможно.

5.7 Нотаризация

Важно! *Эта функция была представлена в версии 12.5, и влияет только на локальные развертывания. Эта функция пока недоступна в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Нотаризация позволяет подтвердить целостность файла и отсутствие изменений в нем с момента резервного копирования. Мы рекомендуем включить нотаризацию при резервном копировании файлов, содержащих юридические документы, а также для всех иных файлов, требующих подтверждения подлинности.

Нотаризация доступна только для резервного копирования на уровне файлов. Файлы с цифровой подписью пропускаются, поскольку нет необходимости их нотаризировать.

Нотаризация *недоступна*:

- Если используется формат резервной копии **Версия 11**
- Если местом назначения резервной копии является Зона безопасности
- Если местом назначения резервной копии является управляемое расположение с включенной дедупликацией или шифрованием

Использование нотаризации

Для включения нотаризации всех файлов, выбранных для резервного копирования (за исключением файлов с цифровой подписью), включите переключатель **Нотаризация** при создании плана резервного копирования.

При настройке восстановления нотаризованные файлы будут помечены значком, и вы сможете верифицировать подлинность файла (стр. 147).

Принцип работы

Выполняя резервное копирование, агент рассчитывает хэш-коды файлов в создаваемой резервной копии, формирует дерево хэшей (на основе структуры папок), сохраняет дерево в резервной копии, а затем отправляет дерево хэшей службе нотаризации. Служба нотаризации сохраняет корень дерева хэшей в базу данный на основе цепочки блоков Ethereum, чтобы гарантировать, что это значение не изменится.

При проверке аутентичности файла агент рассчитывает хэш файла и сравнивает его с хэшем, сохраненным в дереве хэшей в резервной копии. Если эти хэши не совпадают, файл не считается подлинным. В противном случае подлинность файла гарантируется деревом хэшей.

Чтобы удостовериться в том, что дерево хэшей само не было скомпрометировано, агент отправляет корень дерева хэшей в службу нотаризации. Служба нотаризации сравнивает его с корнем, который сохранен в базе данный на основе цепочки блоков. Если хэши совпадают, то выбранный файл гарантированно является подлинным. В противном случае в программном обеспечении отображается сообщение о том, что файл не является подлинным.

5.8 Преобразование в виртуальную машину

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Преобразование в виртуальную машину возможно только для резервных копий на уровне дисков. Если в резервной копии есть системный том и вся информация, необходимая для запуска операционной системы, то созданная виртуальная машина может запускаться без стороннего содействия. В противном случае можно добавить ее виртуальные диски на другую виртуальную машину.

Чтобы выполнить преобразование, необходимо иметь хост ESXi или Hyper-V и агент резервного копирования (агент для VMware или агент для Hyper-V), который управляет этим хостом.

Методы преобразования

- **Обычное преобразование**

  Есть два способа настроить регулярное преобразование:

  - **Сделать преобразование частью плана резервного копирования** (стр. 103)

    Преобразование будет выполняться после каждого резервного копирования (если настроено для первичного хранилища) или после каждой репликации (если настроено для второго и последующих хранилищ).

  - **Создать отдельный план преобразования** (стр. 166)

    Этот метод позволяет указать отдельное расписание преобразования.

- **Восстановить на новую виртуальную машину** (стр. 138)

  Этот метод позволяет выбрать диски для восстановления и задать настройки для каждого виртуального диска. Этот метод позволяет выполнять преобразование только один раз или время от времени, например, для выполнения миграции с физической машины на виртуальную (стр. 245).

Сравнение регулярного преобразования и преобразования виртуальной машины из резервной копии

Обе операции предоставляют в ваше распоряжение виртуальную машину, которую можно запустить за считанные секунды в случае сбоя оригинальной машины.

Для регулярного преобразования требуются ресурсы ЦП и памяти. Файлы виртуальной машины постоянно занимают место в хранилище данных. Если рабочий хост используется для преобразования, это может быть непрактично. Однако производительность виртуальной машины ограничена только ресурсами хоста.

Во втором случае ресурсы потребляются только в том случае, когда виртуальная машина запущена. Место на хранилище данных требуется только для того, чтобы сохранить изменения в виртуальных дисках. Однако виртуальная машина может работать медленно, поскольку хост работает с виртуальными дисками не напрямую, а через агент, который считывает данные с резервной копии. Кроме того, виртуальная машина является временной. Сделать машину постоянной можно только для ESXi.

5.8.1 Преобразование в виртуальную машину в плане резервного копирования

Можно настроить преобразование в виртуальную машину с любой резервной копии или хранилища репликации, которое присутствует в плане резервного копирования. Преобразование будет выполняться после каждого резервного копирования или репликации.

Чтобы выполнить преобразование, необходимо иметь хост ESXi или Hyper-V и агент резервного копирования (агент для VMware или агент для Hyper-V), который управляет этим хостом.

Обратите внимание на следующие ограничения:

- Агент для VMware (Windows) и агент для Hyper-V не могут преобразовать резервные копии, которые хранятся в системе NFS
- Резервные копии, которые хранятся в Зона безопасности, могут быть преобразованы только агентом, который выполняется та той же машине.

Настройка преобразования в виртуальную машину в плане резервного копирования

1. Определите, с какого хранилища резервных копий необходимо выполнить преобразование.
2. На панели плана резервного копирования под этим хранилищем щелкните **Преобразовать в виртуальную машину**.
3. Включите параметр **Преобразование**.
4. В поле **Преобразовать в** выберите тип целевой виртуальной машины. Можно выбрать один из следующих вариантов:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
5. Щелкните **Хост**, выберите целевой хост, а затем укажите новый шаблон имени машины.

   Имя по умолчанию — **[Имя машины]_converted**.
6. [Необязательно] Щелкните **Агенты, которые будут выполнять преобразование** и выберите агент.
7. [Дополнительно] Можно также выполнить следующие действия:
   - Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
   - Измените режим распределения ресурса дисков. По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.
8. Нажмите кнопку **Готово**.

5.9 Репликация

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

В данном разделе описана репликация резервных копий, являющаяся частью плана резервного копирования. Информацию о создании отдельного плана репликации см. в разделе «Обработка данных Off-host» (стр. 162).

Если включить репликацию резервных копий, то каждая резервная копия копируется в другое хранилище сразу же после создания. Если более ранние резервные копии не были реплицированы (например, из-за сбоя сетевого подключения), программа также реплицирует все резервные копии, появившиеся после последней успешной репликации.

Реплицированные резервные копии не зависят от резервных копий, оставшихся в исходном хранилище и наоборот. Можно восстановить данные из любой резервной копии без доступа к другим хранилищам.

Примеры использования

- **Надежное аварийное восстановление**

  Храните резервные копии локально (для немедленного восстановления) и удаленно (чтобы защитить резервные копии при отказе локального хранилища данных или стихийных бедствиях)
- **Использование облачного хранилища данных для защиты данных при стихийных бедствиях**

  Реплицируйте резервные копии в облачное хранилище данных, передав только изменения данных.
- **Сохранение только последних точек восстановления**

  Удалите старые резервные копии из быстродействующего запоминающего устройства в соответствии с правилами резервного копирования, чтобы без необходимости не использовать емкость хранения данных.

Поддерживаемые расположения

Можно выполнить репликацию резервной копии *из* любого указанного ниже расположения:

- Локальная папка
- Сетевая папка
- Зона безопасности
- SFTP-сервер
- Хранилище под управлением узла хранения

Можно выполнить репликацию резервной копии *в* любое указанное ниже расположение:

- Локальная папка
- Сетевая папка
- Облачное хранилище данных
- SFTP-сервер
- Хранилище под управлением узла хранения
- Ленточное устройство

Включение репликации резервных копий

1. На панели плана резервного копирования нажмите **Добавить хранилище**.

   Элемент управления **Добавить хранилище** отображается только в том случае, если поддерживается репликация *из*последнего выбранного хранилища.
2. Укажите хранилище, в котором будет проведена репликация резервных копий.
3. [Необязательно] В поле **Срок хранения** измените правила хранения для указанного хранилища, как описано в разделе «Правила хранения» (стр. 98).
4. [Необязательно] В поле **Преобразовать в VM**укажите настройки преобразования в виртуальную машину, как описано в «Преобразование в виртуальную машину» (стр. 102).
5. [Необязательно] Повторите шаги 1–4 для всех хранилищ, где необходимо реплицировать резервные копии. Можно использовать до пяти последовательных хранилищ (включая основное).

5.9.1 Рекомендации для пользователей с лицензией Advanced

Совет

Можно настроить репликацию резервных копий *из* облачного хранилища данных путем создания отдельного плана репликации. Дополнительную информацию см. в разделе «Обработка данных Off-host» (стр. 162).

Ограничения

- Репликация резервных копий *из* хранилища, управляемого узлом хранения, на локальную папку не поддерживается. Локальной папкой называется папка на машине с агентом, создавшим резервную копию.
- Репликация резервных копий *в* управляемое хранилище с включенной дедупликацией не поддерживается для резервных копий, имеющих формат резервной копии (стр. 113) **Версии 12**.

Какая машина выполняет операцию?

Репликация резервной копии *из* любого хранилища инициируется агентом, создавшим резервную копию и выполняется:

- Этим агентом, если хранилище *не* управляется узлом хранения.
- Соответствующим узлом хранения, если хранилище является управляемым. Однако репликация резервной копии из управляемого хранилища в облачное хранилище данных выполняется агентом, создавшим резервную копию.

Как следует из вышеуказанного, операция будет выполнена только в том случае, если машина с агентом включена.

Репликация резервных копий между управляемыми хранилищами

Репликация резервной копии из одного управляемого хранилища в другое выполняется узлом хранения.

Если для целевого хранилища включена дедупликация (возможно, на другом узле хранения), узел хранения источника отправляет только те блоки данных, которые отсутствуют в целевом хранилище. Другими словами, узел хранения, как и агент, выполняет дедупликацию в источнике. Это помогает уменьшить сетевой трафик при репликации данных между географически разделенными узлами хранения.

5.10 Запуск резервного копирования вручную

1. Выберите машину, для которой задан хотя бы один план резервного копирования.
2. Нажмите кнопку **Резервное копирование**.
3. Если применено несколько планов, выберите один из них.
4. Выполните одно из следующих действий:
   - Для запуска инкрементного резервного копирования нажмите **Запустить сейчас**. Это единственная доступная опция при резервном копировании в облачное хранилище.
   - Для запуска полного резервного копирования нажмите стрелочку на кнопке **Запустить сейчас**, после чего выберите **Полное**.
   - Для запуска дифференциального резервного копирования нажмите стрелочку на кнопке **Запустить сейчас**, после чего выберите **Дифференциальное**. Этот параметр отображается только в том случае, если одновременно соблюдены несколько условий.
     - Используется схема резервного копирования **Пользовательская** или «Дед-отец-сын» (**GFS**).
     - Репликация в облачное хранилище данных не поддерживается.

Первая резервная копия, созданная по плану резервного копирования, всегда является полной.

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

5.11 Параметры резервного копирования

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Чтобы изменить параметры резервного копирования, щелкните значок шестерни рядом с именем плана резервного копирования и нажмите кнопку **Параметры резервного копирования**.

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	Windows

	Резервное копирование на уровне дисков			Резервное копирование на уровне файлов			Виртуальные машины		SQL и Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Windows
Оповещения (стр. 109)	+	+	+	+	+	+	+	+	+
Консолидация резервных копий (стр. 109)	+	+	+	+	+	+	+	+	–
Имя файла резервной копии (стр. 110)	+	+	+	+	+	+	+	+	+
Формат резервной копии (стр. 113)	+	+	+	+	+	+	+	+	+
Проверка резервных копий (стр. 114)	+	+	+	+	+	+	+	+	+
Условия запуска резервного копирования (стр. 115)	+	+	–	+	+	–	+	+	+
Функция Changed Block Tracking (CBT) (стр. 115)	+	–	–	–	–	–	+	+	–
Способ резервного копирования кластера (стр. 116)	–	–	–	–	–	–	–	–	+
Уровень сжатия (стр. 117)	+	+	+	+	+	+	+	+	+
Уведомления по электронной почте (стр. 117)	+	+	+	+	+	+	+	+	+
Обработка ошибок (стр. 118)									
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 (стр. 119)	+	+	+	–	–	–	–	–	–
Фильтры файлов (стр. 119)	+	+	+	+	+	+	+	+	–

	Резервное копирование на уровне дисков			Резервное копирование на уровне файлов			Виртуальные машины		SQL и Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Windows
Моментальные снимки резервных копий на уровне файлов (стр. 121)	–	–	–	+	+	+	–	–	–
Безопасность на уровне файлов (стр. 121)	–	–	–	+	–	–	–	–	–
Сокращение журнала (стр. 122)	–	–	–	–	–	–	+	+	Только SQL
Создание моментальных снимков LVM (стр. 122)	–	+	–	–	–	–	–	–	–
Точки подключения (стр. 122)	–	–	–	+	–	–	–	–	–
Многотомные моментальные снимки (стр. 123)	+	–	–	+	–	–	–	–	–
Производительность (стр. 124)	+	+	+	+	+	+	+	+	+
Команды до и после процедуры (стр. 125)	+	+	+	+	+	+	+	+	+
Команды до и после захвата данных (стр. 126)	+	+	+	+	+	+	–	–	+
Моментальные снимки оборудования SAN (стр. 128)	–	–	–	–	–	–	+	–	–
Планирование (стр. 129)									
Распределять время запуска по доступному времени	+	+	+	+	+	+	+	+	+
Ограничить число одновременно выполняющихся операций резервного копирования	–	–	–	–	–	–	+	+	–
Посекторное резервное копирование (стр. 129)	+	+	–	–	–	–	+	+	–
Разбиение (стр. 130)	+	+	+	+	+	+	+	+	+
Управление лентами (стр. 130)	+	+	+	+	+	+	+	+	+
Действия при сбое задания (стр. 133)	+	+	+	+	+	+	+	+	+

	Резервное копирование на уровне дисков			Резервное копирование на уровне файлов			Виртуальные машины		SQL и Exchange
	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Windows
Служба теневого копирования томов (VSS) (стр. 133)	+	–	–	+	–	–	–	+	+
Служба теневого копирования томов (VSS) для виртуальных машин (стр. 134)	–	–	–	–	–	–	+	+	–
Еженедельное резервное копирование (стр. 134)	+	+	+	+	+	+	+	+	+
Журнал событий Windows (стр. 135)	+	–	–	+	–	–	+	+	+

5.11.1 Оповещения

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

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли создаваться оповещение, если за указанный период времени планом резервного копирования 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.

5.11.2 Консолидация резервной копии

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

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

- Местом назначения резервной копии является ленточное устройство или облачное хранилище данных.
- Используется схема резервного копирования **Всегда инкрементное (один файл)**.
- Используется формат резервной копии (стр. 113) **Версии 12**.

Резервные копии, хранимые на лентах, невозможно консолидировать. Резервные копии, сохраненные в облачном хранилище данных, а также копии версии 12 и резервные копии в

виде одного файла, всегда консолидированы, поскольку их внутренняя структура позволяет ускорить и упростить консолидацию.

Значение по умолчанию: **Отключено**.

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

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

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

Важно! *Необходимо помнить, что консолидация 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.*

5.11.3 Имя файла резервной копии

Этот параметр определяет имена файлов резервных копий, создаваемые планом резервного копирования.

Эти имена можно увидеть в диспетчере файлов при обзоре хранилища резервной копии.

Что такое файл резервной копии?

В зависимости от схемы резервного копирования и используемого формата резервной копии (стр. 113), каждый план резервного копирования создает один или более файлов в хранилище резервной копии. 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 (традиционный формат)
Формат резервной копии **Версии 12**	Один файл .tibx на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии)	

Все файлы имеют одинаковое имя с добавлением метки времени или порядкового номера, или без них. При создании или редактировании плана резервного копирования можно задать такое имя (называемое именем файла резервной копии).

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 резервного копирования.

Обратите внимание, что можно задать имена файлов резервных копий для хранилищ, обзор которых невозможно выполнить с помощью диспетчера файлов (например, облачного

хранилища данных или ленточного устройства). Это целесообразно в том случае, если требуется просмотр пользовательских имен на вкладке **Резервные копии**.

Где можно просмотреть имена файлов резервных копий?

Выберите вкладку **Резервные копии**, 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 **Резервные копии** в колонке **Имя**.

Ограничения для имени файла резервной копии

- Имя файла резервной копии не должно заканчиваться цифрой.

  Чтобы имя не заканчивалось цифрой, в конце имени резервной копии по умолчанию добавляется буква «A». При создании пользовательского имени убедитесь, что оно не заканчивается цифрой. При использовании переменных имя не должно заканчиваться на переменную, поскольку она может заканчиваться цифрой.
- Имя файла резервной копии не должно содержать следующие символы: **()&?*$<>»:\|/#**, символы окончания строки (**\n**) и знаки табуляции (**\t**).

Имя файла резервной копии по умолчанию

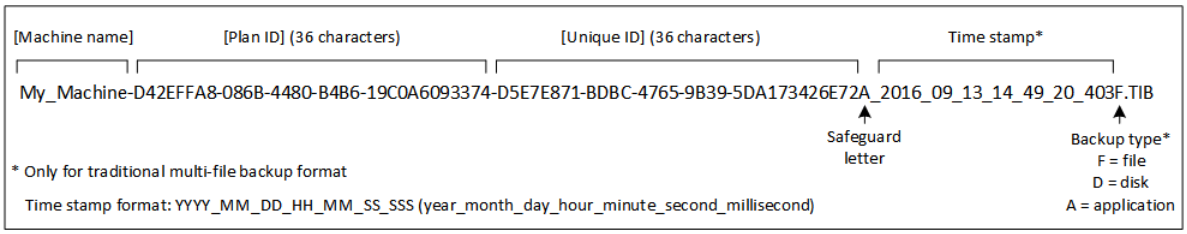
Имя файла резервной копии по умолчанию имеет вид **`[Machine Name]-[Plan ID]-[Unique ID]A`**.

Имя файла резервной копии по умолчанию для почтового ящика имеет вид **`[Mailbox ID]_mailbox_[Plan ID]A`**.

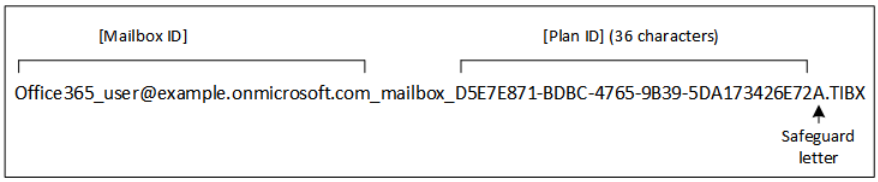
Имя состоит из следующих переменных:

- **`[Machine Name]`** Эта переменная заменяется именем машины (такое же имя отображается в консоли резервного копирования) для всех типов резервных копий данных, за исключением почтовых ящиков Office 365. Для почтовых ящиков Office 365 она заменяется именем участника-пользователя (UPN) почтового ящика.
- **`[Plan ID]`** Эта переменная заменяется уникальным идентификатором плана резервного копирования. При переименовании плана это значение не изменяется.
- **`[Unique ID]`** Эта переменная заменяется уникальным идентификатором выбранной машины или почтового ящика. При изменении имени машины или UPN почтового ящика это значение не изменяется.
- **`[Mailbox ID]`** Эта переменная заменяется UPN почтового ящика.
- **`"A"`** — это защитная буква, которая добавляется для того, чтобы имя файла не заканчивалось цифрой.

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



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



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 **Версии 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
...
```

Для формата **Версии 11** со схемой резервного копирования **Всегда инкрементное (один файл)**:

```
MyBackup.xml
MyBackup.tib
```

Для формата **Версии 11** с другими схемами резервного копирования:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Использование переменных

Кроме переменных, используемых по умолчанию, можно использовать переменную **[Plan name]**, которая заменяется именем плана резервного копирования.

Если выбрано резервное копирование нескольких машин или почтовых ящиков, имя файла резервной копии должно содержать переменную **[Machine Name]**, **[Mailbox ID]** или **[Unique ID]**.

Сравнение имени файла резервной копии и упрощенного именования файлов

Используя обычный текст и/или переменные можно создать такие же имена файлов, как и в более ранних версиях Acronis Backup. Однако упрощенные имена файлов не могут быть созданы заново — в версии 12 имя файла содержит отметку времени, если не используется формат одного файла.

Примеры использования

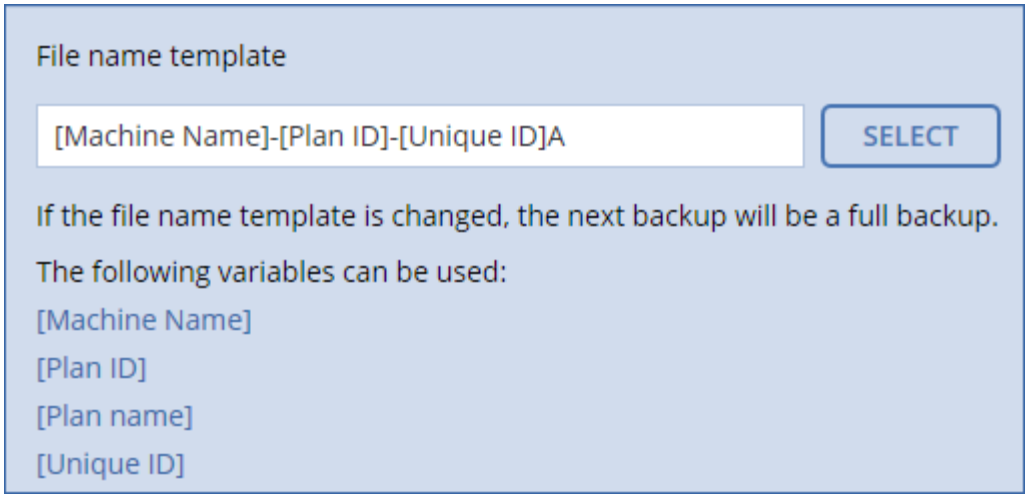
- **Просмотр дружественных к пользователю имен файлов**

При обзоре хранилища с помощью диспетчера файлов легко отличить резервные копии.

- **Продолжение существующей последовательности резервных копий**

  Предположим, что план резервного копирования применен к одной машине и необходимо удалить эту машину из консоли резервного копирования или удалить агента вместе с его настройками конфигурации. После повторного добавления машины или установки агента можно применить план резервного копирования 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 **Обзор** выводит резервные копии в хранилище, выбранном в разделе **Место сохранения резервной копии** на панели плана резервного копирования. Обзор невозможно выполнить за пределами этого хранилища.



- **Переход с предыдущих версий продукта**

  Если при переходе на новую версию не произошел автоматический перенос плана резервного копирования, создайте план заново и примените его к старому файлу резервной копии. Если для резервного копирования выбрана только одна машина, щелкните **Обзор** и выберите требуемую резервную копию. Если для резервного копирования выбраны несколько машин, заново создайте старое имя файла резервной копии с использованием переменных.

5.11.4 Формат резервной копии

Этот параметр определяет формат резервных копий, создаваемых планом резервного копирования. Можно выбрать между новым форматом **(Версия 12**), созданным для быстрого резервного копирования и восстановления, и устаревшим форматом (**Версия 11**), сохраненным для обратной совместимости и специальных случаев. После применения плана резервного копирования этот параметр будет невозможно изменить.

Этот параметр *не* применим к резервным копиям почтового ящика. Резервные копии почтового ящика всегда имеют новый формат.

Значение по умолчанию: **Автоматический выбор**.

Можно выбрать один из следующих вариантов:

- **Автоматический выбор**

Будет использоваться версия 12, за исключением случаев, когда план резервного копирования добавляет резервные копии к уже созданным в продукте более ранней версии.

- **Версия 12**

  В большинстве случаев для быстрого резервного копирования и восстановления рекомендуется новый формат. Каждая цепочка резервных копий (полного или дифференциального копирования, и всех зависящих от них инкрементных резервных копий) сохраняется в один файл .tibx.

  С этим форматом правило хранения **По общему размеру резервных копий** не применимо.

- **Версия 11**

  Устаревший формат должен использоваться в новом плане резервного копирования, который добавляет резервные копии к уже созданным в более ранней версии продукта.

  Также используйте этот формат (с любой схемой резервного копирования, за исключением **Всегда инкрементное (один файл)**) для полного, инкрементного и дифференциального резервного копирования в отдельные файлы.

  Этот формат выбирается автоматически, если местом назначения резервной копии (или местом назначения репликации) является управляемое хранилище с включенной дедупликацией. Если изменить формат на **Версию 12**, резервное копирование не будет выполнено.

Формат резервной копии и файлы резервных копий

Для хранилищ резервных копий, обзор которых можно выполнить с помощью диспетчера фалов (например, локальные или сетевые папки), формат резервных копий определяет количество файлов и их расширение. Можно назначить имена файлов используя опцию имя файла резервной копии (стр. 110). В следующей таблице перечислены файлы, которые не 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 (традиционный формат)
Формат резервной копии **Версии 12**	Один файл .tibx на каждую цепочку резервных копий (полное или дифференциальное резервное копирование и все зависящие от них инкрементные резервные копии)	

5.11.5 Проверка резервной копии

Проверка — это операция по определению возможности восстановления данных из резервной копии. Если этот параметр включен, то каждая резервная копия, созданная в соответствии с планом резервного копирования, проверяется непосредственно после создания.

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 (стр. 223) в среде ESXi или Hyper-V.

5.11.6 Условия запуска резервного копирования

Этот параметр применим в операционных системах Windows и Linux.

Этот параметр определяет поведение программы в том случае, если резервное копирование готово к запуску (наступает запланированное время или событие, указанное в расписании), однако условие (или любое из нескольких условий) не выполнено. Дополнительную информацию об условиях см. в разделе «Условия запуска» (стр. 92).

Значение по умолчанию: **Ожидайте выполнения условий.**

Ждать выполнения условий

С этой настройкой планировщик начинает отслеживать условия и запускает резервное копирование, как только условия будут выполнены. Если условия не выполняются, резервное копирование не запускается.

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. Выберите **Запустить резервное копирование в любом случае через** и укажите временной промежуток. Резервное копирование запустится, если будут выполнены условия ИЛИ истечет максимальное время задержки, в зависимости от того, что наступит раньше.

Пропустить запланированное резервное копирование

Задержка резервного копирования может быть недопустима, например, если данные необходимо копировать точно в заданное время. В этом случае имеет смысл пропустить резервное копирование, а не ждать выполнения условий, особенно, если резервное копирование происходит достаточно часто.

5.11.7 CBT (Changed Block Tracking)

Этот параметр применим для резервных копий на уровне дисков для виртуальных и физических машин, работающих под управлением Windows.

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 непрерывно отслеживаются на уровне блоков. При запуске резервного копирования изменения могут быть незамедлительно сохранены в резервную копию.

5.11.8 Способ резервного копирования кластера

Этот параметр относится к резервной копии баз данных Microsoft SQL Server и Microsoft Exchange Server.

Этот параметр 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.

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. Дополнительные сведения о резервном копировании групп доступности Always On см. в разделе «Защита группы доступности Always On (AAG)» (стр. 199).

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.

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)» (стр. 201).

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 сервера Exchange 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.

5.11.9 Уровень сжатия

Этот параметр определяет уровень сжатия данных при резервном копировании. Доступные уровни: **Отсутствует**, **Обычное**, **Высокое**.

Значение по умолчанию: **Обычное**.

Чем выше уровень сжатия, тем больше времени занимает процесс резервного копирования, но созданная резервная копия занимает меньше места.

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.

5.11.10 Уведомления по электронной почте

Этот параметр позволяет задать уведомления по электронной почте о событиях, которые возникают во время резервного копирования.

Этот параметр доступен только в локальных развертываниях. В облачных развертываниях настройки задаются для каждой учетной записи при ее создании.

Значение по умолчанию: **Использовать глобальные настройки.**

Можно использовать глобальные настройки или переопределить их, заменив на пользовательские значения, относящееся только к данному плану. Глобальные настройки устанавливаются, как описано в разделе «Уведомления по электронной почте» (стр. 283).

Важно! *При изменении глобальных настроек, будут изменены все планы резервного копирования, в которых используются глобальные настройки.*

Прежде чем включать этот параметр, убедитесь, что установлены настройки **Почтовый сервер** (стр. 284).

Порядок настройки уведомлений электронной почты для плана резервного копирования

1. Выберите **Настроить параметры для этого плана резервного копирования**.
2. В поле **Адрес электронной почты получателя** введите адрес электронной почты получателя. Можно указать несколько адресов, разделяя их точкой с запятой.
3. [Необязательно] В поле **Тема** измените тему уведомления по электронной почте.

   Можно использовать следующие переменные:

   - **`[Alert]`**: сводка оповещений
   - **`[Device]`**: имя устройства
   - **`[Plan]`**: название плана, для которого создано оповещение.
   - **`[ManagementServer]`**: имя хоста машины, на которой установлен сервер управления.
   - **`[Unit]`**: название отдела, которому принадлежит машина.

   Тема по умолчанию: **`[Alert]` устройство: `[Device]`План: `[Plan]`**
4. Установите флажки для событий, о которых необходимо получать уведомления. Их можно выбрать из списка всех оповещений, которые возникают во время резервного копирования, сгруппированных по степени серьезности.

5.11.11 Обработка ошибок

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

В случае ошибки повторите операцию

Значение по умолчанию: **включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены в случае, если операция будет успешно выполнена, ИЛИ после указанного максимального числа попыток.

Например, если место назначения резервной копии в сети станет недоступным, программа будет выполнять попытки подключения каждые 30 секунд, но не более 30 раз. Попытки будут прекращены, когда подключение будет восстановлено ИЛИ число попыток достигнет указанного максимума.

Примечание. *Если облачное хранилище данных выбрано в качестве первичного или вторичного назначения, для параметра автоматически устанавливается значение* ***Включено****.* ***Количество попыток: 300****.*

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

Значение по умолчанию: **включено**.

В режиме без вывода сообщений ситуации, требующие вмешательства пользователя, разрешаются автоматически (за исключением обработки поврежденных секторов, что задается отдельным параметром). Если операция не может быть продолжена без вмешательства

пользователя, она не будет выполнена. Дополнительные сведения об операции, включая информацию об ошибках (если они есть), см. в журнале операций.

Пропуск поврежденных секторов

Значение по умолчанию: **Отключено**.

Если этот параметр отключен, каждый раз, когда встречается поврежденный сектор, действию резервного копирования будет назначено состояние **Требуется вмешательство пользователя**. Чтобы создать резервную копию данных с диска, который быстро выходит из строя, включите параметр пропуска поврежденных секторов. Резервное копирование неповрежденных данных будет выполнено, после чего можно подключить резервную копию диска и извлечь исправные файлы на другой диск.

В случае ошибки при создании моментального снимка виртуальной машины повторите попытку

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 в случае, если операция будет успешно выполнена, ИЛИ после указанного максимального числа попыток.

5.11.12 Быстрое инкрементное или дифференциальное резервное копирование

Этот параметр работает для инкрементных и дифференциальных резервных копий на уровне дисков.

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.

5.11.13 Фильтры файлов

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

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

Включение фильтров файлов

1. Выберите данные для резервного копирования.
2. Щелкните значок шестеренки рядом с именем плана резервного копирования и выберите **Параметры резервного копирования**.
3. Выберите **Фильтры файлов**.
4. Воспользуйтесь любыми из перечисленных ниже вариантов.

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*** *(стр. 113) 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**

Две звездочки (*) замещают 0 или несколько символов в имени или пути файла, включая символ косой черты. Например, критерий ****/Docs/**.txt** соответствует всем TXT-файлам во всех подпапках всех папок **Docs**.

Вопросительный знак (?) замещает в имени файла ровно один символ. Например, условие **Doc?.txt** включает в себя файлы **Doc1.txt** и **Docs.txt**, но не включает файлы **Doc.txt** и **Doc11.txt**

Исключить скрытые файлы и папки

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.

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.

Совет *Просмотреть атрибуты файла или папки можно в их свойствах или с помощью команды attrib. Дополнительные сведения можно получить в центре справки и поддержки Windows.*

5.11.14 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: **Использовать снимок, если это возможно**.

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.

5.11.15 Средства безопасности на уровне файлов

Этот параметр действует только для резервной копии на уровне файлов в Windows.

Этот параметр определяет, должны ли сохраняться резервные копии разрешений NTFS вместе с файлами.

Значение по умолчанию: **включено.**

Если этот параметр включен, резервные копии файлов и папок создаются с исходными правами на чтение, запись и выполнение файлов для каждого пользователя и каждой группы. При восстановлении файла или папки с ограниченными разрешениями на машине, где нет учетной записи пользователя, указанного в разрешениях, такой файл может оказаться недоступным для чтения или изменения.

Если этот параметр отключен, то восстановленные файлы и папки наследуют разрешения от папки, в которую они восстанавливаются, или с диска, если они восстанавливаются в корневую папку.

В качестве альтернативного варианта можно отключить восстановление (стр. 154) параметров безопасности. Результат будет тот же — файлы будут наследовать разрешения от родительской папки.

5.11.16 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.

5.11.17 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.

5.11.18 Точки подключения

Этот параметр действует только в Windows для резервной копии на уровне файлов любого источника данных, который включает 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 пустой.

  Во время восстановления родительской папки содержимое точки восстановления восстанавливается или нет в зависимости от того, включен ли режим для восстановления **Точек подключения** (стр. 155).
- Если выбрана сама точка подключения или любая папка в подключенном томе, выбранные папки рассматриваются как обыкновенные. Их резервное копирование будет выполняться независимо от параметра **Точки подключения** и восстанавливаться независимо от режима для восстановления **Точек подключения** (стр. 155).

Значение по умолчанию: **отключено**.

Совет. *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 подключаемого тома. Том содержит папки **Папка1** и **Папка2**. Создается план резервного копирования для копирования данных на уровне файлов.

Если установить флажок для тома C и включить параметр **Точки подключения**, в папке **C:\Data1** в резервной копии будут находиться **Папка1** и **Папка2**. При восстановлении данных с резервной копии помните о правильном использовании режима для восстановления **Точек подключения** (стр. 155).

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 **Папка1** или **Папка2**, отмеченные папки будут включены в копию как обыкновенные папки независимо от параметра **Точки подключения**.

5.11.19 Многотомный моментальный снимок

Этот параметр работает только в операционных системах Windows.

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» (стр. 121) 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: **включено**.

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.

5.11.20 Производительность

Приоритет процесса

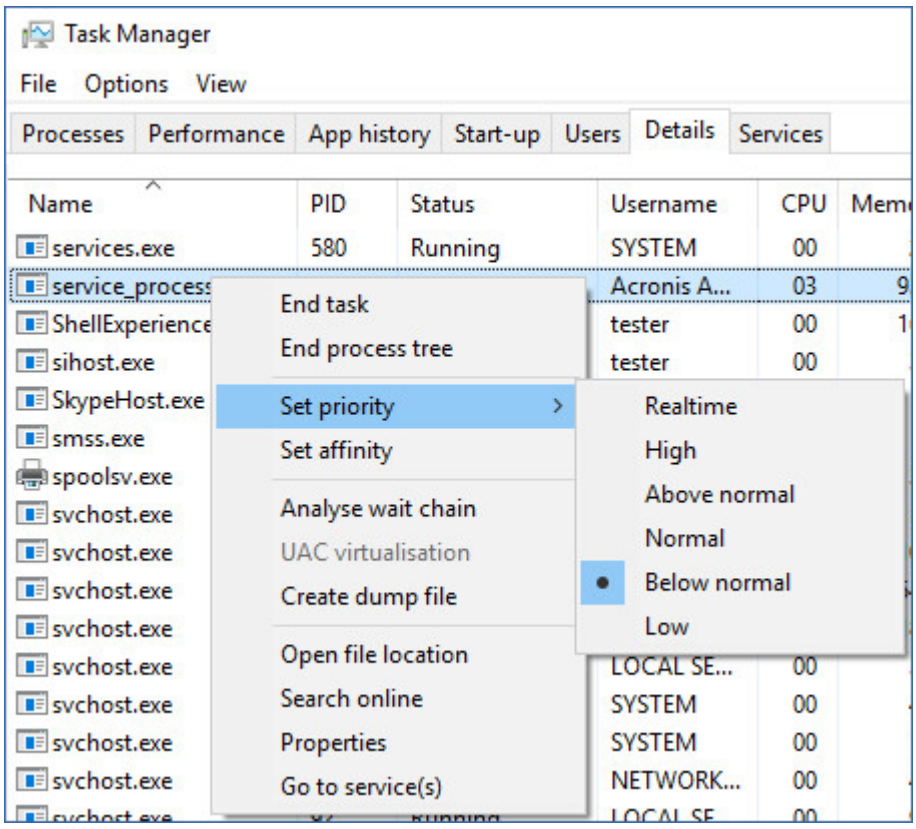
Этот параметр определяет приоритет процесса резервного копирования в операционной системе.

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

Значение по умолчанию: **Низкий** (в Windows, соответствует **Ниже обычного**).

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.



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).

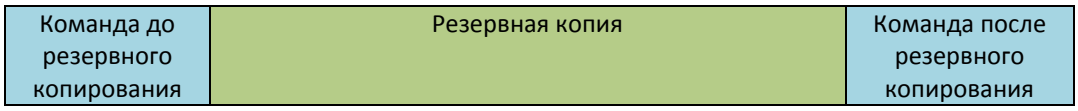
Значение по умолчанию: **Отключено**.

Если этот параметр включен, можно указать максимально разрешенную скорость вывода в КБ/с.

5.11.21 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.



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. Эта возможность может быть полезна, так как операция репликации, заданная в плане резервного копирования, 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).

5.11.21.1 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 выберите 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 папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
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.

5.11.21.2 Команда после резервного копирования

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

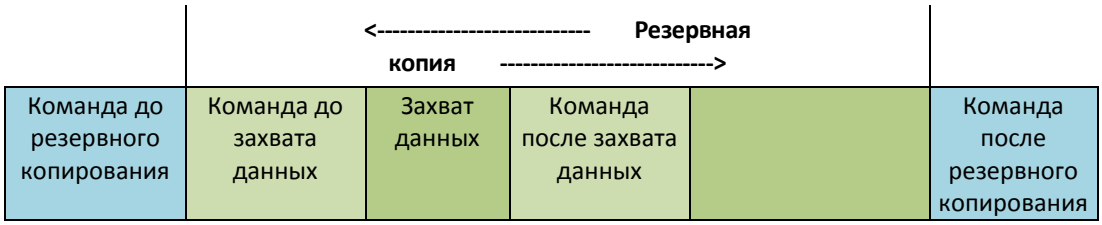
1. Включить переключатель **Выполнение команды после резервного копирования**.
2. В поле **Команда...** введите команду или выберите пакетный файл.
3. В поле **Рабочая папка** укажите путь к папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости 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**.

5.11.22 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.



Если включен параметр (стр. 133) «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.

5.11.22.1 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 выберите 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 папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
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.

5.11.22.2 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 выберите 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 папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
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.

5.11.23 Моментальные снимки оборудования SAN

Эта опция эффективна для резервного копирования виртуальных машин VMware ESXi.

Значение по умолчанию: **Отключено**.

Этот параметр определяет, будет ли использоваться технология моментальных снимков SAN при выполнении резервного копирования.

Если эта опция отключена, содержимое виртуального диска будет прочитано с моментального снимка VMware. Моментальный снимок хранится все время резервного копирования.

Если этот параметр включен, содержимое виртуального диска будет прочитано с моментального снимка SAN. Моментальный снимок VMware будет создан и сохранен на небольшое время, чтобы привести виртуальные диски в согласованное состояние. Если чтение с моментального снимка SAN невозможно, резервное копирование завершится ошибкой.

Перед подключением этой опции проверьте и выполните все требования, указанные в разделе «Использование моментальных снимков оборудования SAN» (стр. 234).

5.11.24 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:

- Локальное развертывание: **Начинать все операции резервного копирования строго по расписанию.**
- Облачное развертывание: **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 резервного копирования к машине и остается неизменной до тех пор, пока в плане резервного копирования 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 резервного копирования применен к нескольким виртуальным машинам. Этот параметр определяет, для скольких виртуальных машин агент может одновременно выполнять резервное копирование при выполнении заданного плана резервного копирования.

  Если в соответствии с планом резервного копирования 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.

  Резервное копирование физических машин запустится точно в соответствии с расписанием.

5.11.25 Резервное копирование в посекторном режиме

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» (стр. 117) задано значение **Отсутствует**). Программное обеспечение автоматически перейдет к посекторному резервному копированию для дисков с нераспознанными или неподдерживаемыми файловыми системами.

5.11.26 Разбиение

Этот параметр применим для следующих схем резервного копирования: **Всегда полное**, **Еженедельно полное, ежедневно инкрементное**, **/Ежемесячное полное, еженедельное дифференциальное, дневное инкрементное (GFS)/** и **Пользовательские**.

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

Значение по умолчанию: **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.

5.11.27 Управление лентами

Эти параметры применимы только при резервном копировании на ленточное устройство.

Включить восстановление файлов из резервных копий дисков, хранящихся на лентах

Значение по умолчанию: **Отключено**.

Если этот флажок установлен, при каждом резервном копировании программа создает дополнительные файлы на жестком диске машины, к которой подсоединено ленточное устройство. Восстановление файлов из резервных копий дисков возможно до тех пор, пока эти дополнительные файлы будут в порядке. Файлы автоматически удаляются при стирании (стр. 274), удалении (стр. 275) или перезаписи ленты с соответствующими резервными копиями.

Дополнительные файлы располагаются в следующих местах:

- В ОС Windows XP и Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- В ОС Windows Vista и более поздних версиях Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- В ОС Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

Пространство, занимаемое этими дополнительными файлами, зависит от количества файлов в соответствующей резервной копии. Для полной резервной копии диска, содержащей примерно 20 000 файлов (обычная резервная копия диска рабочей станции), дополнительные файлы занимают около 150 МБ. Полная резервная копия сервера, содержащая 250 000 файлов,

может создать около 700 МБ дополнительных файлов. Поэтому, если вы уверены, что восстановление отдельных файлов не потребуется, можно не устанавливать этот флажок для экономии дискового пространства.

При настройке резервного копирования на уровне дисков с поддержкой приложений (стр. 203) флажок **Включить восстановление файлов из образов дисков на лентах** устанавливается автоматически. Его можно снять, только изменив место назначения резервной копии или отключив резервное копирование с поддержкой приложений.

Если дополнительные файлы не были созданы в процессе резервного копирования или были удалены, их все равно можно создать, повторно просканировав (стр. 273) ленты, на которых хранится резервная копия.

Вернуть ленту в слот после каждого успешного создания резервной копии каждой машины

Значение по умолчанию: **Включено**.

Если этот параметр отключен, лента будет оставаться на носителе после завершения операции с лентой. В ином случае программное обеспечение вернет ленту в слот, в котором она находилась до операции. Если, согласно плану резервного копирования, за созданием резервной копии следуют другие операции (например, ее проверка или репликация в другое хранилище), ленты будет возвращены в слот после завершения этих операций.

Если включен этот параметр, а также параметр **Извлечь ленты после успешного резервного копирования каждой машины**, лента будет извлечена.

Извлечь ленты после каждого успешного резервного копирования каждой машины

Значение по умолчанию: **Отключено**.

Если установлен этот флажок, программа будет извлекать ленты после любого успешного резервного копирования /каждой машины/. Если, согласно плану резервного копирования, за созданием резервной копии следуют другие операции (например, ее проверка или репликация в другое хранилище), ленты будут извлечены после завершения этих операций.

Перезаписать ленту в автономном ленточном устройстве при создании полной резервной копии

Значение по умолчанию: **Отключено**.

Если этот параметр включен, лента, вставленная в устройство, будет перезаписываться каждый раз при создании полной резервной копии.

Использовать наборы лент в пуле лент, выбранных для резервного копирования

Значение по умолчанию: **Отключено**.

Ленты внутри одного пула можно объединить в так называемые **наборы лент**.

Если оставить этот параметр отключенным, резервное копирование данных будет выполнено на все ленты, принадлежащие пулу. Если включить этот параметр, можно разделить резервные копии в соответствии с предварительно определенными или пользовательскими правилами.

- **Используйте отдельный набор лент для каждого**

При выборе этого варианта возможна организация наборов лент в соответствии с предопределенным правилом. Например, возможно указать отдельные наборы лент для каждого дня недели или хранить резервные копии каждой машины на отдельном наборе лент.

- **Укажите настраиваемое правило для наборов лент**

  При выборе этого варианта возможно указание собственного правила для организации наборов лент. Правило может содержать следующие переменные:

Синтаксис переменной	**Описание переменной**	**Доступные значения**
[Resource Name]	Резервные копии на каждой машине будут храниться на отдельном наборе лент.	Имена машин, зарегистрированных на сервере управления.
[Backup Type]	Полные, инкрементные и дифференциальные резервные копии будут храниться на отдельных наборах лент.	**full**, **inc**, **diff**
[Resource Type]	Резервные копии каждого типа машин будут храниться на отдельном наборе лент.	**Server essentials**, **Server**, **Workstation**, **Physical machine**, **VMware Virtual Machine**, **Virtual-PC Virtual Machine**, **Virtual Server Virtual Machine**, **Hyper-V Virtual Machine**, **Parallels Virtual Machine**, **XEN Virtual Machine**, **KVM Virtual Machine**, **RHEV Virtual Machine**, **Parallels Cloud Virtual Machine**
[Day]	Резервные копии, созданные в каждый день месяца, будут храниться на отдельном наборе лент.	**01**, **02**, **03**, ..., **31**
[Weekday]	Резервные копии, созданные в каждый день недели, будут храниться на отдельном наборе лент.	**Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**
[Month]	Резервные копии, созданные в каждый месяц года, будут храниться на отдельном наборе лент.	**January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November**, **December**
[Year]	Резервные копии, созданные за год, будут храниться на отдельном наборе лент.	**2017**, **2018**, ...

  Например, при указании правила **[Resource Name]-[Backup Type]** будет создан отдельный набор лент для каждой полной, инкрементной и дифференциальной резервной копии каждой машины, к которой применим план резервного копирования.

Возможно указать набор лент (стр. 275) для отдельных лент. В данном случае программное обеспечение сначала запишет резервные копии на ленты, значение набора лент которых совпадает со значением выражения, указанного в плане резервного копирования. После чего при необходимости будут взяты другие ленты этого пула. Если пул пополняемый, после этого будут использованы ленты из пула **Свободные ленты**.

Например, при указании набора лент **Monday** для ленты 1, **Tuesday** для ленты 2 и т. д. и указании **[Weekday]** в параметрах резервного копирования надлежащая лента будет использована в соответствующий день недели.

5.11.28 Действия при сбое задания

Этот параметр определяет поведение программы при сбое запланированного плана резервного копирования. Этот параметр не действует, если план резервного копирования запущен вручную.

Если этот параметр включен, то программа попытается еще раз выполнить план резервного копирования. 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**.

5.11.29 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 SharePoint или Active Directory).

Отключите этот параметр, если база данных несовместима с VSS. В этом случае моментальные снимки создаются быстрее, однако не гарантируется целостность приложений, транзакции которых не завершены на момент создания моментального снимка. Можно использовать Команды до и после захвата данных (стр. 126), чтобы обеспечить согласованность данных, для которых выполняется резервное копирование. Например, укажите команды до захвата данных, которые приостановят работу базы данных и перенесут содержимое всех временных хранилищ для обеспечения корректного выполнения транзакций, укажите команды после захвата данных, которые возобновят операции базы данных после выполнения моментального снимка.

Примечание. *Если этот параметр включен, резервное копирование файлов и папок, указанных в ключе реестра* ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot,*** *не выполняется. В частности, не выполняется резервное копирование файлов данных Outlook (.ost), поскольку они указаны в значении* ***OutlookOST*** *данного ключа.*

Включить полное резервное копирование VSS

Если этот параметр включен, журналы Microsoft Exchange Server и других приложений, поддерживающих VSS (кроме Microsoft SQL Server), будут сокращаться каждый раз после полного, инкрементного или дифференциального резервного копирования на уровне дисков.

Значение по умолчанию: **Отключено**.

Оставьте параметр отключенным в следующих случаях:

- Если для резервного копирования данных Exchange Server используется агент для Exchange или ПО сторонних производителей. В этом случае усечение журналов помешает последующему резервному копированию журналов транзакций.
- Если для резервного копирования данных SQL Server используется программное обеспечение сторонних производителей. Программа стороннего производителя будет воспринимать получившуюся резервную копию диска как «свою собственную» полную резервную копию. В результате следующее дифференциальное резервное копирование данных SQL Server завершится ошибкой. Резервное копирование будет завершаться ошибкой, пока программа стороннего производителя не создаст следующую собственную полную резервную копию.
- Если на машине работают другие VSS-совместимые приложения, журналы которых необходимо хранить по какой-либо причине.

При включении этого параметра не происходит усечения журналов Microsoft SQL Server. Чтобы сократить журнал SQL Server после выполнения резервного копирования, включите параметр резервного копирования Сокращение журнала (стр. 122).

5.11.30 Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр определяет, следует ли создавать замороженные моментальные снимки виртуальных машин. Чтобы создать замороженный моментальный снимок, программное обеспечение резервного копирования применяет VSS в виртуальной машине, используя VMware Tools или Hyper-V Integration Services.

Значение по умолчанию: **включено**.

Если этот параметр включен, то транзакции всех приложений с поддержкой VSS, которые запущены на виртуальной машине, завершаются перед созданием моментального снимка. Если после нескольких попыток, количество которых определено параметром «Обработка ошибок» (стр. 118), 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.

5.11.31 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**.

5.11.32 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**). Можно фильтровать события, записываемые в журнал.

Значение по умолчанию: **Отключено**.

6 Восстановление

6.1 Восстановление: памятка

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

Объект восстановления	Метод восстановления
Физическая машина (Windows или Linux)	Использование веб-интерфейса (стр. 136) Использование загрузочного носителя (стр. 141)
Физическая машина (Mac)	Использование загрузочного носителя (стр. 141)
Виртуальная машина (VMware или Hyper-V)	Использование веб-интерфейса (стр. 140) Использование загрузочного носителя (стр. 141)
Конфигурация ESXi	Использование загрузочного носителя (стр. 150)
Файлы и папки	Использование веб-интерфейса (стр. 145) Загрузка файлов из облачного хранилища данных (стр. 146) Использование загрузочного носителя (стр. 149) Извлечение файлов из локальных резервных копий (стр. 149)
Состояние системы	Использование веб-интерфейса (стр. 150)
Базы данных SQL	Использование веб-интерфейса (стр. 205)
Базы данных Exchange	Использование веб-интерфейса (стр. 208)
Почтовые ящики Exchange	Использование веб-интерфейса (стр. 211)
Почтовые ящики Office 365	Использование веб-интерфейса (стр. 219)
Базы данных Oracle	Использование инструмента Oracle Explorer (стр. 221)

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.

6.2 Создание загрузочных носителей

Загрузочный носитель — это компакт-диск, DVD-диск, флэш-накопитель USB или другой съемный носитель, с помощью которого можно запустить агент, не используя операционную систему. Основная задача, для которой применяются такие носители, — восстановление операционной системы, которую не удается загрузить.

Мы настоятельно рекомендуем создать и протестировать загрузочный носитель сразу же после первого создания резервных копий дисков. Кроме того, рекомендуется повторно создавать носитель после каждого серьезного обновления агента резервного копирования.

С помощью одного носителя можно восстановить как ОС Windows, так и Linux. Чтобы восстановить macOS, создайте отдельный носитель на машине с macOS.

Создание загрузочного носителя в Windows и Linux

1. Загрузите ISO-файл загрузочного носителя. Чтобы загрузить файл, щелкните значок учетной записи в правом верхнем углу и выберите **Загрузки** > **Загрузочный носитель**.
2. Выполните любое из следующих действий:
   - Запишите компакт- или DVD-диск, используя ISO-файл.
   - Создайте загрузочный флэш-накопитель USB, используя ISO-файл и один из бесплатных инструментов, доступных в Интернете.

     Для машин с UEFI используйте `ISO to USB` или RUFUS, для машин с BIOS — `Win32DiskImager`. В Linux можно воспользоваться утилитой `dd`.
   - Подключите ISO-файл в качестве CD/DVD-дисковода к виртуальной машине, которую требуется восстановить.

Кроме того, можно создать загрузочный носитель, используя Мастер создания загрузочных копий (стр. 167).

Порядок создания 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.

6.3 Восстановление машины

6.3.1 Физическая машина

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

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

- macOS
- 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

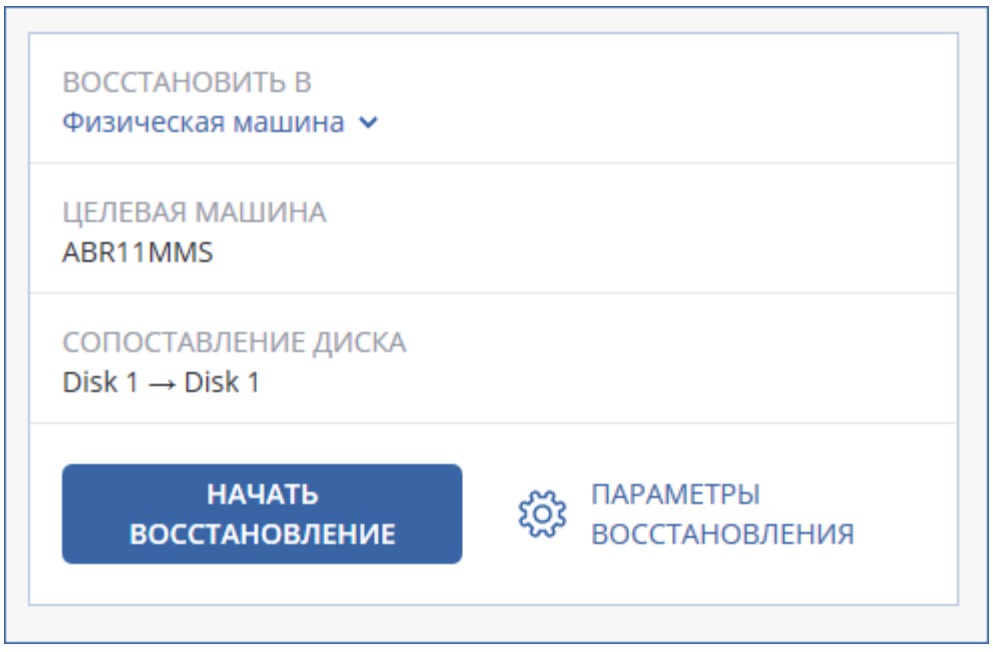
1. Выберите машину, для которой есть резервная копия.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   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 «Резервные копии» (стр. 158).
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя» (стр. 141).
4. Последовательно выберите пункты **Восстановление** > **Вся машина**.

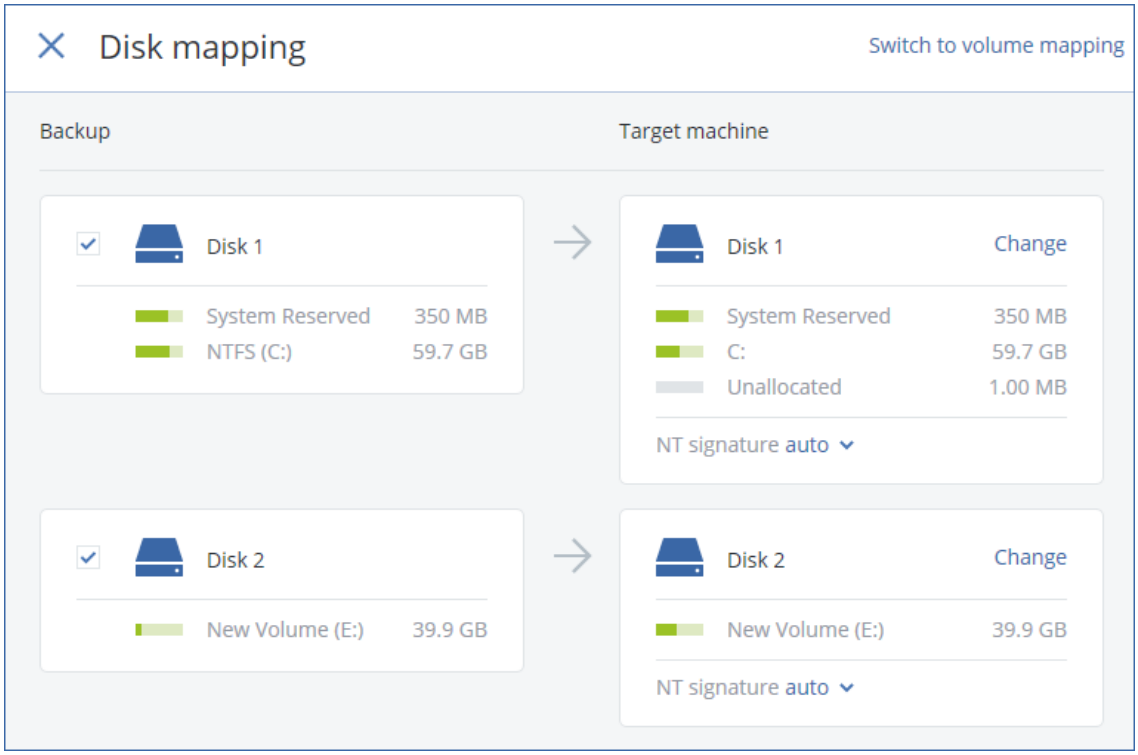
   Программное обеспечение автоматически сопоставит диски из резервной копии с дисками целевой машины.

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



5. Если результат сопоставления вас не удовлетворяет или если выполнить сопоставление не удалось, нажмите **Сопоставление дисков**, 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. Нажмите кнопку **Запуск восстановления**.
7. Подтвердите перезапись дисков версиями из резервной копии. Укажите, следует ли автоматически перезапустить машину.

Ход восстановления отображается на вкладке **Действия**.

6.3.2 Восстановление физической машины в виртуальную

В этом разделе описано восстановление физической машины в качестве виртуальной с использованием веб-интерфейса. Эту операцию можно выполнить, если установлен и зарегистрирован хотя бы один агент для VMware или агент для Hyper-V.

Дополнительную информацию о миграции P2V см. в разделе «Миграция машины» (стр. 245).

Восстановление физической машины как виртуальной

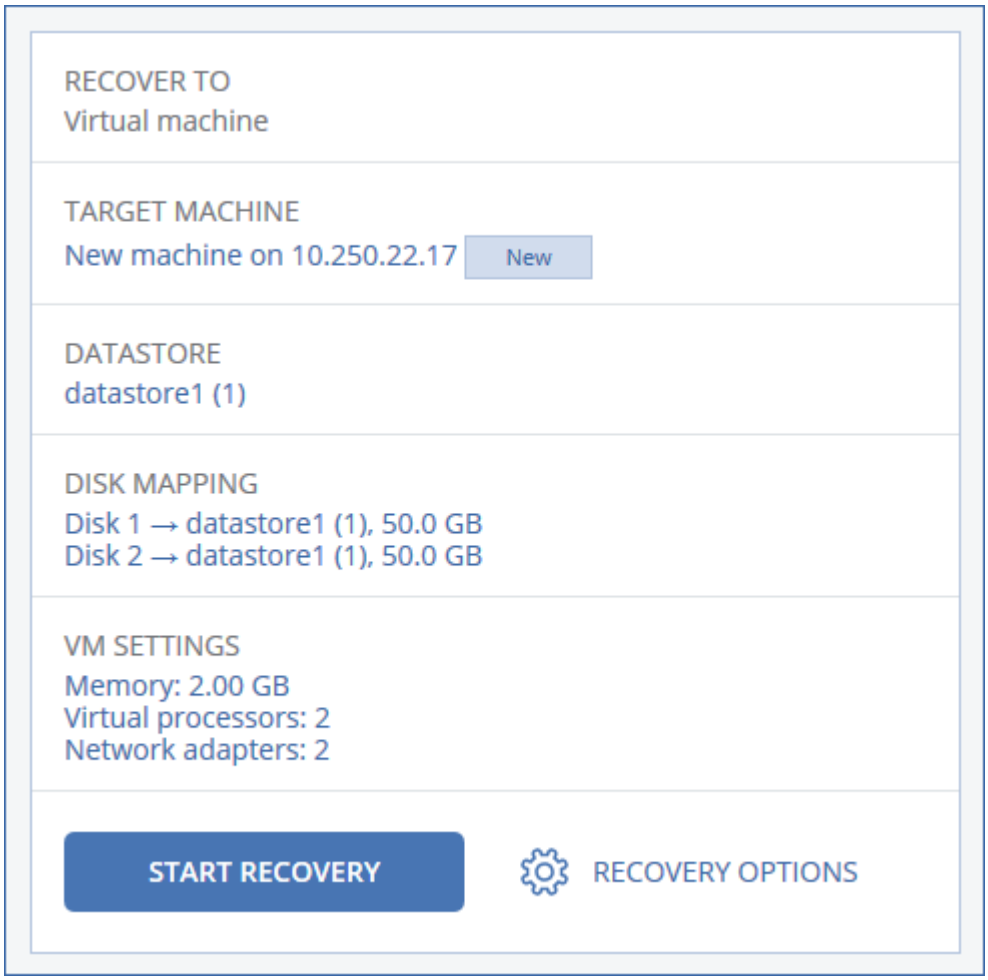
1. Выберите машину, для которой есть резервная копия.
2. Щелкните **Восстановление**.
3. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.

   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 «Резервные копии» (стр. 158).
   - Восстановите машину, как описано в теме «Восстановление дисков с помощью загрузочного носителя» (стр. 141).

4. Последовательно выберите пункты **Восстановление** > **Вся машина**.
5. В поле **Восстановить в** выберите пункт **Виртуальная машина**.
6. Щелкните **Целевая машина**.
   a. Выберите гипервизор (**VMware ESXi** или **Hyper-V**).

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



8. Нажмите кнопку **Запуск восстановления**.

9. При восстановлении в существующую виртуальную машину подтвердите перезапись дисков.

Ход восстановления отображается на вкладке **Действия**.

6.3.3 Виртуальная машина

Восстановление на виртуальную машину выполняется, только когда машина остановлена. Программа останавливает машину без запроса. После завершения восстановления необходимо запустить машину вручную.

Это поведение можно изменить, используя параметр восстановления «Управление питанием ВМ» (выберите **Параметры восстановления** > **Управление питанием ВМ**).

Восстановление виртуальной машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, выберите **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 158).
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.

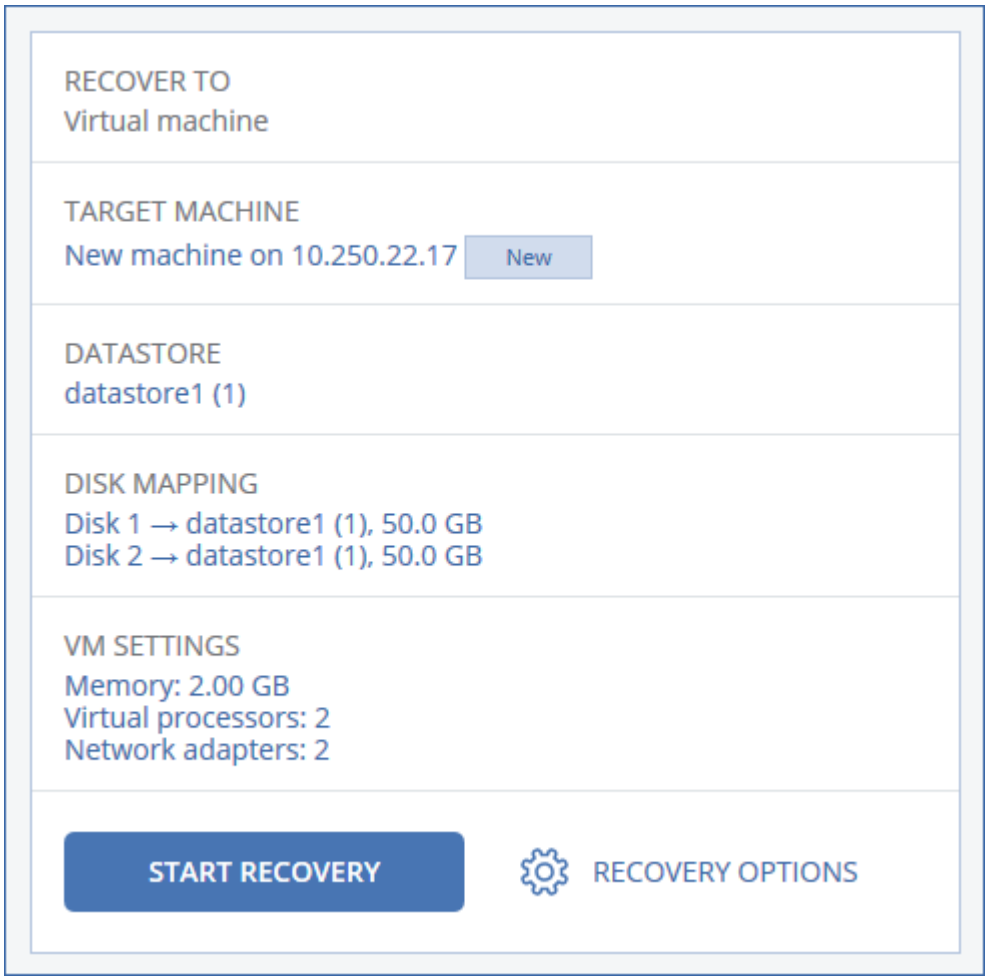
   Восстановление в физическую машину возможно только в том случае, если конфигурация целевой машины в точности соответствует конфигурации диска в данной резервной копии.

   Если это имеет место, продолжите с шага 4 в разделе «Физическая машина» (стр. 136). В противном случае рекомендуется выполнить миграцию V2P, используя загрузочный носитель (стр. 141).
4. 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** или **Hyper-V**).
   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 **ОК**.
5. [Необязательно] При восстановлении в новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
   - Щелкните **Сопоставление дисков**, чтобы выбрать хранилище данных, интерфейс и режим распределения для каждого виртуального диска. Раздел сопоставления также позволяет выбирать отдельные диски для восстановления.

- Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.



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

Ход восстановления отображается на вкладке **Действия**.

6.3.4 Восстановление дисков с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 136).

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. Заново создайте конфигурацию оригинального диска. Инструкции см. по ссылке https://support.apple.com/guide/disk-utility/welcome.
   c. 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, щелкните **Инструменты** > **Прокси-сервер** и укажите имя хоста/IP-адрес и порт прокси-сервера. В противном случае пропустите этот шаг.
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.
   - Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **ОК**, чтобы подтвердить выбор.
8. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
9. В разделе **Содержимое резервной копии** выберите диски, которые нужно восстановить. Нажмите кнопку **ОК**, чтобы подтвердить выбор.
10. В разделе **Место восстановления** программное обеспечение автоматически сопоставит выбранные диски с целевыми.

    Если выполнить сопоставление не удалось или его результат вас не устраивает, сопоставьте диски заново вручную.

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

6.3.5 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 (стр. 143).
5. Нажмите кнопку **ОК**.

6.3.5.1 Universal Restore в Windows

Подготовка

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.

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

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 также выполняет 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.

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 **ОК**.

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.

6.3.5.2 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.

6.4 Восстановление файлов

6.4.1 Восстановление файлов с помощью веб-интерфейса

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. Выберите точку восстановления на вкладке «Резервные копии» (стр. 158) или используйте другие способы восстановления:

   - Загрузка файлов из облачного хранилища данных (стр. 146)
   - Использовать загрузочный носитель (стр. 149)
4. Нажмите **Восстановить** > **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» (стр. 119).

   /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.
8. Нажмите кнопку **Восстановить**.

   В поле **Восстановить в** будет отображаться один из следующих вариантов:

- Машина, на которой изначально были файлы, которые необходимо восстановить (если это машина с агентом).
- Машина, на которой установлен агент для Hyper-V или агент для VMware (если файлы изначально находятся на виртуальной машине) Файлы с виртуальных машин невозможно восстановить на исходную машину.

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
   - 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 восстановления отображается на вкладке **Действия**.

6.4.2 Загрузка файлов из облачного хранилища данных

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

Ограничение: резервные копии состояния системы, баз данных SQL и Exchange недоступны для просмотра.

Загрузка файлов из облачного хранилища данных

1. Выберите машину, для которой была создана резервная копия.
2. Щелкните **Восстановление** > **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 дисков: в разделе **Версии** выберите резервную копию, из 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 и папок.

6. Установите флажки тех элементов, которые необходимо восстановить, и щелкните **Загрузить**.

   Если выбран один файл, он загружается как есть. В противном случае выбранные данные архивируются в ZIP-файл.

7. Выберите место для сохранения данных и нажмите кнопку **Сохранить**.

6.4.3 Проверка подлинности файла с использованием службы нотаризации

Если нотаризация была включена при проведении резервного копирования (стр. 101), можно проверить подлинность файла в резервной копии.

Проверка подлинности

1. Выберите файл, как описано в шагах 1–6 раздела «Восстановление файлов с помощью веб-интерфейса» (стр. 145).
2. Убедитесь, что выбранный файл помечен следующим значком:  . Это означает, что файл нотаризован.
3. Выполните одно из следующих действий:
   - Нажмите **Проверить**.

     Программное обеспечение проверит подлинность файла и отобразит результаты.
   - Нажмите **Получить сертификат**.

     Сертификат, подтверждающий нотаризацию файла, открывается в окне веб-браузера. В окне также есть инструкции, которые позволяют проверить подлинность файла вручную.

6.4.4 Подпись файла с использованием службы ASign

ASign — это служба, позволяющая нескольким пользователям подписывать скопированный файл электронной подписью. Данная функция применима только к резервным копиям, хранящимся в облачном хранилище данных.

Одновременно можно подписать только одну версию файла. Если резервная копия файла создавалась неоднократно, необходимо выбрать версию для подписания, и подписана будет только эта версия.

Например, ASign может быть использована для добавления электронной подписи к следующим файлам:

- арендные или лизинговые договора;
- договора купли-продажи;
- договора о приобретении активов;
- договора займа;
- официальные разрешения;
- финансовые документы;
- страховые документы;
- отказы от ответственности;
- медицинская документация;
- научные исследования;
- сертификаты подлинности продукта;
- соглашения о неразглашении;
- письма о подаче оферты;
- соглашения о конфиденциальности;
- соглашения с независимыми подрядчиками.

Подпись версии файла

1. Выберите файл, как описано в шагах 1–6 раздела «Восстановление файлов с помощью веб-интерфейса» (стр. 145).
2. Убедитесь в правильности выбора даты и времени на левой панели.
3. Нажмите **Подписать эту версию файла**.
4. Укажите пароль для учетной записи облачного хранилища данных, в котором хранится резервная копия. Имя входа учетной записи отображается в окне запроса.

   Интерфейс службы ASign будет открыт в окне веб-браузера.
5. Добавьте других подписантов, указав их адреса электронной почты. Невозможно добавить или удалить подписантов после отправки приглашений, поэтому убедитесь, что в список включены все лица, от которых нужно получить подпись.
6. Щелкните **Пригласить для подписи**, чтобы отправить приглашения подписантам.

   Каждый подписант получит на электронную почту сообщение с запросом подписи. Когда все запрошенные подписанты подпишут файл, он проходит нотаризацию и подписывается в службе нотаризации.

   Вы получите уведомления, когда каждый подписант подпишет файл и весь процесс будет завершен. Доступ к веб-странице ASign можно получить, щелкнув **Просмотреть сведения** в любом полученном сообщении электронной почты.
7. По окончании процесса перейдите на веб-страницу ASign и нажмите кнопку **Получить документ**, чтобы загрузить PDF-документ, который содержит:
   - страница Сертификата подписи с проставленными подписями;
   - Страница журнала аудита с историей действий: время отправки запроса подписантам, время и время проставления каждой подписи для файлов и т. п.

6.4.5 Восстановление файлов с помощью загрузочного носителя

Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 136).

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, щелкните **Инструменты** > **Прокси-сервер** и укажите имя хоста/IP-адрес и порт прокси-сервера. В противном случае пропустите этот шаг.
4. На экране приветствия нажмите кнопку **Восстановить**.
5. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. 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.
   - Чтобы восстановить данные из локальной или сетевой папки, укажите ее в разделе **Локальные папки** или **Сетевые папки**.

   Нажмите кнопку **ОК**, чтобы подтвердить выбор.
7. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
8. В области **Содержимое резервной копии** выберите **Файлы/папки**.
9. Выберите данные, которые необходимо восстановить. Нажмите кнопку **ОК**, чтобы подтвердить выбор.
10. В разделе **Место восстановления** укажите нужную папку. При желании можно запретить перезапись более новых версий файлов или исключить некоторые файлы из списка восстанавливаемых.
11. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
12. Нажмите кнопку **ОК**, чтобы начать восстановление.

6.4.6 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, необходимо установить агент резервного копирования.
- 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, сетевой папке (SMB/CIFS) или в Зоне безопасности.

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 резервного копирования>`
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.

6.5 Восстановление состояния системы

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 восстановления отображается на вкладке **Действия**.

6.6 Восстановление конфигурации ESXi

Чтобы восстановить конфигурацию ESXi, необходим загрузочный носитель на основе Linux. Информацию о том, как создать загрузочный носитель, см. в разделе «Создание загрузочного носителя» (стр. 136).

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. Если резервная копия находится в облачном хранилище данных, доступ к которому выполняется через прокси-сервер, щелкните **Инструменты** > **Прокси-сервер**, а затем укажите имя хоста/IP-адрес прокси-сервера и его порт. В противном случае пропустите этот шаг.
4. На экране приветствия нажмите кнопку **Восстановить**.
5. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. Укажите хранилище резервных копий.

- Укажите папку в разделе **Локальные папки** или **Сетевые папки**.

  Нажмите кнопку **ОК**, чтобы подтвердить выбор.

7. В поле **Показать** выберите **Конфигурации ESXi**.
8. Выберите резервную копию, из которой необходимо восстановить данные. При появлении соответствующего запроса введите пароль для резервной копии.
9. Нажмите кнопку **ОК**.
10. 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.
11. 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**.
12. [Необязательно] В разделе **Сопоставление сети** измените результат автоматического сопоставления виртуальных коммутаторов, присутствующих в резервной копии, с физическими сетевыми картами.
13. [Необязательно] Щелкните **Параметры восстановления**, чтобы указать дополнительные настройки.
14. Нажмите кнопку **ОК**, чтобы начать восстановление.

6.7 Параметры восстановления

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

Доступность параметров восстановления

Набор доступных параметров восстановления зависит от следующих факторов.

- Среда, в которой работает агент, выполняющий восстановление (Windows, Linux, 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 и Hyper-V	Windows
Проверка резервных копий (стр. 152)	+	+	+	+	+	+	+	+	+

	Диски			Файлы				Виртуальные машины	SQL и Exchange
	Windows	Linux	Загрузочный носитель	Windows	Linux	macOS	Загрузочный носитель	ESXi и Hyper-V	Windows
Дата и время для файлов (стр. 153)	–	–	–	+	+	+	+	–	–
Обработка ошибок (стр. 153)	+	+	+	+	+	+	+	+	+
Исключения файлов (стр. 153)	–	–	–	+	+	+	+	–	–
Безопасность на уровне файлов (стр. 154)	–	–	–	+	+	+	+	–	–
Flashback (стр. 154)	+	+	+	–	–	–	–	+	–
Восстановление полного пути (стр. 154)	–	–	–	+	+	+	+	–	–
Точки подключения (стр. 155)	–	–	–	+	–	–	–	–	–
Производительность (стр. 155)	+	+	–	+	+	+	–	+	+
Команды до и после процедуры (стр. 155)	+	+	–	+	+	+	–	+	+
Изменение идентификатора безопасности (стр. 157)	+	–	–	–	–	–	–	–	–
Управление питанием ВМ (стр. 157)	–	–	–	–	–	–	–	+	–
Журнал событий Windows (стр. 157)	+	–	–	+	–	–	–	Только Hyper-V	+

6.7.1 Проверка резервной копии

Этот параметр определяет, выполнять ли проверку резервной копии на повреждения перед восстановлением из нее данных.

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.

6.7.2 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**.

6.7.3 Обработка ошибок

Они позволяют указать, как должны обрабатываться ошибки, возникшие при восстановлении.

В случае ошибки повторите операцию

Значение по умолчанию: **включено. Количество попыток: 30. Интервал между попытками: 30 секунд.**

Если возникла устранимая ошибка, программа будет продолжать попытки выполнить операцию. Задайте временной интервал и количество попыток. Попытки будут прекращены в случае, если операция будет успешно выполнена, ИЛИ после указанного максимального числа попыток.

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.

6.7.4 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.*

6.7.5 Средства безопасности на уровне файлов

Этот параметр действует только для восстановления из резервной копии на уровне файлов в Windows.

Этот параметр определяет, должны ли восстанавливаться разрешения NTFS вместе с файлами.

Значение по умолчанию: **включено**.

Если разрешения NTFS были сохранены при выполнении резервного копирования (стр. 121), можно выбрать восстановление разрешений или наследование файлами их разрешений NTFS из папки, в которую они восстановлены.

6.7.6 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 (например, при восстановлении диска из резервной копии в исходное расположение).

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.

Сравнение данных на уровне блоков — это длительная операция для физических машин. При наличии быстрого подключения к хранилищу резервных копий на восстановление всего диска потребуется меньше времени, чем на вычисления разницы в данных. Поэтому мы рекомендуем включать этот параметр только при медленном подключении к хранилищу резервных копий (например, если резервная копия расположена в облачном хранилище данных или на удаленной сетевой папке).

При восстановлении физической машины предварительная настройка зависит от расположения резервной копии:

- Если хранилище резервных копий является облачным, используется следующая предварительная настройка: **Включено**.
- Для других хранилищ резервных копий используется следующая настройка: **Отключено**.

При восстановлении виртуальной машины предварительно задана настройка **Включено**.

6.7.7 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**.

6.7.8 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 (стр. 122).

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.*

6.7.9 Производительность

Этот параметр определяет приоритет процесса восстановления в операционной системе.

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

Значение по умолчанию: **Обычный**.

Приоритет процесса, выполняющегося в системе, определяет количество выделенных ему ресурсов ЦП и системы. Понизив приоритет восстановления, можно освободить часть ресурсов для других приложений. Повышение приоритета восстановления может ускорить процесс восстановления за счет выделения операционной системой большего объема ресурсов приложению, выполняющему восстановление. Однако результат будет зависеть от общей загрузки процессора и других факторов, например скорости ввода-вывода диска и сетевого трафика.

6.7.10 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.

6.7.10.1 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 выберите 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 папке, в которой будет выполняться команда или пакетный файл.
4. В поле **Аргументы** укажите при необходимости аргументы выполняемой команды.
5. В зависимости от желаемого результата выберите соответствующие параметры из описанных в таблице ниже.
6. Нажмите кнопку **Готово**.

Флажок	**Выбор**			
Прервать восстановление при сбое команды*	Установить	Снять	Установить	Снять
Не начинать восстановление до завершения выполнения команды	Установить	Установить	Снять	Снять
Результат				
	Предустановка Выполнить восстановление только после успешного выполнения команды. Прервать восстановление при сбое команды.	Выполнить восстановление после выполнения команды независимо от результатов ее выполнения (успешно или ошибка).	Н/Д	Выполнить восстановление параллельно с выполнением команды независимо от результата ее выполнения.

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

6.7.10.2 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 выберите пакетный файл.
3. В поле **Рабочая папка** укажите путь к папке, в которой 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.*

6.7.11 Изменение идентификатора безопасности

Этот параметр действует при восстановлении ОС Windows 8.1 и Windows Server 2012 R2 или более ранних версий.

Этот параметр не действует, если восстановление в виртуальную машину выполняется агентом для VMware или агентом для Hyper-V.

Значение по умолчанию: **Отключено**.

Это программное обеспечение может генерировать уникальный идентификатор безопасности (SID компьютера) для восстановленной операционной системы. Этот параметр требуется только для обеспечения работоспособности программного обеспечения сторонних производителей, в котором используется SID компьютера.

Корпорация Майкрософт не поддерживает официально изменение SID в развернутых или восстановленных системах. Это означает, что, используя этот параметр, вы принимаете на себя весь риск.

6.7.12 Управление питанием ВМ

Эти параметры действуют, если восстановление на виртуальную машину выполняется агентом для VMware или агентом для Hyper-V.

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.

6.7.13 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**). Можно фильтровать события, записываемые в журнал.

Значение по умолчанию: **Отключено**.

7 Операции с резервными копиями

7.1 Вкладка «Резервные копии»

На вкладке **Резервные копии** показаны резервные копии всех машин, которые когда-либо были зарегистрированы на сервере управления. Сюда входят отключенные машины и машины, которые больше не зарегистрированы.

Резервные копии, которые хранятся в общем расположении (например на общем ресурсе SMB или NFS) видимы всем пользователям, которые имеют разрешение на чтение в данном расположении.

В облачном хранилище данных у пользователей есть доступ только к собственным резервным копиям. В облачном развертывании администратор может просматривать резервные копии от имени любой учетной записи, которая принадлежит одной группе и ее дочерним группам. Эта учетная запись косвенно выбрана в области **Машина для обзора**. На вкладке **Резервные копии** показаны резервные копии всех машин, когда-либо зарегистрированных под одной учетной записью с этой машиной.

Хранилища резервных копий, которые используются в планах резервного копирования, автоматически добавляются на вкладку **Резервные копии**. Чтобы добавить другую папку (например, съемное USB-устройство) в список хранилищ резервных копий, щелкните **Обзор** и укажите путь к папке.

Порядок выбора точки восстановления с использованием вкладки «Резервные копии»

1. На вкладке **Резервные копии** 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 резервного копирования>`
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.

   Важная информация. *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.

7.2 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.

Подключение томов в режиме чтения/записи позволяет менять содержимое резервной копии, то есть сохранять, перемещать, создавать и удалять файлы или папки и запускать исполняемые сценарии, состоящие из одного файла. В этом режиме программное обеспечение создает инкрементную резервную копию, которая содержит изменения, внесенные в содержимое резервной копии. Помните, что ни одного из этих изменений не будет в последующих резервных копиях.

Требования

- Эта функциональность доступна только в Windows при использовании проводника.
- На машине, которая выполняет операцию подключения, должен быть установлен агент для Windows.
- Файловая система, для которой создана резервная копия, должна поддерживаться в той версии Windows, которая выполняется на данной машине.
- Резервная копия должна хранится в локальной папке, сетевой папке (SMB/CIFS) или в Зоне безопасности.

Сценарии использования

- **Предоставление общего доступа к данным**

  Можно легко предоставить общий доступ к подключенным томам по сети.

- **Временное решение по восстановлению базы данных**

  Подключите том, который содержит базу данных SQL, из вышедшей недавно из строя машины. Это предоставит доступ к базе данных до восстановления этой машины. Этот подход можно использовать для фрагментарного восстановления данных Microsoft SharePoint, используя SharePoint Explorer.

- **Автономная очистка от вирусов**

  Если машина заражена вирусами, подключите ее резервную копию, очистите с помощью антивирусной программы (или найдите последнюю копию, которая не заражена вирусами). После этого восстановите машину из этой резервной копии.

- **Обработка ошибок**

  Сбой восстановления с возможностью восстановления размера тома может происходить по причине ошибки в файловой системе, для которой создана резервная копия. Подключите резервную копию в режиме чтения/записи. После этого проверьте подключенный том на наличие ошибок, используя команду **chkdsk /r**. После исправления ошибок и создания новой инкрементной резервной копии восстановите систему из этой резервной копии.

Порядок подключения тома из резервной копии

1. Перейдите в хранилище резервных копий, используя проводник.
2. Дважды щелкните файл резервной копии. По умолчанию файлы имеют имена на основе следующего шаблона:

   `<machine name> - <backup plan GUID>`
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.

Подсказка *Дважды щелкните том для обзора его содержимого. Можно скопировать файлы и папки из резервной копии в любую папку в файловой системе.*

5. Правой кнопкой мыши щелкните том для подключения, затем выберите один из следующих пунктов меню:
   - **Подключить**
   - **Подключить в режиме «только чтение»**
6. Если резервная копия хранится в сетевой папке, укажите учетные данные для доступа. В противном случае пропустите этот шаг.

   Программа подключит выбранный том. Данному тому назначается первая неиспользованная буква.

Порядок отключения тома

1. В проводнике откройте **Компьютер** (**Этот компьютер** в Windows 8.1 и более поздней версии).
2. Правой кнопкой мыши щелкните подключенный том.
3. Нажмите **Отключить**.
4. Если том подключен в режиме чтения/записи и его содержимое было изменено, выберите, создавать ли инкрементную резервную копию с этими изменениями. В противном случае пропустите этот шаг.

   Программа отключит выбранный том.

7.3 Удаление резервных копий

Порядок удаления резервных копий машины, которая включена и присутствует на консоли резервного копирования

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. Выполните одно из следующих действий:
   - Чтобы удалить одну резервную копию, выберите ее и щелкните значок корзины.
   - Чтобы удалить все резервные копии в выбранном хранилище, щелкните **Удалить все**.
5. Подтвердите операцию.

Порядок удаления резервных копий любой машины

1. На вкладке **Резервные копии** выберите хранилище, из которого необходимо удалить резервные копии.

   В программном обеспечении отображаются все резервные копии, которые разрешено просматривать в выбранном хранилище для вашей учетной записи. Резервные копии объединены по группам. Группы имеют имена на основе следующего шаблона:

   `<имя машины> - <имя плана резервного копирования>`
2. Выберите группу.
3. Выполните одно из следующих действий:
   - Чтобы удалить одну резервную копию, щелкните **Показать резервные копии**, выберите резервную копию для удаления, затем щелкните значок корзины.
   - Чтобы удалить выбранную группу, щелкните **Удалить**.

4. Подтвердите операцию.

8 Операции с планами резервного копирования

Изменение плана резервного копирования

1. Чтобы изменить план резервного копирования для всех машин, на которых он применен, выберите одну из них. В противном случае выберите машины, для которых хотите изменить план.
2. Нажмите кнопку **Резервное копирование**.
3. Выберите план резервного копирования, который хотите изменить.
4. Щелкните по значку шестеренки рядом с именем плана резервного копирования и выберите команду **Изменить**.
5. Чтобы изменить параметры плана, щелкните соответствующий раздел на его панели.
6. Нажмите кнопку **Сохранить изменения**.
7. Чтобы изменить план резервного копирования для всех машин, на которых он применен, щелкните **Применить изменения к этому плану резервного копирования**. Или щелкните **Создать новый план резервного копирования только для выбранных устройств**.

Отзыв плана резервного копирования для машин

1. Выберите машины, для которых нужно отозвать план резервного копирования.
2. Нажмите кнопку **Резервное копирование**.
3. Если для машин применено несколько планов, выберите тот из них, который необходимо отозвать.
4. Щелкните по значку шестеренки рядом с именем плана резервного копирования и выберите команду **Отозвать**.

Удаление плана резервного копирования

1. Выберите любую машину, для которой применен план резервного копирования, подлежащий удалению.
2. Нажмите кнопку **Резервное копирование**.
3. Если для машины применено несколько планов, выберите тот из них, который необходимо удалить.
4. Щелкните по значку шестеренки рядом с именем плана резервного копирования и выберите команду **Удалить**.

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

9 Вкладка «Планы»

Важно! *Эта функция была представлена в версии 12.5, и влияет только на локальные развертывания. Эта функция пока недоступна в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Планами резервного копирования и прочими планами можно управлять на вкладке **Планы**.

Каждый раздел вкладки **Планы** содержит планы конкретного типа. Доступны следующие разделы

- **Резервное копирование**
- **Репликация резервной копии** (стр. 162)

- **Проверка** (стр. 163)
- **Очистка** (стр. 166)
- **Преобразование в ВМ** (стр. 166)
- **Репликация ВМ** (стр. 226)
- **Загрузочный носитель**. В этом разделе отображены планы резервного копирования, созданные для машин, загружаемых с загрузочных носителей (стр. 184) и применяющиеся только к этим машинам.

Планы для репликации, проверки, очистки и преобразования резервных копий в виртуальные машины доступны только для лицензии Advanced. При отсутствии лицензии Advanced эти действия могут выполняться только как часть плана резервного копирования.

В каждом разделе можно создавать, редактировать, отключать, подключать, запускать выполнение и проверять состояние выполнение плана. Клонирование доступно только для планов резервного копирования.

Также возможно экспортировать план в файл и импортировать предварительно экспортированный план.

9.1 Обработка данных Off-host

Большая часть действий, выполняемая в ходе плана резервного копирования, например, репликация, проверка и применение правил хранения, выполняются агентом, выполняющим резервное копирование. Это увеличивает рабочую нагрузку на машину, на которой запущен агент, даже после завершения процесса резервного копирования.

Вынесение планов репликации, проверки, очистки, и преобразования отдельно от плана резервного копирования повышает гибкость и предоставляет следующие возможности:

- выбор другого агента/агентов для выполнения таких операций;
- планирование выполнения таких операций на часы наименьшей загрузки для снижения использования полосы пропускания;
- перенесение выполнения таких операций на нерабочие часы, если в ваши планы не входит настройка вынесенного агента.

Если вы используете узел хранения, установка вынесенного агента на ту же машину не имеет смысла.

9.1.1 Репликация резервной копии

Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами репликации резервных копий.

Хранилище резервных копий	Поддерживается в качестве источника	Поддерживается в качестве назначения
Облачное хранилище данных	+	+
Локальная папка	+	+
Сетевая папка	+	+
Папка NFS	–	–

Зона безопасности	–	–
Сервер SFTP	–	–
Управляемое хранилище	+	+
Ленточное устройство	–	+

Создание плана репликации резервных копий

1. Щелкните **Планы** > **Репликация резервных копий**.
2. Щелкните **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Дополнительно] Для изменения имени плана щелкните имя по умолчанию.
4. Щелкните **Агент**, а затем выберите агента, который выполнит репликацию.

   Можно выбрать любого агента, который имеет доступ к источнику и месту назначения хранилища резервной копии.
5. Щелкните **Элементы для репликации** и выберите резервные копии для репликации этим планом.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии зашифрованы, все они должны использовать одинаковый пароль шифрования.
6. Щелкните **Место назначения** и укажите место назначения.
7. [Дополнительно] В разделе **Порядок репликации** выберите резервные копии для репликации. Можно выбрать один из следующих вариантов:
   - **Все резервные копии** (по умолчанию)
   - **Только полные резервные копии**
   - **Только последнее резервное копирование**
8. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
9. [Необязательно] Щелкните **Правила хранения**, а затем укажите правила хранения для целевого расположения, как описано в разделе «Правила хранения» (стр. 98).
10. Если резервные копии, выбранные в **Элементы для репликации**, зашифрованы, включите переключатель **Пароль резервной копии** и укажите пароль шифрования. В противном случае пропустите этот шаг.
11. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
12. Нажмите кнопку **Создать**.

9.1.2 Проверка

Проверка это операция по определению возможности восстановления данных из резервной копии.

Проверка хранилища резервных копий проверяет все резервные копии, расположенные в хранилище.

Принцип работы

В планах проверки предусмотрено два метода проверки. Если выбрать оба метода, операции будут выполняться последовательно.

- **Вычисление контрольной суммы для каждого блока данных, сохраненных в резервной копии**

  Дополнительную информацию о проверке путем расчета контрольной суммы см. в разделе «Проверка резервных копий» (стр. 114).

- **Запуск виртуальной машины из резервной копии**

  Этот метод работает только для резервных копий дисков, содержащих операционную систему. Чтобы использовать этот метод, необходимо иметь хост ESXi или Hyper-V и агент резервного копирования (агент для VMware или агент для Hyper-V), который управляет этим хостом.

  Агент запускает виртуальную машину с резервной копии и подключается к VMware Tools или службе Hyper-V Heartbeat для проверки успешности запуска операционной системы. При сбое подключения агент пытается подключится каждые две минуты. Всего предпринимается пять попыток подключения. Если ни одна из попыток не будет успешной, проверка завершится сбоем.

  Независимо от количества планов проверки и проверенных резервных копий агент, который выполняет планы проверки, одновременно запускает одну виртуальную машину. Как только результат проверки становится известным, агент удаляет виртуальную машину и запускает следующую.

Если не удается выполнить проверку, можно просмотреть подробные сведения в разделе **Действия** на вкладке **Обзор**.

Поддерживаемые расположения

В следующей таблице представлены хранилища резервных копий, поддерживаемые планами проверки.

Хранилище резервных копий	Вычисление контрольной суммы	Запуск VM
Облачное хранилище данных	+	+
Локальная папка	+	+
Сетевая папка	+	+
Папка NFS	–	–
Зона безопасности	–	–
Сервер SFTP	–	–
Управляемое хранилище	+	+
Ленточное устройство	+	–

Создание нового плана проверки

1. Нажмите **Планы** > **Проверка**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.

3. [Необязательно] Для изменения имени плана нажмите на имя по умолчанию.
4. Щелкните **Агент**, а затем выберите агент, который выполнит проверку.

   Для выполнения проверки посредством запуска виртуальной машины из резервной копии, выберите агент для VMware или агент для Hyper-V. В противном случае выберите любой агент, который зарегистрирован на сервере управления и имеет доступ к хранилищу резервной копии.
5. Щелкните **Элементы для проверки** и выберите резервные копии для проверки этим планом.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии зашифрованы, все они должны использовать одинаковый пароль шифрования.
6. [Необязательно] В **Объект проверки**, выберите резервные копии на проверку. Можно выбрать один из следующих вариантов:
   - **Все резервные копии**
   - **Только последняя резервная копия**
7. [Необязательно] Нажмите **Порядок проверки** и затем выберите любой из указанных ниже методов:
   - **Проверка контрольной суммы**

     Программное обеспечение вычислит контрольную сумму для каждого блока данных резервной копии.
   - **Запуск как виртуальной машины**

     Программное обеспечение запустит виртуальную машину из каждой резервной копии.
8. Если выбрать **Запуск как виртуальной машины**:
   a. Щелкните **Целевая машина** и выберите тип виртуальной машины (ESXi или Hyper-V), хост и шаблон имени машины.

      По умолчанию установлено имя **[Имя машины]_validate**.
   b. Нажмите **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для виртуальной машины.
   c. [Необязательно] Измените режим распределения ресурсов диска.

      По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
   d. Чтобы получить правильный результат проверки, не выключайте **Сигнал пульса ВМ**. Этот переключатель предназначен для будущих выпусков.
   e. [Необязательно] Нажмите **Настройки ВМ**, чтобы изменить размер памяти и сетевые подключения виртуальной машины.

      По умолчанию виртуальная машина *не* подключена к сети, а размер памяти виртуальной машины соответствует размеру памяти оригинальной машины.
9. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
10. Если резервные копии, выбранные в разделе **Элементы для проверки**, зашифрованы, включите переключатель **Пароль резервной копии** и укажите пароль шифрования В противном случае пропустите этот шаг.
11. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
12. Нажмите кнопку **Создать**.

9.1.3 Очистка

Очистка — это операция, которая удаляет устаревшие резервные копии в соответствии с правилами хранения.

Поддерживаемые расположения

Планы очистки поддерживаются всеми хранилищами резервных копий, за исключением папок NFS, SFTP-серверов и Зона безопасности.

Создание нового плана очистки

1. Щелкните **Планы** > **Очистка**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Дополнительно] Для изменения имени плана щелкните имя по умолчанию.
4. Щелкните **Агент**, а затем выберите агента, который будет выполнять очистку.

   Можно выбрать любой агент, который имеет доступ к расположению резервного копирования.
5. Щелкните **Элементы для очистки**, затем выберите резервные копии, которые будут очищены этим планом.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии зашифрованы, все они должны использовать одинаковый пароль шифрования.
6. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
7. [Дополнительно] Щелкните **Правило хранения**, а затем укажите правила хранения, как описано в разделе «Правила хранения» (стр. 98).
8. Если резервные копии, выбранные в **Элементы для очистки** зашифрованы, включите переключатель **Пароль резервной копии** и укажите шифрование пароля. В противном случае пропустите этот шаг.
9. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
10. Нажмите кнопку **Создать**.

9.1.4 Преобразование в виртуальную машину

Предварительные требования

Чтобы выполнить преобразование, необходимо иметь хост ESXi или Hyper-V и агент резервного копирования (агент для VMware или агент для Hyper-V), который управляет этим хостом.

Поддерживаемые хранилища резервных копий

Все хранилища резервных копий за исключением папок NFS, серверов SFTP и Зона безопасности.

Принцип работы

В результате первого преобразования создается новая виртуальная машина. Любые последующие обновления преобразования виртуальной машины в состояние последней точки восстановления.

Создание преобразования в план виртуальной машины

1. Щелкните **Планы** > **Преобразование в ВМ**.
2. Нажмите **Создать план**.

   В программе отобразится новый шаблон плана.
3. [Дополнительно] Для изменения имени плана щелкните имя по умолчанию.
4. В поле **Преобразовать в** выберите тип целевой виртуальной машины. Можно выбрать один из следующих вариантов:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
5. Щелкните **Хост**, выберите целевой хост, а затем укажите новый шаблон имени машины.

   Имя по умолчанию — **[Имя машины]_converted**.
6. Щелкните **Агент**, а затем выберите агент, который выполнит преобразование.
7. Щелкните **Элементы для преобразования**, выберите резервные копии, которые данный план преобразует в виртуальные машины.

   Используя переключатель **Хранилища** / **Резервные копии** в верхнем правом углу, можно переключаться между выбором отдельных резервных копий и выбором хранилищ целиком.

   Если выбранные резервные копии зашифрованы, все они должны использовать одинаковый пароль шифрования.
8. Щелкните **Хранилище данных** для ESXi или **Путь** для Hyper-V и выберите хранилище данных для данной виртуальной машины.
9. [Дополнительно] Можно также выполнить следующие действия:
   - Измените режим распределения ресурса дисков. По умолчанию задана настройка **Экономное** для VMware ESXi и **Динамически расширяемое** для Hyper-V.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.
10. [Дополнительно] Щелкните **Расписание**, а затем измените расписание.
11. Если резервные копии, выбранные в **Элементы для преобразования** зашифрованы, включите переключатель **Пароль резервной копии** и укажите пароль шифрования. В противном случае пропустите этот шаг.
12. [Дополнительно] Для изменения параметров плана щелкните значок шестеренки.
13. Нажмите кнопку **Создать**.

10 Загрузочный носитель

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

10.1 Мастер создания загрузочных носителей

Мастер создания загрузочных носителей — это специальное средство для создания загрузочных носителей. Он доступен только в локальных развертываниях.

Мастер создания загрузочных носителей устанавливается по умолчанию при установке сервера управления. Его можно установить отдельно на любой машине с ОС Windows или Linux. Поддерживаются те же операционные системы, что и для соответствующих агентов.

Цели использования мастера создания носителей

Загрузочный носитель, доступный для загрузки на консоли резервного копирования, можно использовать только для восстановления. Этот носитель основан на ядре Linux. В отличие от среды Windows PE, он не позволяет вводить пользовательские драйверы на лету.

- С помощью мастера создания носителей можно создавать настраиваемые загрузочные носители на основе Linux или WinPE с функциями резервного копирования.
- Помимо создания физического носителя или его ISO-образа, можно добавить носитель в службы развертывания Windows (WDS) и использовать загрузку по сети.
- Наконец, можно записать носитель непосредственно на флэш-накопитель, не используя средства сторонних производителей.

32- или 64-разрядная версия

Мастер создания загрузочных носителей можно установить с помощью как 32-разрядной, так и 64-разрядной программы установки. Разрядность носителя соответствует разрядности программы установки. Однако если загрузить 32-разрядный подключаемый модуль, то можно создать 32-разрядный носитель на основе WinPE с помощью 64-разрядного мастера создания носителей.

Помните, что в большинстве случаев для загрузки машины, которая использует интерфейс UEFI, требуется 64-разрядный носитель.

10.1.1 Загрузочные носители на основе Linux

Порядок создания загрузочного носителя на основе Linux

1. Запустите мастер создания загрузочных носителей.
2. Укажите лицензионный ключ. Лицензия не будет назначена или переназначена. Она определяет, какие функции следует включить для созданного носителя. Без лицензионных ключей можно создать носитель только для восстановления.
3. Выберите **Тип загрузочного носителя: По умолчанию (носители на основе Linux)**.

   Выберите способ обработки томов и сетевых ресурсов, так называемый стиль носителя:

   - На носителе, для которого выбран способ обработки в стиле Linux, тома отображаются как, например, hda1 и sdb2. Перед началом восстановления предпринимается попытка реконструировать MD-устройства и LVM (диспетчер логических томов).
   - На носителе с обработкой тома на основе Windows тома отображаются как, например, C: и D: Он обеспечивает доступ к динамическим томам (LDM).
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**

   Список параметров см. в разделе Параметры ядра (стр. 170).
5. Выберите компоненты, которые будут размещены на носителе: загрузочный агент и/или Universal Restore.

Используя носитель с загрузочным агентом, можно выполнять операции резервного копирования, восстановления и управления дисками на любом ПК-совместимом оборудовании, включая «голое железо».

С помощью Universal Restore можно загружать восстанавливаемую операционную систему на другом оборудовании или на виртуальной машине, если возникла проблема с загрузкой системы. Это средство находит и устанавливает драйверы для устройств, необходимых для запуска операционной системы, таких как контроллеры памяти, системная плата или набор микросхем.

6. [Необязательно] Укажите время ожидания для меню загрузки и компонент, который будет автоматически запускаться по истечении этого времени.

   Если значение не задано, загрузчик ожидает, пока пользователь не выберет, загружать ли операционную систему (если есть) или компонент.

   Если задать, например, это значение равным **10 сек.**, то загрузочный агент будет запущен по истечении 10 секунд с момента появления меню. Это позволяет автоматически выполнять операции на рабочем месте при загрузке из WDS или RIS.

7. [Необязательно] Чтобы автоматизировать операции загрузочного агента, установите флажок **Использовать следующий сценарий**. Затем выберите один из сценариев (стр. 171) и задайте его параметры.

8. [Optional] Specify the remote logon settings: the user name and password to be specified in a command string if the **acrocmd** utility is running on a different machine. Если оставить эти поля пустыми, команда не обязательно должна содержать учетные данные.

   Эти учетные данные также необходимы при регистрации носителя на сервере управления с консоли резервного копирования (стр. 184).

9. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительные сведения о настройках регистрации см. разделе «Сервер управления» (стр. 177).

10. [Необязательно] Укажите сетевые настройки (стр. 178): Настройки TCP/IP для назначения сетевым адаптерам машины.

11. [Необязательно] Укажите сетевой порт (стр. 179): TCP-порт, который прослушивается загрузочным агентом для приема входящих подключений.

12. [Необязательно] Если в сети включен прокси-сервер, укажите его имя хоста или IP-адрес и порт.

13. Выберите тип создаваемого носителя. Можно сделать следующее:

    - создать загрузочный компакт-диск, DVD-диск или другой загрузочный носитель, например съемный флэш-накопитель USB, если BIOS машины поддерживает загрузку с таких носителей;
    - создать ISO-образ для последующей записи на чистый диск или подключения к виртуальной машине;
    - Передать выбранные компоненты на PXE-сервер Acronis.
    - Загрузить выбранные компоненты в WDS или RIS.

14. [Необязательно] Добавьте системные драйверы Windows для использования компонентом Universal Restore (стр. 180). Это окно отображается в том случае, если компонент Universal Restore добавлен на носитель и выбран носитель, отличный от WDS и RIS.

15. При необходимости укажите имя хоста или IP-адрес и учетные данные для WDS или RIS либо путь к ISO-файлу носителя.

16. Проверьте произведенные настройки в итоговом окне и нажмите кнопку **Приступить**.

10.1.1.1 Параметры ядра

Это окно позволяет указывать параметры для ядра Linux. Они будут применены автоматически при запуске загрузочного носителя.

Обычно эти параметры используются при наличии проблем с работой загрузочных носителей. Как правило, это поле оставляется пустым.

Кроме того, можно указать любой из этих параметров, нажав клавишу F11 в меню загрузки.

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=*номер_режима*

Задает видеорежим для графического пользовательского интерфейса загрузочного носителя. Номер режима задается параметром *номер_режима* в шестнадцатеричном формате, например **vga=0x318**

Разрешение экрана и количество цветов, соответствующее номеру режима, может различаться на разных машинах. Рекомендуется в качестве значения **номер_режима** сначала использовать параметр *vga=ask*.

quiet

Отключает отображение загрузочных сообщений при загрузке ядра Linux и запускает консоль управления после загрузки ядра.

Этот параметр указан неявно при создании загрузочного носителя, однако его можно удалить из меню загрузки.

Без этого параметра будут отображаться все сообщения загрузки, потом появится командная строка. Чтобы запустить консоль управления из командной строки, запустите следующую команду: **/bin/product**

nousb

Отключает загрузку подсистемы USB.

nousb2

Отключает поддержку USB 2.0. Устройства USB 1.1 при наличии этого параметра продолжают работать. Этот параметр позволяет использовать некоторые USB-устройства в режиме USB 1.1, если они не работают в режиме USB 2.0.

nodma

Отключает прямой доступ к памяти access (DMA) для всех жестких дисков IDE. Предотвращает зависание ядра с некоторым оборудованием.

nofw

Отключает поддержку интерфейса FireWire (IEEE1394).

nopcmcia

Отключает распознавание оборудования PCMCIA.

nomouse

Отключает поддержку мыши.

имя_модуля=**off**

Отключает модуль, имя которого задано параметром *имя_модуля*. 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.

10.1.1.2 Сценарии на загрузочных носителях

Примечание *Эта функция доступна только при наличии лицензии Advanced для Acronis Backup.*

Для того, чтобы на загрузочном носителе выполнялся определенный набор операций, укажите сценарий при создании носителя в Bootable Media Builder. При каждой загрузке носителя вместо отображения пользовательского интерфейса начнется выполнение сценария.

Выберите один из предопределенных сценариев или создайте пользовательский сценарий в соответствии со стандартами создания сценариев.

Предопределенный сценарий

Bootable Media Builder предоставляет следующие предопределенные сценарии:

- резервное копирование данных в облачное хранилище и восстановление данных из облачного хранилища (**entire_pc_cloud**);
- резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя (**entire_pc_local**);

- резервное копирование данных в сетевую папку и восстановление данных из сетевой папки (**entire_pc_share**);
- восстановление данных из облачного хранилища (**golden_image**).

Сценарии находятся на машине, на которой установлено приложение Bootable Media Builder, в следующих папках:

- В ОС Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- В ОС Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Резервное копирование данных в облачное хранилище и восстановление данных из облачного хранилища

Сценарий создаст резервную копию машины в облачном хранилище или восстановит машину из последней резервной копии, созданной этим сценарием в облачном хранилище. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder укажите следующие параметры сценария:

1. имя пользователя и пароль для доступа в облачное хранилище;
2. [Необязательно] пароль, который сценарий будет использовать для шифрования или доступа к резервным копиям.

Резервное копирование данных на загрузочный носитель и восстановление данных с загрузочного носителя

Сценарий создаст резервную копию машины на загрузочном носителе или восстановит машину из последней резервной копии, созданной этим сценарием на том же носителе. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder вы можете указать пароль, который сценарий будет использовать для шифрования или доступа к резервным копиям.

Резервное копирование данных в сетевую папку и восстановление данных из сетевой папки

Сценарий создаст резервную копию машины в сетевой папке или восстановит машину из последней резервной копии, расположенной в сетевой папке. При запуске сценарий отправит пользователю запрос с возможностью выбора между созданием резервной копии, восстановлением из резервной копии и запуском пользовательского интерфейса.

В Bootable Media Builder укажите следующие параметры сценария:

1. путь к сетевой папке;
2. имя пользователя и пароль для доступа в сетевую папку;
3. [Необязательно] имя файла резервной копии. Значением по умолчанию является **AutoBackup** (Автоматическое резервное копирование). Если вы хотите, чтобы сценарий добавлял резервные копии к уже существующим резервным копиям, или провести восстановление из резервной копии с заданным пользователем именем, измените значение по умолчанию на имя файла желаемой резервной копии.

   Как узнать имя файла резервной копии

1. В консоли резервного копирования перейдите в **Резервные копии** > **Хранилища**.
2. Выберите сетевую папку (нажмите **Добавить хранилище**, если нужной папки нет в списке).
3. Выберите резервную копию.
4. Нажмите **Сведения**. Имя файла отобразиться в поле **Имя файла резервной копии**.

4. [Необязательно] пароль, который сценарий будет использовать для шифрования или доступа к резервным копиям.

Восстановление из облачного хранилища

Сценарий восстановит машину из последней резервной копии, расположенной в облачном хранилище. При запуске сценарий запросит у пользователя следующие данные:

1. имя пользователя и пароль для доступа в облачное хранилище;
2. пароль, если резервная копия зашифрована.

Мы рекомендуем хранить под данной учетной записью облачного хранилища резервные копии только одной машины. В ином случае, если в хранилище будет расположена резервная копия другой машины, созданная позднее резервной копии необходимой машины, сценарий выберет для восстановления более новую резервную копию.

Пользовательские сценарии

Важно! *Создание пользовательских сценариев требует знания команд оболочки Bash и формата JavaScript Object Notation (JSON). Если вы не знакомы с командной оболочкой Bash, хороший учебник можно найти по ссылке http://www.tldp.org/LDP/abs/html. Спецификация JSON доступна на сайте http://www.json.org.*

Файлы сценария

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

- В ОС Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- В ОС Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Сценарий должен состоять из по меньшей мере трех файлов:

- **<файл_сценария>.sh** — файл со сценарием Bash. При создании сценария используйте только ограниченный набор команд оболочки, который вы можете найти по ссылке https://busybox.net/downloads/BusyBox.html. Также могут быть использованы следующие команды:
  - **`acrocmd`** — утилита командной строки для создания резервной копии и восстановления
  - **`product`** — команда, запускающая пользовательский интерфейс загрузочного носителя

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

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** — файл формата JSON, содержащий следующее:
  - Имя сценария и описания будут отображаться в мастере создания загрузочных носителей.
  - Имена переменных сценария должны быть настроены через мастер создания загрузочных носителей.
  - параметры элементов управления, которые будут отображены в Bootable Media Builder для каждой переменной.

Структура autostart.json

Объект высшего уровня

Пара		Требуется	Описание
Имя	**Тип значения**		
displayName	string	Да	Имя сценария, которое будет отображаться в Bootable Media Builder.
description	string	Нет	Описание сценария, которое будет отображаться в Bootable Media Builder.
timeout	number	Нет	Время ожидания (в секундах) для меню загрузки перед запуском сценария. Если пара не указана, время ожидания составит десять секунд.
variables	объект	Нет	Любые переменные для **<файл_сценария>.sh**, которые вы хотите сконфигурировать посредством Bootable Media Builder. Значение должно быть указано в виде набора следующих пар: идентификатор строки переменной и объект переменной (см. в таблице ниже).

Объект переменной

Пара		Требуется	Описание
Имя	**Тип значения**		
displayName	string	Да	Имя переменной, использованное в **<файл_сценария>.sh**.
type	string	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	string	Да	Метка элемента управления, отображаемая над элементом управления в Bootable Media Builder.
default	строка, если **type** является **string**, **multiString**, **password** или **enum** номер, если **type** является **number**, **spinner** или **checkbox**	Нет	Значение по умолчанию элемента управления. Если пара не указана, значением по умолчанию будет являться пустая строка или ноль, в зависимости от типа элемента управления. Значением по умолчанию для флажка может быть **0** (флажок не установлен) или **1** (флажок установлен).

Пара		Требуется	Описание
Имя	**Тип значения**		
order	number (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**)	number	Нет	Минимальное значение элемента управления «счетчик» в поле счетчика. Если пара не указана, значением будет **0**.
max (только для **spinner**)	number	Нет	Максимальное значение элемента управления «счетчик» в поле счетчика. Если пара не указана, значением будет **100**.
step (только для **spinner**)	number	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**)	number	Нет	Указывает, может ли значение элемента управления быть пустым (**0**) или нет (**1**). Если пара не указана, значение элемента управления может быть пустым.

Тип элемента управления

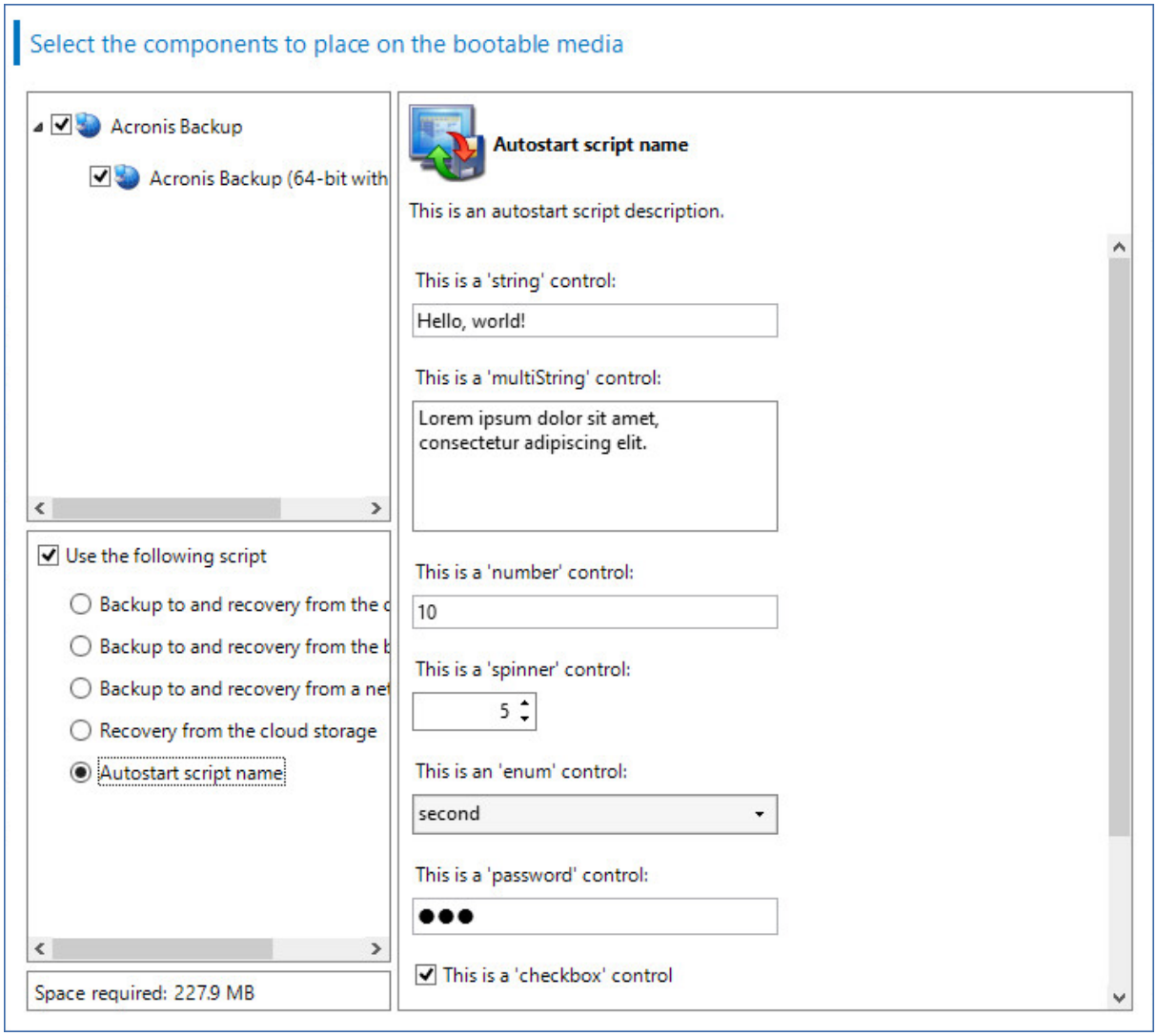
Имя	Описание
string	Текстовое поле высотой в одну строку и без ограничений ширины, используемое для введения или редактирования коротких строк.
multiString	Текстовое поле высотой в несколько строк и без ограничений ширины, используемое для введения или редактирования коротких строк.
password	Текстовое 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": "Autostart script name",
   "description": "This is an autostart script description.",
   "variables": {
      "var_string": {
```

```
            "displayName": "VAR_STRING",
            "type": "string", "order": 1,
            "description": "This is a 'string' control:", "default": "Hello,
            world!"
        },
        "var_multistring": {
            "displayName": "VAR_MULTISTRING",
            "type": "multiString", "order": 2,
            "description": "This is a 'multiString' control:",
            "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
            "displayName": "VAR_NUMBER",
            "type": "number", "order": 3,
            "description": "This is a 'number' control:", "default": 10
        },
        "var_spinner": {
            "displayName": "VAR_SPINNER",
            "type": "spinner", "order": 4,
            "description": "This is a 'spinner' control:",
            "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
            "displayName": "VAR_ENUM",
            "type": "enum", "order": 5,
            "description": "This is an 'enum' control:",
            "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
            "displayName": "VAR_PASSWORD",
            "type": "password", "order": 6,
            "description": "This is a 'password' control:", "default": "qwe"
        },
        "var_checkbox": {
            "displayName": "VAR_CHECKBOX",
            "type": "checkbox", "order": 7,
            "description": "This is a 'checkbox' control", "default": 1
        }
    }
}
```

Вот так все вышеописанное выглядит в Bootable Media Builder.



10.1.1.3 Сервер управления

При создании загрузочного носителя есть возможность предварительно сконфигурировать регистрацию носителя на сервере управления.

Регистрация носителя позволит выполнять операции управления с загрузочным носителем посредством консоли резервного копирования, словно с зарегистрированной машиной. Кроме удобства удаленного доступа это дает системному администратору возможность отслеживать все операции, выполняемые на загрузочном носителе. Операции находятся хранятся на вкладке **Действия**, где можно увидеть, кто и когда начал выполнение операции.

Если регистрация не была предварительно сконфигурирована, остается возможность зарегистрировать носитель после загрузки с него машины (стр. 184).

Как выполнить предварительную конфигурацию регистрации на сервере управления.

1. Установите флажок **Зарегистрировать носитель на сервере управления**.
2. В строке **Имя или IP-адрес сервера** укажите имя хоста или IP-адрес машины, на которой установлен сервер управления. Используйте один из следующих форматов.

- `http://<сервер>`. Например, `http://10.250.10.10` или `http://server1`
- `<IP address>`. Например, `10.250.10.10`
- `<имя хоста>`. Например, `server1` или `server1.example.com`

3. В строке **Порт** укажите порт, который будет использоваться для доступа к серверу управления. Значение по умолчанию составляет 9877.
4. В строке **Отображаемое имя** укажите имя, которое будет отображаться для этой машины на консоли резервного копирования. Если это поле будет оставлено пустым, в качестве отображаемого имени будет указано одно из следующих.
   - Если машина ранее была зарегистрирована на сервере управления, у нее будет то же имя.
   - В ином случае будет использовано полное доменное имя (FQDN) или IP-адрес машины.
5. Выберите учетную запись, которая будет использована для регистрации носителя на сервере управления. Доступны следующие параметры:
   - **Спрашивать имя пользователя и пароль при загрузке**

     Учетные данные необходимо вводить при каждой загрузке машины с носителя.

     Для успешной регистрации учетная запись должна находится в списке администраторов сервера управления (**Настройки** > **Администраторы**). На консоли резервного копирования носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которыми обладает данная учетная запись.

     В интерфейсе загрузочного носителя будет возможно изменить имя пользователя и пароль, перейдя по пути **Инструменты** > **Зарегистрировать носитель на сервере управления**.
   - **Зарегистрироваться под следующей учетной записью**

     Машина будет регистрироваться автоматически при каждой загрузке с носителя.

     Указанная учетная запись должна находится в списке администраторов сервера управления (**Настройки** > **Администраторы**). На консоли резервного копирования носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которыми обладает данная учетная запись.

     В интерфейсе загрузочного носителя будет *невозможно* сменить параметры регистрации.
   - **Не спрашивайте имя пользователя и пароль**

     Машина будет зарегистрирована анонимно. На вкладке **Действия** консоли резервного копирования не будет указано, кто использует носитель.

     На консоли резервного копирования носитель будет доступен в разделе организации.

     В интерфейсе загрузочного носителя будет возможно изменить имя пользователя и пароль, перейдя по пути **Инструменты** > **Зарегистрировать носитель на сервере управления**.

10.1.1.4 Сетевые настройки

При создании загрузочного носителя можно предварительно настроить сетевые подключения, которые будут использоваться загрузочным агентом. Предварительно настроить можно следующие параметры:

- IP-адрес;
- маску подсети;
- шлюз;

- DNS-сервер;
- WINS-сервер.

После запуска загрузочного агента на машине конфигурация применяется к сетевому адаптеру (NIC) машины. Если параметры не были предварительно настроены, агент использует автонастройку DHCP. Также вы можете задать сетевые параметры вручную при запуске загрузочного агента на машине.

Предварительная настройка нескольких сетевых подключений

Можно предварительно настроить параметры TCP/IP вплоть до десяти сетевых адаптеров. Чтобы убедиться, что каждому сетевому адаптеру будут назначены соответствующие параметры, создайте носитель на сервере, для которого настраивается носитель. При выборе существующего сетевого адаптера в окне мастера ее настройки выбираются для сохранения на носителе. MAC-адрес каждого существующего сетевого адаптера также сохраняется на носителе.

Параметры, кроме MAC-адреса, можно изменить или при необходимости настроить для несуществующего сетевого адаптера.

После запуска загрузочного агента на сервере он получает список доступных сетевых адаптеров. Этот список сортируется по слотам, которые занимают сетевые адаптеры: чем ближе к процессору, тем выше в списке.

Загрузочный агент назначает каждому известному сетевому адаптеру соответствующие настройки, идентифицируя адаптеры по MAC-адресам. После настройки сетевых адаптеров с известными MAC-адресами оставшимся сетевым адаптерам назначаются настройки, созданные для несуществующих сетевых адаптеров, начиная с верхнего неназначенного адаптера.

Загрузочный носитель можно настроить для любой машины, а не только для той, на которой он был создан. Для этого настройте сетевые адаптеры в соответствии с порядком их слотов на нужной машине: NIC1 занимает ближайший к процессору слот, NIC2 — следующий слот и т. д. При запуске загрузочного агента на этой машине он не найдет сетевых адаптеров с известными MAC-адресами и настроит адаптеры в том порядке, который вы указали.

Пример

Загрузочный агент может использовать один из сетевых адаптеров для связи с консолью управления через производственную сеть. Для этого подключения можно выполнить автоматическую настройку. Объемные данные для восстановления можно передавать через второй сетевой адаптер, включенный в выделенную резервную сеть посредством статических настроек TCP/IP.

10.1.1.5 Сетевой порт

Во время создания загрузочного носителя можно предварительно настроить сетевой порт, который будет прослушиваться загрузочным агентом на наличие входящего подключения от утилиты **acrocmd**. Можно выбрать один из указанных ниже вариантов.

- Порт по умолчанию
- Текущий используемый порт
- Новый порт (введите номер порта)

Если порт не был предварительно настроен, агент использует порт 9876.

10.1.1.6 Драйверы для Universal Restore

При создании загрузочного носителя есть возможность добавить на него драйверы Windows. Эти драйверы будут использоваться компонентом Universal Restore для загрузки системы Windows, перенесенной на отличающееся оборудование.

Universal Restore можно будет настроить для следующих целей:

- для поиска на носителе драйверов, наилучшим образом подходящих для целевого оборудования;
- для получения драйверов устройств хранения данных, явно заданных с носителя. Это необходимо, если на целевом оборудовании установлен особый контроллер запоминающего устройства (SCSI, RAID или адаптер Fiber Channel) для жесткого диска.

Драйверы будут размещены в видимой папке Drivers на загрузочном носителе. Драйверы не загружаются в ОЗУ целевоймашины, поэтому носитель должен оставаться вставленным или подключенным в течение всей операции Universal Restore.

Добавить драйверы на загрузочный носитель можно при создании съемного носителя, его ISO-образа или подключаемого носителя, такого как флэш-накопитель. Драйверы невозможно загрузить в WDS или RIS.

Драйверы можно добавить в список только группами, путем добавления INF-файлов или папок, содержащих такие файлы. Выбор отдельных драйверов из INF-файлов невозможен, однако мастер создания загрузочных носителей отображает содержимое файла для сведений.

Как добавить драйверы

1. Нажмите кнопку **Добавить** и перейдите к INF-файлу или папке, содержащей INF-файлы.
2. Выберите INF-файл или папку.
3. Нажмите кнопку **ОК**.

Драйверы можно удалить из списка только группами, путем удаления INF-файлов.

Как удалить драйверы

1. Выберите INF-файл.
2. Нажмите кнопку **Удалить**.

10.1.2 Загрузочный носитель на основе WinPE

Мастер создания загрузочных носителей предоставляет три способа интеграции Acronis Backup с WinPE:

- Создание ISO-образа PE с подключаемым модулем с нуля.
- Добавление подключаемого модуля Acronis к WIM-файлу для использования в будущем (ручное создание ISO-образа, добавление других средств к образу и т. д.).

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.

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

10.1.2.1 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/ru-ru/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 обработчик 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.

Рекомендуется ознакомиться со справкой, идущей в комплекте с пакетом Windows AIK. Для доступа к документации выберите **Microsoft Windows AIK -> Документация** в меню «Пуск».

10.1.2.2 Подготовка: WinPE 4.0 и более поздние версии

Для создания или изменения образов PE 4 или более поздних версий установите мастер создания загрузочных носителей на машину с установленным комплектом средств для развертывания и оценки Windows (ADK). Если у вас нет машины с ADK, подготовьте ее следующим образом.

Как подготовить машину с ADK

1. Загрузите программу установки комплекта средств для развертывания и оценки (ADK).

Комплект ADK для Windows 8 (PE 4,0):
http://www.microsoft.com/en-us/download/details.aspx?id=30652.

Комплект 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 10 для Windows 10):
https://msdn.microsoft.com/ru-ru/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.

10.1.2.3 Добавление подключаемого модуля Acronis к WinPE

Для добавления подключаемого модуля Acronis к WinPE:

1. Запустите мастер создания загрузочных носителей.
2. Укажите лицензионные ключи. Лицензионные ключи не будут назначены или переназначены. Они определяют, какие функции следует включить для созданного носителя. Без лицензионных ключей можно создать носитель только для восстановления.
3. Выберите **Тип загрузочного носителя: Windows PE** или **Тип загрузочного носителя: Windows PE (64-разрядный)**. 64-разрядный носитель требуется для загрузки машины, которая использует интерфейс UEFI.

   Если выбран вариант **Тип загрузочного носителя: Windows PE**, сначала выполните указанные ниже действия.

   - Выберите **Загрузить подключаемый модуль для WinPE (32-разрядный)**.
   - Сохраните подключаемый модуль в папке **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

   Если планируется восстановить операционную систему на компьютере с другим оборудованием или на виртуальной машине и необходимо обеспечить загружаемость системы, установите флажок **Включить средство Universal Restore...**
4. Выберите пункт **Создать WinPE автоматически**.

   Программа запускает соответствующий сценарий и переходит к следующему окну.
5. Выберите язык, который будет использоваться в загрузочном носителе.
6. Выберите, разрешить или запретить удаленное подключение к машине, загружаемой с носителя. If enabled, enter a user name and password to be specified in a command line if the **acrocmd** utility is running on a different machine. Если оставить эти поля пустыми, удаленное подключение через интерфейс командной строки будет невозможно.

   Эти учетные данные также необходимы при регистрации носителя на сервере управления с консоли резервного копирования (стр. 184).
7. Укажите сетевые настройки (стр. 178) для сетевых адаптеров машины или выберите автоконфигурацию DHC.
8. [Необязательно] Выберите способ регистрации носителя на сервере управления при загрузке. Дополнительные сведения о настройках регистрации см. разделе «Сервер управления» (стр. 177).
9. [Необязательно] Укажите драйверы Windows, которые нужно добавить к Windows PE.

   После загрузки Windows PE на машину эти драйверы помогут получить доступ к устройствам, на которых расположена резервная копия. Добавьте 32-разрядные драйверы,

если вы используете 32-разрядный дистрибутив WinPE, или 64-разрядные драйверы, если вы используете 64-разрядный дистрибутив WinPE.

Кроме того, можно будет указать добавленные драйверы при настройке компонента Universal Restore для Windows. Для использования Universal Restore следует добавить 32- или 64-разрядные драйверы в зависимости от того, какую ОС Windows планируется восстанавливать:

Порядок добавления драйверов

- Нажмите кнопку **Добавить** и задайте путь к INF-файлу для соответствующего контроллера SCSI, RAID или SATA, сетевого адаптера, ленточного устройства или другого устройства.
- Повторите эту процедуру для каждого драйвера, который необходимо записать на носитель WinPE.

10. Выберите, следует ли создать ISO- или WIM-образ либо загрузить носитель на сервер (WDS или RIS).
11. Задайте полный путь к полученному файлу образа, включая его имя, или укажите сервер и задайте имя пользователя и пароль для доступа к нему.
12. Проверьте произведенные настройки в итоговом окне и нажмите кнопку **Приступить**.
13. Запишите ISO-образ на CD- или DVD-диск с помощью программы стороннего производителя или скопируйте его на флэш-накопитель.

После загрузки машины в WinPE агент запустится автоматически.

Чтобы создать образ среды предустановки (ISO-файл) из получившегося WIM-файла,

- Замените в папке Windows PE файл boot.wim, используемый по умолчанию, созданным WIM-файлом. Для примера выше введите:

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- Используйте инструмент **Oscdimg**. Для примера выше введите:

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
c:\winpe_x86\winpe_x86.iso
```

Не копируйте этот пример. Введите команду вручную.

Дополнительные сведения о настройке среды предустановки Windows PE 2.x и 3.x см. в руководстве пользователя для этой среды (Winpe.chm). Сведения о настройке среды Windows PE 4.0 и более поздних версий доступны в библиотеке Microsoft TechNet.

10.2 Подключение к машине, загружаемой с носителя

После загрузки машины с загрузочного носителя терминал машины отображает окно загрузки с IP-адресами, полученными от сервера DHCP или установленными в соответствии с предварительно заданными значениями.

Конфигурирование настроек сети

Чтобы изменить сетевые параметры для текущего сеанса, щелкните **Настроить параметры сети** в окне запуска. Появится окно **Сетевые параметры**, где можно задать сетевые настройки для каждого сетевого адаптера (NIC) машины.

Изменения, внесенные во время сеанса, будут потеряны после перезагрузки машины.

Добавление VLAN

В окне **Сетевые параметры** можно добавить виртуальные локальные сети (VLAN). Используйте эту функцию, если требуется доступ к хранилищу резервных копий, включенному в определенную сеть VLAN.

В основном сети VLAN используются для разделения локальной сети на сегменты. Сетевой адаптер, подключенный к порту *доступа* коммутатора, всегда имеет доступ к сети VLAN, указанной в настройках порта. Сетевой адаптер, подключенный к *магистральному* порту коммутатора, имеет доступ к сетям VLAN, указанным в настройках порта, только в случае, если сети VLAN заданы в сетевых параметрах.

Включение доступа к сети VLAN через магистральный порт

1. Щелкните **Добавить VLAN**.
2. Выберите сетевой адаптер, обеспечивающий доступ к локальной сети с нужной сетью VLAN.
3. Укажите идентификатор VLAN.

После щелчка на **ОК** появится новая запись в списке сетевых адаптеров.

Если требуется удалить VLAN, щелкните соответствующую сеть VLAN и нажмите кнопку **Удалить VLAN**.

Локальное подключение

Для непосредственной работы на машине, загружаемой с носителя, щелкните **Локальное управление этой машиной** в окне загрузки.

Удаленное подключение

Для удаленного подключения к носителю зарегистрируйте его на сервере управления, как описано в разделе «Регистрация носителя на сервере управления» (стр. 184).

10.3 Регистрация носителя на сервере управления

Регистрация загрузочного носителя позволит выполнять операции управления с загрузочным носителем посредством консоли резервного копирования, словно с зарегистрированной машиной. Это применимо ко всем загрузочным носителям вне зависимости от метода загрузки (физический носитель, Startup Recovery Manager, Acronis PXE Server, WDS или RIS). Невозможно зарегистрировать загрузочный носитель, созданные в ОС macOS.

Регистрация носителей возможна только при наличии на сервере управления хотя бы одной расширенной лицензии Acronis Backup.

Вы можете зарегистрировать носитель в консоли резервного копирования или в пользовательском интерфейсе носителя.

Параметры регистрации могут быть предварительно настроены в опции Сервер управления (стр. 177) Bootable Media Builder. Если параметры регистрации настроены предварительно, носитель автоматически появится на панели резервного копирования. Если некоторые параметры настроены предварительно, некоторые шаги описанной далее процедуры могут быть недоступны.

Регистрация носителя в консоли резервного копирования

Такой носитель должен быть создан с помощью Bootable Media Builder (стр. 167). Имя пользователя и пароль для удаленного подключения должны быть указаны в опции **Параметры удаленного подключения** Bootable Media Builder.

Регистрация носителя в консоли резервного копирования

1. Загрузите машину с носителя. Обратите внимание на IP-адрес, указанный в окне запуска.
2. В консоли резервного копирования нажмите **Добавить**.
3. Пролистайте вниз до **Загрузочный носитель** и затем нажмите **Зарегистрировать машину, загружаемую с загрузочного носителя**.
4. Введите IP-адрес машины, загруженной с носителя.
5. Введите имя пользователя и пароль, которые были указаны при создании носителя в разделе **Параметры удаленного подключения** Bootable Media Builder.
6. Выберите имя или IP-адрес, которые будут использоваться носителем для доступа к серверу управления.

   По умолчанию выбрано имя сервера. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою регистрации носителя.
7. Нажмите кнопку **Добавить**.

Регистрация носителя в пользовательском интерфейсе носителя

Носитель можно создать или загрузить с использованием Bootable Media Builder (стр. 167).

Регистрация носителя в пользовательском интерфейсе носителя

1. Загрузите машину с носителя.
2. Выполните одно из следующих действий:
   - В окне запуска в поле **Сервер управления** нажмите **Редактировать**.
   - В интерфейсе загрузочного носителя нажмите **Инструменты** > **Зарегистрировать носитель на сервере управления**.
3. В поле **Зарегистрировать в** укажите имя хоста или IP-адрес машины, на которой установлен сервер управления. Используйте один из следующих форматов.
   - `http://<сервер>`. Например, **`http://10.250.10.10`** или **`http://server`**
   - `<IP address>`. Например, **`10.250.10.10`**
   - `<имя хоста>`. Например, **`server`** или **`server.example.com`**
4. В полях **Имя пользователя** и **Пароль** введите учетные данные учетной записи, которая находится в списке администраторов сервера управления (**Настройки** > **Администраторы**). На консоли резервного копирования носитель будет доступен в разделе организации или конкретного отдела в соответствии с правами, которыми обладает данная учетная запись.
5. В строке **Отображаемое имя** укажите имя, которое будет отображаться для этой машины на консоли резервного копирования. Если это поле будет оставлено пустым, в качестве отображаемого имени будет указано одно из следующих.
   - Если машина ранее была зарегистрирована на сервере управления, у нее будет то же имя.
   - В ином случае будет использовано полное доменное имя (FQDN) или IP-адрес машины.
6. Нажмите кнопку **ОК**.

10.4 Настройка устройств iSCSI и NDAS

В этом разделе описана настройка устройств iSCSI и NDAS при работе с загрузочного носителя. После выполнения описанных ниже этапов можно использовать эти устройства так, как если бы они были подключены локально к машине, загружаемой с помощью загрузочного носителя.

Целевой сервер iSCSI (или **целевой портал**) — это сервер, на котором находится устройство iSCSI. **Целевое устройство iSCSI** — это компонент на целевом сервере; этот компонент обеспечивает совместное использование устройства и составляет список инициаторов iSCSI, которым разрешен доступ к устройству. **Инициатор iSCSI** — это компонент на машине; этот компонент обеспечивает взаимодействие между машиной и целевым устройством iSCSI. При настройке доступа к устройству iSCSI на машине, загруженной с помощью загрузочного носителя, необходимо указать целевой портал iSCSI устройства, а также один из инициаторов iSCSI, перечисленный на целевом устройстве. Если в целевом объекте предоставлен общий доступ к нескольким устройствам, вы получите доступ ко всем ним.

Для добавления устройства iSCSI на загрузочный носитель на основе Linux

1. Нажмите **Инструменты** > **Настроить устройства iSCSI/NDAS**.
2. Нажмите кнопку **Добавить хост**.
3. Укажите IP-адрес и порт портала целевого устройства iSCSI, а также имя любого инициатора iSCSI, который разрешил доступ к устройству.
4. Если хост требует проверки подлинности, укажите имя пользователя и пароль.
5. Нажмите кнопку **ОК**.
6. Выберите целевое устройство iSCSI в списке и нажмите кнопку **Подключиться**.
7. Если в настройках целевого устройства iSCSI включена проверка подлинности CHAP, поступит запрос на учетные данные для доступа к целевому устройству iSCSI. Укажите имя пользователя и секрет целевого устройства, которые указаны в настройках целевого устройства iSCSI. Нажмите кнопку **ОК**.
8. Нажмите кнопку **Закрыть**, чтобы закрыть окно.

Для добавления устройства iSCSI на загрузочный носитель на основе PE

1. Нажмите **Инструменты** > **Запустить установку iSCSI**.
2. Выберите кладку **Обнаружение**.
3. Под пунктом **Целевые порталы** нажмите кнопку **Добавить**, а затем укажите IP-адрес и порт портала целевого устройства iSCSI. Нажмите кнопку **ОК**.
4. Откройте вкладку **Общие**, нажмите кнопку **Изменить**, а затем укажите имя инициатора iSCSI, который разрешил доступ к устройству.
5. Откройте вкладку **Цели**, нажмите кнопку **Обновить**, выберите целевое устройство iSCSI в списке, а затем нажмите кнопку **Подключить**. Нажмите кнопку **ОК**, чтобы подключиться к целевому устройству iSCSI.
6. Если в настройках целевого устройства iSCSI включена проверка подлинности CHAP, отобразится ошибка **Сбой аутентификации**. В этом случае щелкните **Подключиться**, затем щелкните **Дополнительно**, установите флажок **Включить вход CHAP** и укажите имя пользователя и секрет целевого устройства, которые указаны в настройках целевого устройства iSCSI. Нажмите кнопку **ОК**, чтобы закрыть окно, затем нажмите кнопку **ОК**, чтобы подключиться к целевому устройству iSCSI.
7. Нажмите кнопку **ОК**, чтобы закрыть окно.

Для добавления устройства NDAS (только на загрузочный носитель на основе Linux)

1. Нажмите **Инструменты** > **Настроить устройства iSCSI/NDAS**.

2. Щелкните **Устройства NDAS** и нажмите кнопку **Добавить устройство**.
3. Укажите 20-значный идентификатор устройства.
4. Чтобы разрешить запись данных на устройство, укажите пятизначный ключ записи. Без этого ключа устройство будет доступно только для чтения.
5. Нажмите кнопку **ОК**.
6. Нажмите кнопку **Закрыть**, чтобы закрыть окно.

10.5 Startup Recovery Manager

Startup Recovery Manager — это загрузочный компонент, находящийся на системном диске Windows или в разделе /boot Linux и настроенный на запуск во время загрузки системы при нажатии клавиши F11. При его использовании не требуется отдельный носитель или сетевое подключение для запуска загрузочной утилиты аварийного восстановления.

Startup Recovery Manager особенно полезен для мобильных пользователей. В случае сбоя перезагрузите машину, дождитесь появления запроса «Press F11 for Acronis Startup Recovery Manager...» и нажмите клавишу F11. Программа запустится, и можно будет выполнить восстановление.

Кроме того, с помощью Startup Recovery Manager можно «на ходу» выполнять резервное копирование.

На машинах с установленным загрузчиком GRUB пользователь не нажимает клавишу F11, а выбирает Startup Recovery Manager в меню загрузки.

Машина, загруженная с помощью Startup Recovery Manager, может быть зарегистрирована на сервере управления таким же образом, как машина, загруженная с загрузочного носителя. Для этого выберите **Инструменты** > **Зарегистрировать носитель на сервере управления**, а затем следуйте пошаговой процедуре, описанной в разделе «Регистрация носителя на сервере управления» (стр. 184).

Активация Startup Recovery Manager

На машине, где работает агент для Windows или агент для Linux, Startup Recovery Manager можно активировать с помощью консоли резервного копирования.

Для активации Startup Recovery Manager с помощью консоли резервного копирования

1. Выберите машину, на которой нужно активировать Startup Recovery Manager.
2. Нажмите **Сведения**.
3. Активируйте переключатель **Startup Recovery Manager**.
4. Дождитесь активации Startup Recovery Manager программным обеспечением.

Для активации Startup Recovery Manager на машине без агента

1. Загрузите машину с загрузочного носителя.
2. Выберите **Инструменты** > **Активировать Startup Recovery Manager**.
3. Дождитесь активации Startup Recovery Manager программным обеспечением.

Что происходит при активации Startup Recovery Manager

Активация включает при загрузке подсказку «Press F11 for Acronis Startup Recovery Manager...» (при отсутствии загрузчика GRUB) или добавляет пункт «Startup Recovery Manager» в меню загрузчика GRUB (при его наличии).

Для активации Startup Recovery Manager системный диск (или раздел /boot в Linux) должен иметь по крайней мере 100 МБ свободного пространства.

За исключением случая, когда используется загрузчик GRUB и он установлен в основную загрузочную запись (MBR), активация Startup Recovery Manager перезаписывает основную загрузочную запись (MBR) своим собственным загрузочным кодом. Таким образом, при использовании загрузчиков сторонних производителей может потребоваться их повторное активирование.

В ОС Linux при использовании загрузчика, отличного от GRUB (такого как LILO), возможна его установка в загрузочную запись корневого (или загрузочного) раздела Linux вместо MBR до активации Startup Recovery Manager. В противном случае измените конфигурацию этого загрузчика вручную после активации.

Деактивация Startup Recovery Manager

Деактивация выполняется аналогично активации.

Деактивация отключает подсказку «Press F11 for Acronis Startup Recovery Manager…» при загрузке (или пункт меню в GRUB). Если Startup Recovery Manager не активирован, для восстановления системы, которая не смогла загрузиться, требуется выполнить одно из следующих действий:

- загрузить машину с отдельного загрузочного носителя.
- использовать сеть, чтобы загрузиться с PXE-сервера или службы удаленной установки Microsoft (RIS).

10.6 PXE-сервер Acronis

PXE Server Acronis служит для загрузки машин в загрузочные компоненты Acronis через сеть.

Загрузка по сети:

- устраняет потребность в специалисте для установки загрузочного носителя в систему, которая должна быть загружена;
- при групповых операциях снижает количество времени, требуемого для загрузки нескольких машин, по сравнению с использованием физического загрузочного носителя.

Загрузочные компоненты загружаются на PXE Server Acronis при помощи мастера создания загрузочных носителей Acronis. Чтобы загрузить загрузочные компоненты, запустите мастер создания загрузочных носителей и следуйте пошаговым инструкциям, описанным в разделе «Загрузочные носители на основе Linux» (стр. 168).

Загрузка нескольких машин с PXE Server Acronis имеет смысл, если в сети присутствует DHCP-сервер. При этом сетевые интерфейсы загруженных машин автоматически получат IP-адреса.

Ограничение:

PXE Server Acronis не поддерживает загрузчик UEFI.

10.6.1 Установка PXE-сервера Acronis

Порядок установки PXE-сервера Acronis

1. Войдите как администратор и запустите программу установки Acronis Backup Advanced.

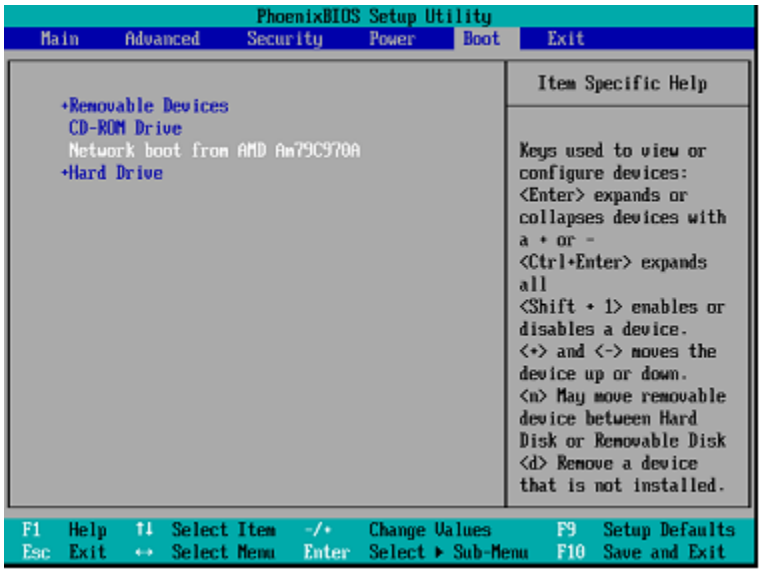
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Установка языка**.
3. Примите условия лицензионного соглашения и укажите, будет ли машина участвовать в программе улучшения качества Acronis Customer Experience Program (CEP).
4. Щелкните **Настройка параметров установки**.
5. Рядом с пунктом **Устанавливаемые компоненты** щелкните **Изменить**.
6. Установите флажок **PXE Server**. Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки. Чтобы продолжить, нажмите кнопку **Готово**.
7. [Необязательно] Измените другие настройки установки.
8. Нажмите **Установить**, чтобы продолжить установку.
9. После завершения установки нажмите кнопку **Закрыть**.

PXE-сервер Acronis запускается в виде службы сразу же после установки. Позже он автоматически стартует при каждом запуске операционной системы. Остановить или запустить PXE-сервер Acronis можно так же, как службу Windows.

10.6.2 Настройка машины на загрузку с PXE

В случае «голого железа» достаточно, чтобы система BIOS машины поддерживала сетевую загрузку.

На тех машинах, операционная система которых расположена на жестком диске, система BIOS должна быть настроена так, чтобы сетевая интерфейсная плата была первым загрузочным устройством либо чтобы она предшествовала жесткому диску в приоритете загрузки. На следующем примере показана одна из приемлемых конфигураций BIOS. Если в машину не вставлен загрузочный носитель, будет производиться загрузка по сети.



В некоторых версиях BIOS необходимо сохранить изменения BIOS после включения сетевой интерфейсной платы, чтобы плата появилась в списке загрузочных устройств.

Если установлено несколько сетевых интерфейсных плат, убедитесь, что к плате, поддерживаемой BIOS, подключен сетевой кабель.

10.6.3 Работа в подсетях

Чтобы Acronis PXE-сервер мог работать в другой подсети (подключенной через коммутатор), необходимо настроить коммутатор для передачи трафика PXE. IP-адреса PXE-сервера настраиваются отдельно для каждого интерфейса с помощью вспомогательной службы IP таким же способом, как адреса DHCP-сервера. Дополнительные сведения см. на странице https://support.microsoft.com/en-us/help/257579/pxe-clients-do-not-receive-an-ip-address-from-a-dhcp-server.

11 Защита мобильных устройств

Чтобы выполнить резервное копирование и восстановление данных на мобильных устройствах, используйте приложение резервного копирования.

Поддерживаемые мобильные устройства

- Смартфоны и планшетные ПК с Android 4.1 или более поздней версии.
- Устройства iPhone, iPad и iPod с iOS 8 или более поздней версии.

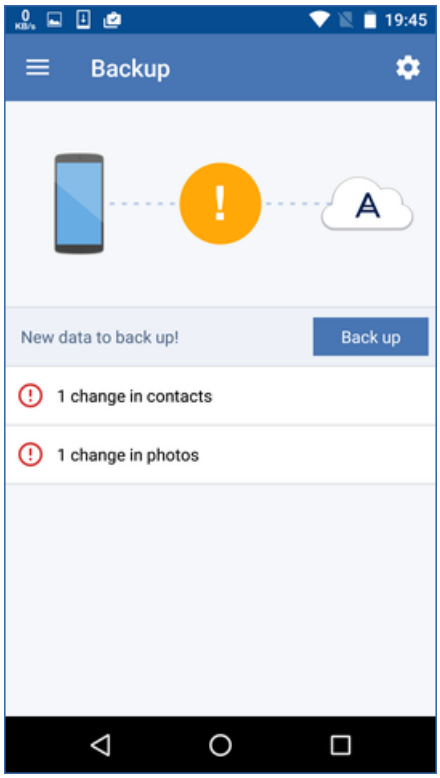
Данные, для которых можно создать резервную копию

- Контакты
- Фотографии
- Видео
- Календари
- Текстовые сообщения (только в устройствах Android)
- Напоминания (только в устройствах iOS)

Что необходимо знать?

- Скопировать данные можно только в облачное хранилище данных.

- При каждом открытии приложения отображаются итоговые изменения данных. Вы можете приступить к созданию резервной копии вручную.



- Функция **Непрерывное резервное копирование** включена по умолчанию. В этом режиме приложение резервного копирования проверяет изменения данных каждые шесть часов и автоматически запускает резервное копирование, если некоторые данные изменены. Можно отключить непрерывное резервное копирование или изменить его на **Только при зарядке** в настройках приложения.
- Можно получить доступ к данным резервной копии с любого мобильного устройства, зарегистрированного в вашей учетной записи. Это поможет передать данные со старого мобильного устройства на новое. Контакты и фотографии с устройства Android можно восстановить на устройство iOS и в обратном порядке. Кроме того, на компьютер можно загрузить фотографии, видео или контакты, используя консоль резервного копирования.
- Данные, для которых резервная копия создана с мобильных устройств, зарегистрированных в вашей учетной записи, доступны только в этой учетной записи. Кроме вас, никто не сможет просмотреть или восстановить эти данные.
- В приложении резервного копирования можно восстановить данные только с последней резервной копии. Если необходимо выполнить восстановление с более старых резервных копий, используйте консоль резервного копирования на планшетном ПК или компьютере.
- Правила хранения не применяются к резервным копиям мобильных устройств.
- При наличии SD-карты в ходе выполнения резервного копирования хранящиеся на ней данные также будут скопированы. Эти данные будут восстановлены на SD-карту, если она будет доступна при восстановлении. В противном случае они будут восстановлены на внутреннее хранилище данных.
- Независимо от того, были ли оригинальные данные сохранены во внутреннем хранилище устройства или на SIM-карте, данные будут восстанавливаться во внутреннее хранилище данных.

Пошаговые инструкции

Порядок получения приложения резервного копирования

1. На мобильном устройстве откройте браузер и введите URL-адрес https://backup.acronis.com/.
2. Войдите, используя свою учетную запись Acronis.
3. Щелкните **Все устройства** > **Добавить**.
4. В разделе **Мобильные устройства** выберите тип устройства.

   В зависимости от типа устройства будет выполнено перенаправление в App Store или Google Play Store.
5. [Только в устройствах iOS] Щелкните **Получить**.
6. Щелкните **Установить**, чтобы установить приложение резервного копирования.

Порядок создания резервной копии устройства iOS

1. Откройте приложение резервного копирования.
2. Войдите, используя свою учетную запись Acronis.
3. Выберите категории данных, резервную копию которых необходимо создать. По умолчанию выбраны все категории.
4. Коснитесь значка **Создать резервную копию сейчас**.
5. Разрешите приложению получать доступ к вашим личным данным. Если вы запретите доступ к некоторым категориям данных, для них не будет создана резервная копия.

Начнется резервное копирование.

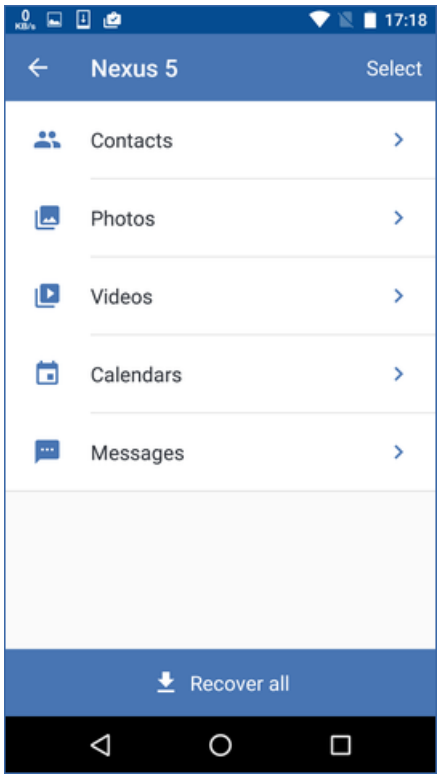
Порядок создания резервной копии устройства Android

1. Откройте приложение резервного копирования.
2. Войдите, используя свою учетную запись Acronis.
3. [В Android 6.0 и более поздних версий] Разрешите приложению получать доступ к вашим личным данным. Если вы запретите доступ к некоторым категориям данных, для них не будет создана резервная копия.
4. [Дополнительно] Выберите категории данных, для которых не нужно создавать резервную копию. Для этого коснитесь значка шестерни, коснитесь ползунков для категорий данных, которые необходимо исключить из резервного копирования, а затем коснитесь стрелки назад.
5. Коснитесь значка **Создать резервную копию**.

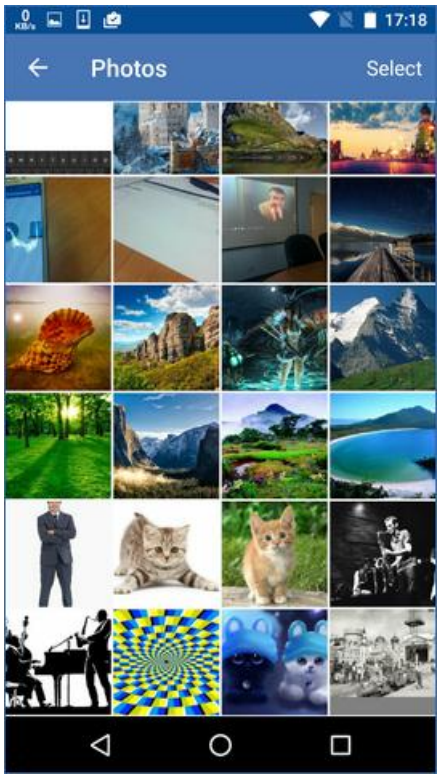
Порядок восстановления данных на мобильное устройство

1. Откройте приложение резервного копирования.
2. Смахните влево и коснитесь **Доступ и восстановление**.
3. Коснитесь имени устройства.
4. Выполните одно из следующих действий:
   - Чтобы восстановить все данные, для которых создана резервная копия, коснитесь **Восстановить все**. Никаких дополнительных действий не требуется.
   - Чтобы восстановить одну или несколько категорий данных, коснитесь **Выбрать**, затем коснитесь флажков для требуемых категорий данных. Коснитесь значка **Восстановить**. Никаких дополнительных действий не требуется.

- Чтобы восстановить один или несколько элементов данных, которые принадлежат к одной категории данных, коснитесь этой категории данных. Продолжите выполнять дальнейшие действия.



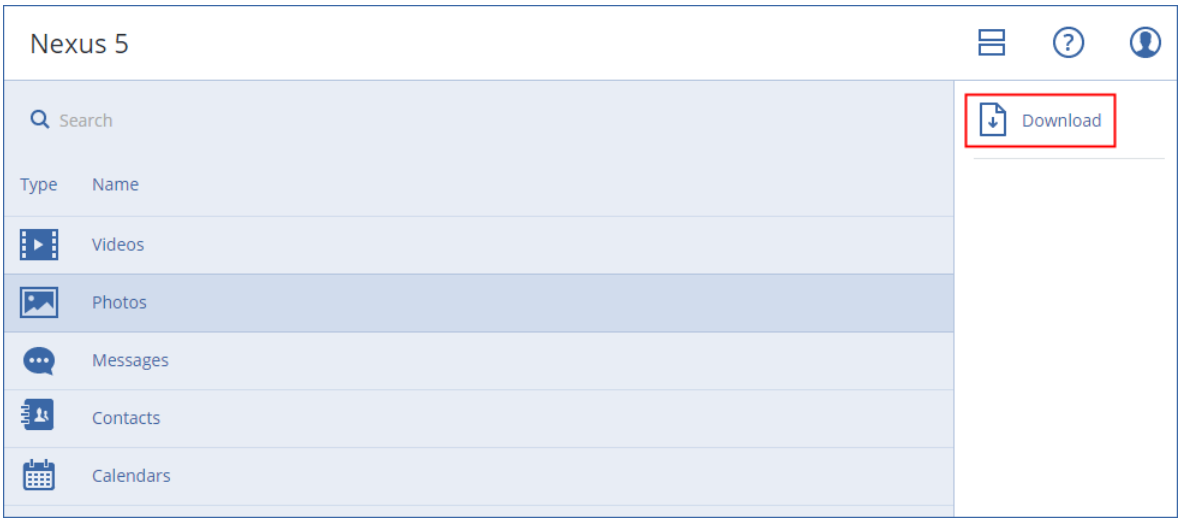
5. Выполните одно из следующих действий:
   - Чтобы восстановить один элемент данных, коснитесь его.
   - Чтобы восстановить несколько элементов данных, коснитесь **Выбрать**, затем коснитесь флажков для требуемых элементов данных.



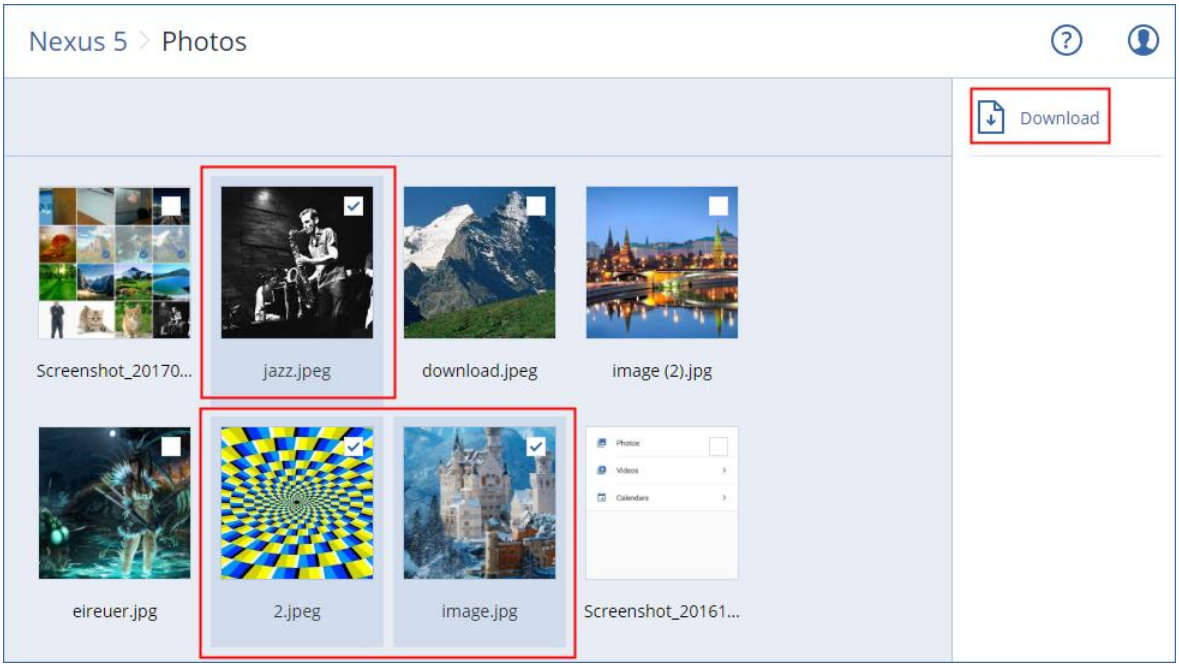
6. Коснитесь значка **Восстановить**.

Порядок получения доступа к данным через консоль резервного копирования

1. На другом компьютере откройте браузер и перейдите на сайт https://backup.acronis.com/.
2. Войдите, используя свою учетную запись Acronis.
3. На вкладке **Все устройства** выберите имя мобильного устройства, затем щелкните **Восстановление**.
4. Выберите точку восстановления.
5. Выполните любое из следующих действий:
   - Чтобы загрузить все фотографии, видео или контакты, выберите соответствующую категорию данных. Нажмите кнопку **Загрузить**.



   - Чтобы загрузить отдельные фотографии, видео или контакты, щелкните имя соответствующей категории данных, а затем установите флажки для требуемых элементов данных. Нажмите кнопку **Загрузить**.



   - Для предварительного просмотра текстового сообщения, фотографии или контакта, щелкните имя соответствующей категории данных, затем щелкните требуемый элемент данных.

Дополнительную информацию см. по ссылке http://www.acronis.com/redirector/products/atimobile/docs/?lang=ru. Эта справка также доступна в приложении резервного копирования (в меню приложения последовательно коснитесь пунктов **Настройки** > **Справка**).

12 Защита приложений Microsoft

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

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 резервного копирования 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 или на Microsoft Office 365. Резервное копирование почтовых ящиков поддерживается Microsoft Exchange Server 2010 Service Pack 1 (SP1) и более поздней версии.

Защита Microsoft SharePoint

Ферма Microsoft SharePoint состоит из серверов веб-интерфейса, на которых выполняются службы SharePoint, серверов баз данных, на которых выполняется Microsoft SQL Server и (необязательно) серверов приложений, которые разгружают серверы веб-интерфейса от некоторых служб SharePoint. Некоторые серверы веб-интерфейса и серверы приложений могут быть идентичны друг другу.

Чтобы защитить всю ферму SharePoint, выполните указанные ниже действия:

- Создайте резервные копии серверов базы данных, выполнив резервное копирование с поддержкой приложений.
- Создайте резервные копии всех уникальных серверов веб-интерфейса и серверов приложений, выполнив обычное резервное копирование на уровне дисков.

Резервные копии всех серверов должны быть выполнены по одному расписанию.

Чтобы защитить только содержимое, можно создать резервные копии баз данных по отдельности.

Защита контроллера домена

Машину под управлением доменных служб Active Directory можно защитить резервным копированием с поддержкой приложений. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

Восстановление приложений

В таблице приведена сводка доступных методов восстановления приложений.

	Из резервной копии базы данных	Из резервной копии с поддержкой приложений	Из резервной копии диска
Microsoft SQL Server	Базы данных в запущенный экземпляр SQL Server (стр. 205) Базы данных как файлы (стр. 205)	Вся машина (стр. 136) Базы данных в запущенный экземпляр SQL Server (стр. 205) Базы данных как файлы (стр. 205)	Вся машина (стр. 136)
Microsoft Exchange Server	Базы данных в запущенный Exchange (стр. 208) Базы данных как файлы (стр. 208) Фрагментарное восстановление в запущенный Exchange или Office 365 (стр. 211)*	Вся машина (стр. 136) Базы данных в запущенный Exchange (стр. 208) Базы данных как файлы (стр. 208) Фрагментарное восстановление в запущенный Exchange или Office 365 (стр. 211)*	Вся машина (стр. 136)
Серверы базы данных Microsoft SharePoint	Базы данных в запущенный экземпляр SQL Server (стр. 205) Базы данных как файлы (стр. 205) Фрагментарное восстановление с использованием SharePoint Explorer	Вся машина (стр. 136) Базы данных в запущенный экземпляр SQL Server (стр. 205) Базы данных как файлы (стр. 205) Фрагментарное восстановление с использованием SharePoint Explorer	Вся машина (стр. 136)
Интерфейсные веб-серверы Microsoft SharePoint	–	–	Вся машина (стр. 136)
Доменные службы Active Directory	–	Вся машина (стр. 136)	–

* Фрагментарное восстановление также доступно из резервной копии почтового ящика.

12.1 Предварительные требования

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

Чтобы проверить состояние модулей записи VSS, используйте команду **`vssadmin list writers`**.

Общие требования

Для Microsoft SQL Server убедитесь, что выполнены указанные ниже требования:

- Запущен хотя бы один экземпляр Microsoft SQL Server.
- Модуль записи SQL для VSS включен.

Для Microsoft Exchange Server убедитесь, что выполнены указанные ниже требования:

- Запущена служба банка данных Microsoft Exchange.
- Установлена оболочка Windows PowerShell. 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.

На контроллере домена убедитесь, что:

- Модуль записи Active Directory для VSS включен.

При создании плана резервного копирования убедитесь, что:

- Для физических машин включен параметр резервного копирования Служба теневого копирования томов (VSS) (стр. 133).
- Для виртуальных машин включен параметр резервного копирования Служба теневого копирования томов (VSS) для виртуальных машин (стр. 134).

Дополнительные требования для операций резервного копирования с поддержкой приложений

При создании плана резервного копирования убедитесь, что для резервного копирования выбран параметр **Вся машина**.

Если приложения выполняются на виртуальных машинах, резервная копия которых создана агентом для VMware, убедитесь в том, что:

- Виртуальные машины для резервного копирования соответствуют требованиям совместимого с приложениями замораживания, которые перечислены в следующей статье базы знаний VMware: https://pubs.vmware.com/vsphere-6-5/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBkupVadp.9.6.html
- На машинах установлен и обновлен набор утилит VMware Tools.
- Учетные записи пользователей (UAC) отключены на машинах. Если вы не хотите отключать учетные записи пользователей (UAC), то при включении резервного копирования приложения необходимо предоставить учетные данные встроенного администратора домена (DOMAIN\Administrator).

12.2 Резервная копия базы данных

Прежде чем приступить к созданию резервных копий баз данных, убедитесь, что выполнены требования, перечисленные в разделе «Предварительные требования» (стр. 196).

Выберите базы данных, как указано ниже, а затем укажите другие настройки плана резервного копирования в зависимости от требований (стр. 73).

12.2.1 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. Сокращение журнала SQL можно отключить в параметрах плана резервного копирования (стр. 122).

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 нажмите на элемент 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. Дополнительные сведения о резервном копировании групп AAG см. в разделе «Защита групп Always On Availability Groups (AAG)» (стр. 199).
   - 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. Нажмите кнопку **Резервное копирование**. Если потребуется, введите учетные данные для доступа к SQL Server. Соответствующая учетная запись должна входить в группу **Операторы архива** или **Администраторы** на этой машине, а также иметь роль **системный администратор** в каждом из экземпляров, для которых создается резервная копия.

12.2.2 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	Базы данных, Группы обеспечения доступности баз данных (DAG)	Участие в группе ролей **Управление организацией**.

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) сервера Exchange, машины, на которых запущен сервер Microsoft Exchange, базы данных и почтовые ящики.
2. Перейдите к данным, для которых требуется создать резервные копии.

   Разверните узлы дерева или дважды нажмите на элемент списка, расположенного справа от дерева.
3. Выберите данные, резервную копию которых необходимо создать. Выберите DAG, машины, на которых запущен сервер Microsoft Exchange, отдельные базы данных или почтовые ящики.
   - При выборе DAG будет создана резервная копия всех баз данных , включенных в выбранную DAG. Дополнительные сведения о резервном копировании групп DAG см. в разделе«Защита групп обеспечения доступности базы данных (DAG)» (стр. 201).
   - 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.
   - При выборе почтовых ящиков, будет создана резервная копия только выбранных почтовых ящиков. Дополнительные сведения о резервном копировании отдельных почтовых ящиков см. в разделе«Резервное копирование почтовых ящиков» (стр. 204).
4. Если потребуется, введите учетные данные для доступа к информации.
5. Нажмите кнопку **Резервное копирование**.

12.2.3 Защита группы Always On Availability Groups (AAG)

Обзор решений для SQL Server высокой доступности

Функция отказоустойчивой кластеризации Windows Server (WSFC) позволяет настроить SQL-сервер с высоким уровнем доступности посредством избыточности на уровне экземпляра (экземпляр отказоустойчивого кластера, FCI) или на уровне базы данных (AlwaysOn Availability Group, AAG). Оба метода можно сочетать.

В экземпляре отказоустойчивого кластера базы данных SQL расположены в общем хранилище. Доступ к этому хранилищу возможен только с активного узла кластера. При сбое активного узла происходит переход, и активным становится другой узел.

В группе обеспечения доступности все реплики баз данных располагаются на разных узлах. Если основная реплика становится недоступна, основная роль назначается дополнительной реплике, расположенной на другом узле.

Таким образом, уже сами кластеры являются решением по аварийному восстановлению. Однако в некоторых случаях кластеры не могут обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера. Кроме того, кластерные решения не защищают от вредоносных изменений содержимого, поскольку обычно эти изменения немедленно реплицируются на все узлы кластера.

Поддерживаемые конфигурации кластеров

Acronis Backup поддерживает *только* Always On Availability Group (AAG) для SQL Server версии 2012 или более новой. Прочие конфигурации кластеров, такие как, например, Failover Cluster Instances, зеркальное отображение базы данных и доставка журналов, *не* поддерживаются.

Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления данных кластера необходимо установить агент для SQL на каждом узле кластера WSFC.

В AAG включено резервное копирование баз данных

1. Установите агент для SQL на каждый узел кластера WSFC.

   Подсказка *После установки агента на одном из узлов программное обеспечение отобразит AAG и ее узлы в поле* ***Устройства*** *>* ***Microsoft SQL*** *>* ***Базы данных****. Для установки агента для SQL на остальных узлах выберите AAG, нажмите* ***Сведения****, после чего нажмите* ***Установить агент*** *возле каждого узла.*

2. Выберите AAG для создания резервной копии в соответствии с инструкциями «Выбор баз данных SQL» (стр. 198).

   Важно! *Вы должны выбрать именно AAG, а не отдельные содержащиеся в ней узлы и базы данных. Если вы выберете отдельные элементы, содержащиеся в AAG, резервные копии не будут поддерживать кластеры и будут созданы резервные копии только выбранных копий элементов.*

3. Настройте параметр резервного копирования «Способ резервного копирования кластера» (стр. 116).

Восстановление баз данных, включенных в AAG

1. Выберите базы данных, которые необходимо восстановить, а затем выберите желаемую точку восстановления данных.

   При переходе **Устройства** > **Microsoft SQL** > **Базы данных**, выборе кластеризованной базы данных и нажатии **Восстановить**, программное обеспечение отобразит только те точки восстановления, которые соответствуют временам создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных — выбор резервной копии всей AAG на вкладке «Резервные копии» (стр. 158). Имена резервных копий AAG помечены особым значком и составляются по следующему шаблону: `<имя AAG> - <имя плана резервного копирования>`.

2. Для конфигурирования восстановления выполните действия, описанные в разделе «Восстановление баз данных SQL» (стр. 205) (начиная с шага 5).

Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

Важно! *База данных, включенная в группу Always On Availability Group, не может быть перезаписана во время восстановления, поскольку это запрещено правилами Microsoft SQL Server. Необходимо исключить целевую базу данных из AAG перед восстановлением. Либо можно просто восстановить базу данных как новую базу, не входящую в AAG. После завершения восстановления можно воссоздать исходную конфигурацию AAG.*

12.2.4 Защита групп обеспечения доступности базы данных (DAG)

Обзор кластеров Exchange Server

Основная идея кластеров Exchange обеспечить высокую доступность базы данных с быстрым переходом к реплике и без потери данных. Обычно для этого одна или несколько копий баз данных или групп хранения находятся на элементах (узлах) кластера. В случае отказа узла кластера, на котором находится активная копия базы данных, или самой активной копии базы данных, другой узел кластера, содержащий пассивную копию, автоматически берет на себя операции с отказавшего узла и предоставляет доступ к службам Exchange с минимальным простоем. Таким образом, уже сами кластеры являются решением по аварийному восстановлению.

Однако в некоторых случаях решение с использованием отказоустойчивых кластеров не может обеспечить защиту данных: например, при логическом повреждении базы данных, отсутствии копии или реплики какой-то базы данных в кластере или отказе всего кластера. Кроме того, кластерные решения не защищают от вредоносных изменений содержимого, поскольку обычно эти изменения немедленно реплицируются на все узлы кластера.

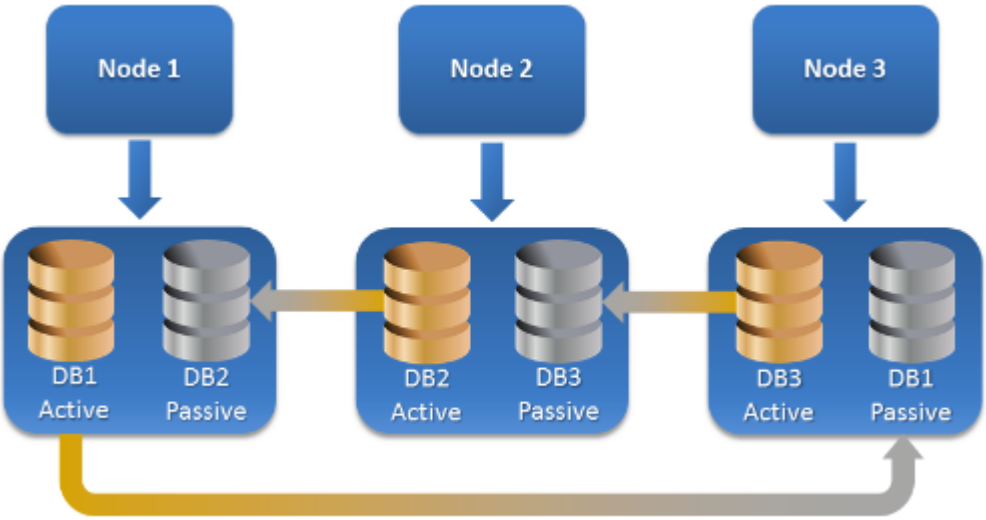
Резервное копирование с поддержкой кластеров

Используя резервное копирование с поддержкой кластеров, вы создаете только одну копию кластеризированных данных. Если данные меняют свое расположение в кластере (например, из-за переключения или перехода к реплике), программное обеспечение отслеживает все перемещения этих данных и благополучно создает их резервную копию.

Поддерживаемые конфигурации кластеров

Резервное копирование с поддержкой кластеров поддерживается *только* для группы обеспечения доступности баз данных (DAG) в Exchange Server 2010 или более поздней версии. Другие кластерные конфигурации, такие как кластер с единым хранилищем (SCC) и непрерывная репликация кластера (CCR) для Exchange 2007 *не* поддерживаются.

Группа DAG включает до 16 серверов почтовых ящиков Exchange. На любом узле может располагаться копия базы данных почтовых ящиков с любого другого узла. Каждый узел может содержать пассивные и активные копии базы данных. Может быть создано до 16 копий каждой базы данных.



Сколько требуется агентов для резервного копирования и восстановления данных кластера?

Для успешного резервного копирования и восстановления кластеризованных баз данных необходимо установить агент для Exchange на каждом узле кластера Exchange.

Подсказка *После установки агента на одном из узлов программное обеспечение отобразит DAG и ее узлы в поле* ***Устройства*** *>* ***Microsoft Exchange*** *>* ***Базы данных****. Для установки агента для Exchange на остальных узлах выберите DAG, нажмите* ***Сведения****, после чего нажмите* ***Установить агент*** *возле каждого узла.*

Создание резервной копии данных кластера Exchange

1. При создании плана резервного копирования выберите DAG в соответствии с инструкциями в разделе «Выбор данных Exchange Server» (стр. 198).
2. Настройте параметр резервного копирования «Способ резервного копирования кластера» (стр. 116).
3. Укажите другие необходимые (стр. 73) настройки плана резервного копирования.

Важная информация *Для резервного копирования с поддержкой кластеров необходимо выбрать саму группу обеспечения доступности баз данных. Если выбрать отдельные узлы или базы данных в группе обеспечения доступности баз данных, то будет создана резервная копия только для выбранных элементов, а параметр* ***Способ резервного копирования кластера*** *будет проигнорирован.*

Восстановление данных кластера Exchange

1. Если в разделе **Устройства** > **Microsoft Exchange** > **Базы данных** выбрать кластеризованную базу данных и нажать кнопку **Восстановить**, программное обеспечение покажет только те точки восстановления, которые соответствуют временам создания резервной копии выбранной копии базы данных.

   Самый легкий способ просмотра всех точек восстановления кластеризованной базы данных — выбор соответствующей резервной копии на вкладке «Резервные копии» (стр. 158).
2. Для конфигурирования восстановления выполните действия, описанные в разделе «Восстановление баз данных Exchange» (начиная с шага 5).

Программное обеспечение автоматически определяет узел кластера, на который будут восстановлены данные. Имя узла отображается в поле **Восстановить на**. Вы можете вручную изменить целевой узел.

12.3 Резервное копирование с поддержкой приложений

Резервная копия на уровне дисков с поддержкой приложений доступна для физических машин и виртуальных машин ESXi.

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 приложения.

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. Сокращение журнала SQL можно отключить в параметрах плана резервного копирования (стр. 122). Журналы транзакций Exchange сокращаются только на виртуальных машинах. Чтобы сократить журналы транзакций Exchange на физической машине, можно включить параметр полного восстановления VSS (стр. 133).
4. Если домен содержит несколько контроллеров домена, то при восстановлении одного из них выполняется непринудительное восстановление; при этом откат USN не выполняется после восстановления.

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).

Другие требования перечислены в разделах «Предварительные требования» (стр. 196) и «Необходимые права пользователя» (стр. 203).

12.3.1 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 ролей **Администраторы организации Exchange**.

  Exchange 2010 и более поздней версии: Данная учетная запись должна входить в группу ролей **Управление организацией**.
- Для Active Directory:

  Данная учетная запись должна быть администратором домена.

12.4 Резервная копия почтового ящика

Резервная копия почтового ящика доступна, если на сервере управления зарегистрирован по меньшей мере один агент для Exchange. Этот агент должен быть установлен на машине, которая находится в одном лесу Active Directory с сервером Microsoft Exchange Server.

Перед выполнением резервного копирования почтовых ящиков вы должны подключить агент для Exchange к машине с серверной ролью (CAS) **Client Access** сервера Microsoft Exchange Server.

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.
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 данные учетной записи, которая входит в состав группы роли **Управление организацией**.
10. Нажмите кнопку **Добавить**.

В результате почтовый ящик будет находиться по пути **Устройства** > **Microsoft Exchange** > **Почтовые ящики**.

12.4.1 Выбор почтовых ящиков сервера Exchange

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 73).

Выбор почтовых ящиков Exchange

1. Нажмите **Устройства** > **Microsoft Exchange**.

   Программное обеспечение отобразит дерево баз данных и почтовых ящиков Exchange
2. Нажмите **Почтовые ящики**, после чего выберите почтовые ящики, для которых необходимо создать резервные копии.
3. Нажмите кнопку **Резервное копирование**.

12.5 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» (стр. 208).

Если используется только агент для VMware, то единственный доступный метод восстановления — восстановить базы данных как файлы.

Системные базы данных восстанавливаются в целом так же, как и пользовательские. Особенности этой процедуры описаны в разделе «Восстановление системных баз данных» (стр. 207).

/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 «Резервные копии» (стр. 158).

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: 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. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается 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 «Резервные копии» (стр. 158).

   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. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

12.5.1 Восстановление системных баз данных

Все системные базы данных экземпляра восстанавливаются одновременно. При восстановлении системных баз программа автоматически перезапускает целевой экземпляр в однопользовательском режиме. После завершения восстановления программа перезапускает экземпляр и восстанавливает другие базы данных (если есть).

При восстановлении системной базы данных также обращайте внимание на перечисленные ниже моменты.

- Системные базы данных можно восстановить только на экземпляре той же версии, что и исходный.
- Системные базы данных всегда восстанавливаются в состоянии «готово к использованию».

Восстановление базы данных master

В число системных баз данных входит база **master**. В базе данных **master** содержатся сведения обо всех базах данных экземпляра. Это означает, что база данных **master** в резервной копии содержит информацию о базах данных, существовавших в экземпляре на момент резервного копирования. После восстановления базы данных **master** может потребоваться следующее.

- Базы данных, которые появились в экземпляре после выполнения резервного копирования, становятся невидимыми для экземпляра. Чтобы снова перевести их в режим эксплуатации, прикрепите их к экземпляру вручную с помощью SQL Server Management Studio.
- Базы данных, которые были удалены после выполнения резервного копирования, отображаются в экземпляре как находящиеся в автономном режиме. Удалите эти базы данных с помощью SQL Server Management Studio.

12.5.2 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. Щелкните правой кнопкой мыши пункт **Базы данных** и выберите **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 **ОК**.

12.6 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	Базы данных	Участие в группе ролей **Управление организацией**.

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 (стр. 210).

Если используется только агент для VMware, то единственный доступный метод восстановления — восстановить базы данных как файлы.

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 «Резервные копии» (стр. 158).

   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. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается 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 «Резервные копии» (стр. 158).

   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. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается на вкладке **Действия**.

12.6.1 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). При восстановлении базы данных в другое хранилище (например, новую базу данных или в качестве базы данных восстановления) базу данных

невозможно подключить до тех пор, пока она не будет переведена в состояние «Чистое отключение» с использованием команды **`Eseutil /r <Enn>`**. **`<Enn>`** указывает префикс файла журнала для базы данных (или группы хранилища данных, которая содержит базу данных), к которой 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:

- Exchange 2016: http://technet.microsoft.com/ru-ru/library/aa998871.aspx
- Exchange 2013: http://technet.microsoft.com/ru-ru/library/aa998871(v=EXCHG.150).aspx
- Exchange 2010: http://technet.microsoft.com/ru-ru/library/aa998871(v=EXCHG.141).aspx
- Exchange 2007: http://technet.microsoft.com/ru-ru/library/aa998871(v=EXCHG.80).aspx

12.7 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 или на Microsoft Office 365.

Какие элементы можно восстановить?

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.

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.

Восстановить в Office 365

Восстановление можно выполнить из резервных копий Microsoft Exchange Server 2010 и более поздней версии.

Если почтовый ящик восстанавливается в существующий почтовый ящик Office 365, существующие элементы не будут затронуты, а восстановленные элементы будут помещены рядом с ними.

При восстановлении одного почтового ящика необходимо выбрать целевой ящик Office 365. При восстановлении нескольких почтовых ящиков в рамках одной операции восстановления программное обеспечение попытается восстановить каждый почтовый ящик в почтовый ящик пользователя с именем того пользователя, ящик которого восстанавливается. Если такой пользователь не найден, почтовый ящик пропускается. Если некоторые почтовые ящики будут пропущены, восстановление продолжится с предупреждением. Если все почтовые ящики будут пропущены, восстановление завершится сбоем.

Дополнительную информацию о восстановлении Office 365 см. в разделе «Защита почтовых ящиков Office 365» (стр. 217).

12.7.1 Восстановление почтовых ящиков

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

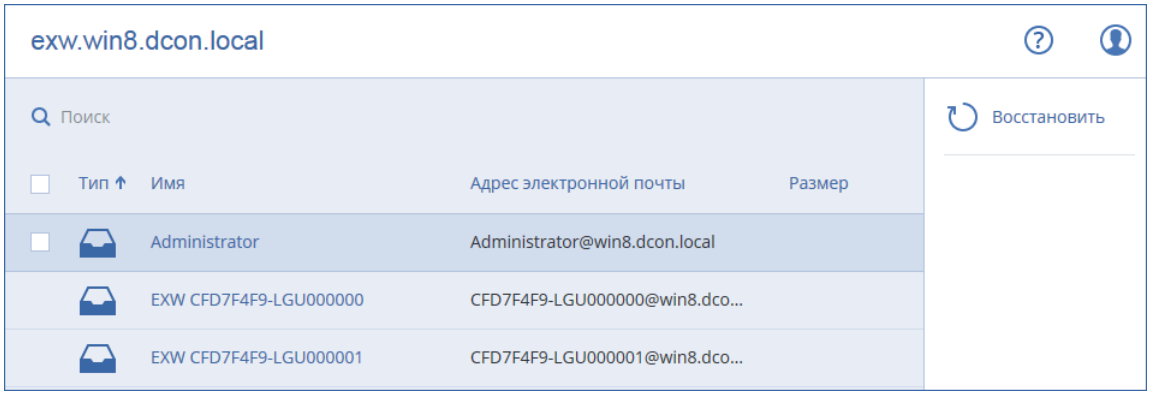
1. [Только при восстановлении из базы данных в Office 365] Если агент для Office 365 не установлен на машине, резервная копия которой создается, выполните одно из указанных ниже действий:
   - Если в вашей организации нет агента для Office 365, установите агент для Office 365 на машине, резервная копия которой создана.
   - Если в вашей организации уже есть агент для Office 365, скопируйте библиотеки с машины, резервная копия которой была создана на машине с агентом Office 365, как описано в таблице по ссылке http://kb.acronis.com/content/33029.

2. 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.
3. Щелкните **Восстановление**.
4. 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 «Резервные копии» (стр. 158).

   Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.
5. Щелкните **Восстановление** > **Почтовые ящики Exchange**.
6. Выберите почтовые ящики, которые необходимо восстановить.

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



7. Нажмите кнопку **Восстановить**.
8. Восстановление в Office 365
   a. В поле **Восстановить в** выберите пункт **Microsoft Office 365**.
   b. [Если в шаге 6 выбран только один почтовый ящик] В поле **Целевой почтовый ящик** укажите целевой почтовый ящик.
   c. Нажмите кнопку **Запуск восстановления**.

   Для этой процедуры не требуется никаких дополнительных шагов.

   Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.
9. 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 машины, на которой включена роль **Клиентский доступ** Microsoft Exchange Server. Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

При поступлении соответствующего запроса укажите данные учетной записи, которая входит в состав группы роли **Управление организацией**.

10. [Необязательно] Чтобы изменить автоматически выбранную базу данных, щелкните **База данных для воссоздания отсутствующих почтовых ящиков**.
11. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается 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 Резервные копии (стр. 158) 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.

12.7.2 Восстановление элементов почтовых ящиков

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

1. [Только при восстановлении из базы данных в Office 365] Если агент для Office 365 не установлен на машине, резервная копия которой создается, выполните одно из указанных ниже действий:
   - Если в вашей организации нет агента для Office 365, установите агент для Office 365 на машине, резервная копия которой создана.
   - Если в вашей организации уже есть агент для Office 365, скопируйте библиотеки с машины, резервная копия которой была создана на машине с агентом Office 365, как описано в таблице по ссылке http://kb.acronis.com/content/33029.
2. 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.
3. Щелкните **Восстановление**.
4. 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 «Резервные копии» (стр. 158).

Вместо выключенной исходной машины восстановление будет выполнено машиной, которая выбранная для просмотра одним из двух указанных выше действий.

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

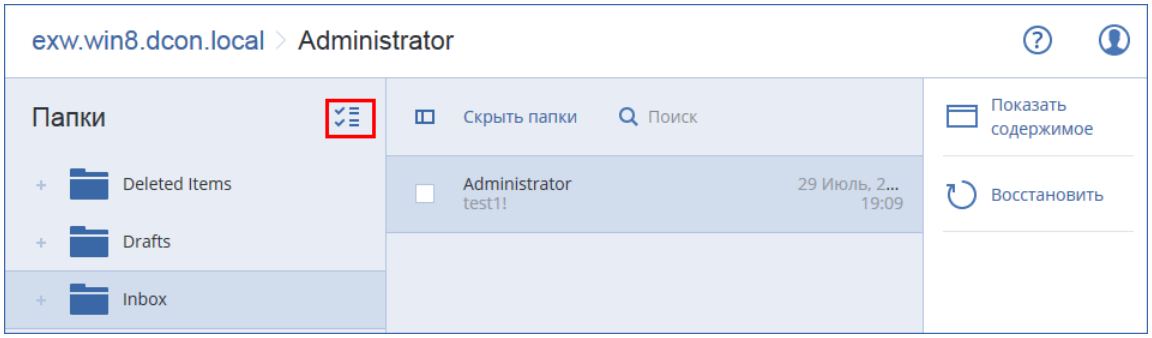
   Доступны указанные ниже параметры поиска. Подстановочные символы не поддерживаются.

   - 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.

   Совет *Чтобы загрузить вложенный файл, щелкните его имя.*

   Чтобы иметь возможность выбрать файлы, щелкните значок восстановления папок.



8. Нажмите кнопку **Восстановить**.
9. Чтобы выполнить восстановление в Office 365, выберите **Microsoft Office 365** в поле **Восстановить в**.

   Чтобы выполнить восстановление на Exchange Server, сохраните значение по умолчанию **Microsoft Exchange** в поле **Восстановить в**.
10. [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 машины, на которой включена роль **Клиентский доступ** Microsoft Exchange Server. Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

    При поступлении соответствующего запроса укажите данные учетной записи, которая входит в состав группы роли **Управление организацией**.

11. 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.
12. [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**.
13. Нажмите кнопку **Запуск восстановления**.

Ход восстановления отображается 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 Резервные копии (стр. 158) 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.

   Совет *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.

12.8 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 доступности Always On, группу обеспечения доступности баз данных, экземпляр SQL Server или машину под управлением Microsoft Exchange Server для которых необходимо изменить учетные данные для доступа.
3. Щелкните **Укажите учетные данные**
4. Укажите новые учетные данные доступа, а затем нажмите кнопку **ОК**.

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

1. Щелкните **Устройства**, а затем щелкните **Microsoft Exchange** > **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**.

13 Защита почтовых ящиков Office 365

Зачем создавать резервную копию почтовых ящиков Office 365?

Несмотря на то что Microsoft Office 365 — это облачный сервис, регулярное создание резервных копий обеспечит дополнительный уровень защиты от ошибок пользователя и преднамеренных вредоносных действий. Удаленные элементы можно восстановить из резервной копии, даже если период хранения в Office 365 истек. Кроме того, можно сохранить локальную копию почтовых ящиков Office 365, если это необходимо в соответствии с нормативными требованиями.

Что необходимо для резервного копирования почтовых ящиков?

Для выполнения резервного копирования почтовых ящиков Office 365 необходимо иметь роль глобального администратора в Microsoft Office 365.

Установите агент для Office 365 на машине Windows, которая подключена к Интернету. В организации должен быть только один агент для Office 365. В облачных развертываниях агент должен быть зарегистрирован под учетной записью администратора самого высокого уровня (администратор клиентов).

- В облачных развертываниях введите учетные данные администратора клиентов при установке агента и при входе в веб-интерфейс.
- Введите учетные данные глобального администратора Office 365 на странице **Microsoft Office 365** веб-интерфейса.

  Агент будет входить в Office 365, используя эту учетную запись. Чтобы обеспечить доступ агента к содержимому всех почтовых ящиков, этой учетной записи будет назначена роль управления **ApplicationImpersonation**.

Восстановление

Из резервной копии почтового ящика можно восстановить следующие элементы:

- почтовые ящики;
- папки электронной почты;
- сообщения электронной почты;
- события календаря;
- задания;
- контакты;
- записи журнала.
- Примечание

Чтобы найти эти элементы, можно воспользоваться поиском.

Восстановление может выполняться в почтовый ящик Microsoft Office 365 или на запущенный сервер Exchange Server.

Если почтовый ящик восстанавливается в существующий почтовый ящик Office 365, существующие элементы с одинаковыми идентификаторами перезаписываются. Если почтовый ящик восстанавливается в существующий почтовый ящик Exchange Server, существующие элементы остаются без изменений. Восстановленные элементы помещаются рядом с ним.

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

Ограничения

- Невозможно создать резервную копию архивированных почтовых ящиков (**архив на месте**).
- Невозможно выполнить восстановление в новый почтовый Office 365. Сначала необходимо создать нового пользователя Office 365, затем восстановить элементы в почтовый ящик этого пользователя.
- Восстановление в учетную запись другой организации Microsoft Office 365 не поддерживается.
- Некоторые типы или свойства, которые поддерживаются в Office 365, могут не поддерживаться Exchange Server. Они будут пропущены при восстановлении на Exchange Server.

13.1 Выбор почтовых ящиков Office 365

Выберите почтовый ящики, как указано ниже, а затем укажите другие настройки плана резервного копирования как требуется (стр. 73).

Порядок выбора почтовых ящиков Microsoft Office 365

1. Щелкните **Microsoft Office 365**.
2. Войдите в Microsoft Office 365 как глобальный администратор при поступлении соответствующего запроса
3. Выберите почтовые ящики, для которых необходимо создать резервные копии.

4. Нажмите кнопку **Резервное копирование**.

13.2 Восстановление почтовых ящиков и элементов почтового ящика Office 365

13.2.1 Восстановление почтовых ящиков

1. [Только при восстановлении в Exchange Server] Убедитесь, что существует пользователь Exchange с таким же именем входа, как и пользователь, почтовый ящик которого восстанавливается. В противном случае создайте пользователя. Другие требования для этого пользователя доступны в теме«Восстановление почтовых ящиков Exchange и элементов почтового ящика» (стр. 211) раздела «Требования для учетных записей пользователя».
2. Щелкните **Устройства** > **Microsoft Office 365**.
3. 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 Резервные копии (стр. 158) и щелкните **Показать резервные копии**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Последовательно выберите пункты **Восстановление** > **Почтовый ящик**.
6. Чтобы выполнить восстановление на Exchange Server, выберите **Microsoft Exchange** в поле **Восстановить в**. Продолжите восстановление, как описано в разделе «Восстановление почтовых ящиков» (стр. 212), начиная с шага 9. Для этой процедуры не требуется никаких дополнительных шагов.

   Чтобы выполнить восстановление в Office 365, сохраните установленное по умолчанию значение **Microsoft Office 365** в поле **Восстановить в**.
7. Раздел **Целевой почтовый ящик** позволяет просмотреть, изменить или указать целевой почтовый ящик.

   По умолчанию выбран исходный почтовый ящик. Если этот почтовый ящик не существует, необходимо указать целевой почтовый ящик.
8. Нажмите кнопку **Запуск восстановления**.

13.2.2 Восстановление элементов почтовых ящиков

1. [Только при восстановлении в Exchange Server] Убедитесь, что существует пользователь Exchange с таким же именем входа, как и пользователь, элементы почтового ящика которого восстанавливаются. В противном случае создайте пользователя. Другие требования для этого пользователя доступны в теме«Восстановление почтовых ящиков Exchange и элементов почтового ящика» (стр. 211) раздела «Требования для учетных записей пользователя».
2. Щелкните **Устройства** > **Microsoft Office 365**.
3. 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 Резервные копии (стр. 158) и щелкните **Показать резервные копии**.

4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Последовательно выберите пункты **Восстановление** > **Сообщения электронной почты**.
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.

   Совет *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: 
7. Нажмите кнопку **Восстановить**.
8. Чтобы выполнить восстановление на Exchange Server, выберите **Microsoft Exchange** в поле **Восстановить в**.

   Чтобы выполнить восстановление в Office 365, сохраните установленное по умолчанию значение **Microsoft Office 365** в поле **Восстановить в**.
9. [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 машины, на которой включена роль **Клиентский доступ** Microsoft Exchange Server. Эта машина должна принадлежать тому же лесу Active Directory, что и машина, которая выполняет восстановление.

   При поступлении соответствующего запроса укажите данные учетной записи, которая входит в состав группы роли **Управление организацией**.
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, 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**.
12. Нажмите кнопку **Запуск восстановления**.

13.3 Изменение учетных данных для доступа к Office 365

Можно изменить учетные данные для доступа к Office 365 без переустановки агента.

Для изменения учетных данных для доступа к Office 365

1. Щелкните **Устройства** > **Microsoft Office 365**.
2. Выберите организацию Office 365.
3. Щелкните **Укажите учетные данные**
4. Введите учетные данные глобального администратора Office 365 и нажмите кнопку **ОК**.

   Агент будет входить в Office 365, используя эту учетную запись. Чтобы обеспечить доступ агента к содержимому всех почтовых ящиков, этой учетной записи будет назначена роль управления **ApplicationImpersonation**.

14 Защита Oracle Database

Защита Oracle Database описана в отдельном документе, который доступен по адресу http://dl2.acronis.com/u/pdf/AcronisBackup_12.5_OracleBackup_whitepaper.pdf

15 Активная защита

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Активная защита обеспечивает защиту системы от вредоносных программ, известных как программы-вымогатели, которые шифруют файлы и требуют выкуп за предоставление ключа шифрования.

Активная защита доступна для машин, работающих под управлением ОС Windows 7 и более поздних версий, а также Windows Server 2008 R2 и более поздних версий. На машине должен быть установлен агент для Windows.

Принцип работы

Активная защита контролирует процессы, выполняемые на защищенной машине. Когда сторонний процесс пытается выполнить шифрование файлов, активная защита выдает уведомление и выполняет дополнительные действия, заданные в конфигурации.

Помимо защиты файлов активная защита предотвращает несанкционированные изменения собственных процессов программного обеспечения для резервного копирования, записей в реестрах, исполняемых файлов и файлов конфигурации, а также основных загрузочных записей защищенной машины.

Для идентификации вредоносных процессов активная защита использует поведенческую эвристику. Активная защита сравнивает цепочку действий, выполняемых процессом, с цепочками событий, записанными в базе данных вредоносных моделей поведения. Этот подход позволяет активной защите обнаруживать новые вредоносные программы по их типичному поведению.

Настройки активной защиты

Для минимизации ресурсов, используемых для эвристического анализа, и устранения так называемых ложноположительных срабатываний, когда доверенная программа рассматриваться как программа-вымогатель, можно задать следующие настройки:

- Доверенные процессы, которые никогда не рассматриваться как связанные с программами-вымогателями. Процессам, подписанные Microsoft, можно всегда доверять.
- Вредные процессы, которые всегда рассматриваться как связанные с программами-вымогателями. Эти процессы не смогут запуститься, пока на машине включена активная защита.
- Папки, в которых не будут отслеживаться изменения файлов.

Укажите полный путь к файлу для выполняемого процесса, начиная с буквы диска. Например, **C:\Windows\Temp\er76s7sdkh.exe**.

Чтобы указать папки, можно использовать подстановочные символы * и ?. Звездочка (*) замещает 0 или более символов. Знак вопроса (?) заменяет только один символ. Нельзя использовать переменные среды, такие как %AppData%.

План активной защиты

Все настройки активной защиты содержаться в плане активной защиты. Этот план можно применить к нескольким машинам.

В организации может быть только один план активной защиты. Если в организации есть отделы, их администраторам запрещается применять, редактировать или отзывать план.

Применение плана активной защиты

1. Выберите машину, для которой необходимо активировать активную защиту.
2. Выберите **Active Protection**.
3. [Необязательно] Нажмите кнопку **Редактировать**, чтобы изменить следующие настройки:
   - В окне **Действие при обнаружении** выберите действие, которое программа выполнит при обнаружении деятельности программы-вымогателя, а затем нажмите кнопку **Готово**. Можно выбрать один из следующих вариантов:
     - **Только уведомить** (по умолчанию)

       Программа выдаст оповещение о процессе.
     - **Остановить процесс**

       Программа выдаст оповещение и остановит процесс.
     - **Отменить изменения, используя кэш**

       Программа выдаст оповещение, остановит процесс и отменит внесенные в файл изменения, используя кэш службы.
   - В окне **Вредоносные процессы** укажите процессы, которые всегда будут рассматриваться как связанные с программами-вымогателями, а затем нажмите кнопку **Готово**.
   - В окне **Доверенные процессы** укажите процессы, которые никогда не будут рассматриваться как связанные с программами-вымогателями, а затем нажмите кнопку **Готово**. Процессам, подписанные Microsoft, можно всегда доверять.
   - В окне **Исключения для папок** укажите папки в которых не будут отслеживаться изменения файлов, а затем нажмите кнопку **Готово**.
   - Деактивируйте выключатель **Самозащита**.

Самозащита предотвращает несанкционированные изменения собственных процессов программного обеспечения, записей в реестрах, исполняемых файлов и файлов конфигурации, а также основных загрузочных записей устройств. Не рекомендуется выключать эту функцию.

4. После изменения настроек нажмите кнопку **Сохранить настройки**. Изменения будут применены ко всем машинам, на которых включена активная защита.
5. Нажмите кнопку **Применить**.

16 Специальные операции с виртуальными машинами

16.1 Запуск виртуальной машины из резервной копии (мгновенное восстановление)

Примечание *Эта функция доступна только при наличии лицензии Advanced для Acronis Backup.*

Можно запустить виртуальную машину с резервной копии на уровне дисков, которая содержит операционную систему. Эта операция, которая также известна как мгновенное восстановление, позволяет ускорить виртуальный сервер за считанные секунды. Виртуальные диски эмулируются непосредственно с резервной копии и поэтому не занимают место в хранилище данных. Место хранения требуется только для того, чтобы сохранить изменения в виртуальных дисках.

Рекомендуем запустить эту временную виртуальную машину на срок до трех дней. После этого можно полностью удалить ее или преобразовать в обычную виртуальную машину (финализировать) без простоя.

Пока существует временная виртуальная машина, правила хранения нельзя применить к резервной копии, которая используется этой машиной. Резервные копии исходной машины могут продолжать выполняться.

Примеры использования

- **Аварийное восстановление**

  Мгновенное восстановление виртуальной машины, на которой произошел сбой.
- **Тестирование резервного копирования**

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

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

Предварительные требования

- В сервисе резервного копирования необходимо зарегистрировать хотя бы один агент для VMware или агент для Hyper-V.
- Резервная копия может храниться в сетевой папке, на узле хранения или в локальной папке машины, на которой установлен агент для VMware или агент для Hyper-V. Сетевая папка должна быть доступной с данной машины. Виртуальную машину можно также запустить из резервной копии, которая хранится в облачном хранилище данных, но в этом случае она

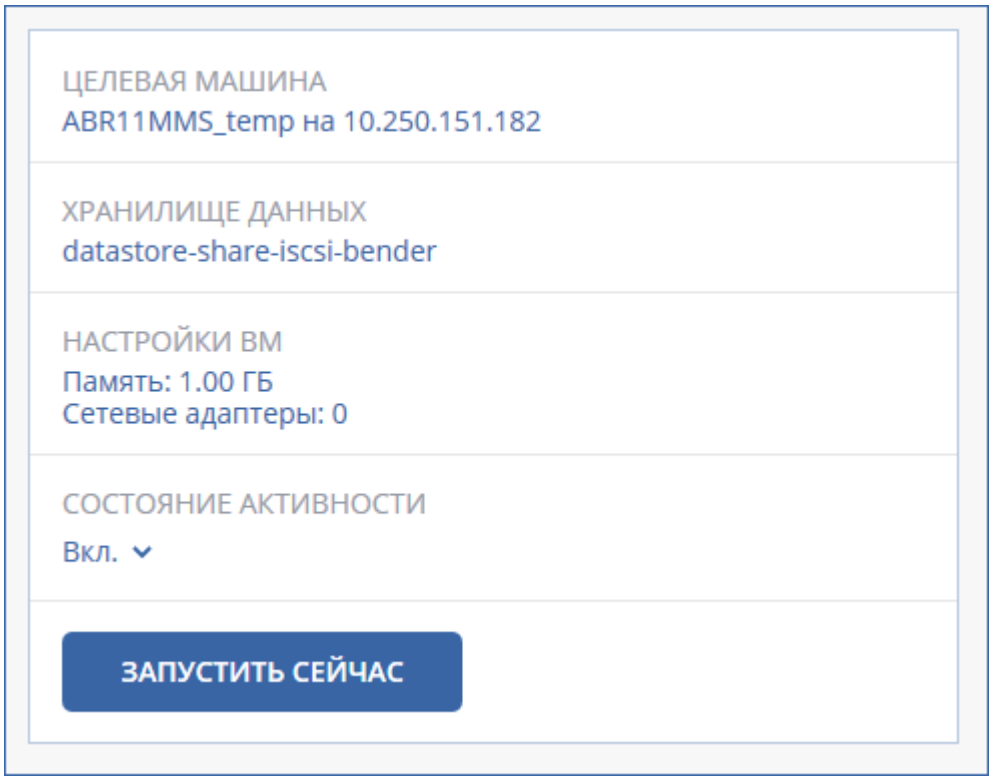
будет работать медленнее. Причина состоит в том, что для этой операции требуется интенсивное чтение из резервной копии с произвольным доступом к данным. Виртуальную машину невозможно запустить из резервной копии, хранящейся на сервере SFTP, на ленточном устройстве или в зоне безопасности.

- Резервная копия должна содержать всю машину или все тома, которые необходимы для запуска операционной системы.
- Могут использоваться резервные копии физических и виртуальных машин. Нельзя использовать резервные копии *контейнеров* Virtuozzo.

16.1.1 Запуск машины

1. Выполните одно из следующих действий:
   - Выберите машину, для которой создана резервная копия, щелкните **Восстановление** и выберите точку восстановления.
   - Выберите точку восстановления на вкладке «Резервные копии» (стр. 158).
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.
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.

16.1.2 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.

16.1.3 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 резервного копирования машина становится недоступной или даже повреждается.

Машину ESXi 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.

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.

16.2 Работа в VMware vSphere

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

16.2.1 Репликация виртуальных машин

Репликация доступна только для виртуальных машин VMware ESXi.

Репликация — это процесс создания точной копии (реплики) виртуальной машины с последующей поддержкой реплики в синхронизированном состоянии с исходной машиной. Репликация критически важных машин позволяет всегда иметь копию этой машины в готовом к запуску состоянии.

Репликацию можно запустить вручную или по расписанию, которое определяется пользователем. Первая репликация является полной (выполняется копирование всей машины). Все последующие репликации являются инкрементными и выполняются с помощью функции Changed Block Tracking (стр. 229), если этот параметр не отключен.

Репликация и резервное копирование

В отличие от запланированных процессов резервного копирования, в реплику сохраняется только актуальное на момент создания реплики состояние. Для реплики необходимо пространство хранилища данных, а резервные копии могут храниться на более дешевых хранилищах данных.

Однако включение реплики выполняется гораздо быстрее, чем восстановление и запуск виртуальной машины из резервной копии. Включенная реплика работает быстрее виртуальной машины, запущенной из резервной копии и не загружает агент для VMware.

Примеры использования

- **Репликация виртуальных машин на удаленную площадку.**

  Репликация позволяет сохранить работоспособность при частичном или полном отказе центра обработки данных. Это возможно за счет клонирования виртуальных машин с основной площадки на вторичную площадку. Эта вторичная площадка обычно располагается на удаленном оборудовании, которое не подвергается воздействию тех факторов окружающей среды, инфраструктурных или иных факторов, которые могли привести к отказу основной площадки.

- **Репликация виртуальных машин в рамках одной площадки (с одного хоста/хранилища данных на другой хост/другое хранилище данных).**

  Репликацию на месте можно использовать в сценариях High Availability и аварийного восстановления.

Действия, которые можно выполнить с репликой

- **Тестирование реплики** (стр. 228)

  Реплика будет включена для тестирования. Чтобы проверить правильность работы реплики, воспользуйтесь клиентом vSphere или другими инструментами. При выполнении тестирования репликация приостанавливается.

- **Переход к реплике** (стр. 228)

  Переход к реплике — это перенос рабочей нагрузки с исходной виртуальной машины на ее реплику. При выполнении перехода к реплике репликация приостанавливается.

- **Резервное копирование реплики**

  Как для резервного копирования, так и для репликации необходим доступ к виртуальным дискам. Это влияет на производительность работы хоста, на котором запущена виртуальная машина. Если необходимо иметь и реплику, и резервные копии виртуальной машины, то, чтобы не создавать дополнительную нагрузку для рабочего хоста, реплицируйте машину на другой хост и задайте резервные копии данной реплики.

Ограничения

Невозможно выполнить репликацию указанных ниже типов виртуальных машин:

- Отказоустойчивые машины, которые выполняются в ESXi 5.5 и более ранних версий.
- Машины, которые запущены из резервных копий.
- Реплики виртуальных машин.

16.2.1.1 Создание плана репликации

План репликации необходимо создать отдельно для каждой машины. Невозможно применить существующий план к другим машинам.

Порядок создания плана репликации

1. Выберите виртуальную машину для репликации.
2. Нажмите кнопку **Репликация**.

   В программе отображается новый шаблон плана репликации.
3. [Необязательно] Чтобы изменить имя плана репликации, щелкните имя по умолчанию.
4. Щелкните **Целевая машина** и выполните указанные ниже действия:
   a. Выберите, создавать ли новую или использовать уже существующую реплику исходной машины.
   b. Выберите хост ESXi и укажите имя новой реплики или выберите существующую реплику.

      Новая реплика будет иметь имя по умолчанию **[Имя исходной машины]_replica**.
   c. Нажмите кнопку **ОК**.
5. [Только при репликации на новую машину] Щелкните **Хранилище данных** и выберите хранилище данных для виртуальной машины.
6. [Необязательно] Щелкните **Расписание**, чтобы изменить расписание репликации.

   По умолчанию репликация выполняется ежедневно с понедельника по пятницу. Можно выбрать время для запуска репликации.

   Чтобы изменить частоту выполнения репликации, перетащите ползунок и задайте расписание.

   Можно также выполнить следующие действия:
   - Задать интервал дат, в течение которого будет использоваться указанное расписание. Установите флажок **Выполнять план в диапазоне дат** и укажите диапазон дат.
   - Отключить расписание. В этом случае репликацию можно запустить вручную.
7. [Необязательно] Щелкните значок шестерни, чтобы изменить параметры репликации (стр. 229).
8. Нажмите кнопку **Применить**.
9. [Необязательно] Чтобы запустить план вручную, щелкните **Запустить сейчас** на панели плана.

В результате выполнения плана репликации реплика виртуальной машины появляется в списке **Все устройства** с указанным ниже значком: 

16.2.1.2 Тестирование реплики

Порядок подготовки реплики к тестированию

1. Выберите реплику для тестирования.
2. Нажмите кнопку **Тестировать реплику**.
3. Нажмите кнопку **Начать тестирование**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика не будут подключена к сети.
5. [Необязательно] Если выбрано подключение реплики к сети, установите флажок **Остановить исходную виртуальную машину**, чтобы остановить исходную виртуальную машину до включения реплики.
6. Нажмите кнопку **Запустить**.

Порядок остановки тестирования реплики

1. Выберите реплику, для которой выполняется тестирование
2. Нажмите кнопку **Тестировать реплику**.
3. Нажмите кнопку **Остановить тестирование**.
4. Подтвердите операцию.

16.2.1.3 Переход к реплике

Переход с машины к реплике

1. Выберите реплику, к которой необходимо перейти.
2. Щелкните **Действия с репликой**.
3. Щелкните **Переход к реплике**.
4. Выберите, подключить ли включенную реплику к сети. По умолчанию реплика будет подключена к той же сети, что и исходная машина.
5. [Необязательно] Если выбрано подключение реплики к сети, снимите флажок **Остановить исходную виртуальную машину**, чтобы не выключать исходную виртуальную машину.
6. Нажмите кнопку **Запустить**.

При выполнении перехода к реплике можно выбрать одно из указанных ниже действий:

- **Остановить переход к реплике** (стр. 229)

  Остановите переход к реплике, если исходная машина исправлена. Реплика будет выключена. Репликация будет продолжена.

- **Выполнить окончательный переход на реплику** (стр. 229)

  Эта мгновенная операция позволяет удалить флаг «реплика» из виртуальной машины, чтобы сделать репликацию невозможной. Чтобы продолжить репликацию, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.

- **Возврат из реплики** (стр. 229)

  Выполните возврат из реплики, если выполнен переход на площадку, которая не предназначена для непрерывных операций. Реплика будет восстановлена на исходную или новую виртуальную машину. По окончании восстановления на исходную машину она включается и репликация продолжается. Если выбрано восстановление на новую машину, измените план репликации таким образом, чтобы эта машина была выбрана как исходная.

Остановка перехода к реплике

Порядок остановки перехода к реплике

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Остановить переход к реплике**.
4. Подтвердите операцию.

Выполнение окончательного перехода на реплику

Порядок выполнения окончательного перехода на реплику

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Окончательный переход на реплику**.
4. [Необязательно] Измените имя виртуальной машины.
5. [Необязательно] Установите флажок **Остановить исходную виртуальную машину**.
6. Нажмите кнопку **Запустить**.

Возврат из реплики

Порядок выполнения возврата из реплики

1. Выберите реплику, к которой выполняется переход.
2. Щелкните **Действия с репликой**.
3. Щелкните **Возврат из реплики**.

   Данное программное обеспечение автоматически выбирает исходную машину в качестве целевой.
4. [Необязательно] Щелкните **Целевая машина** и выполните следующие действия:
   a. Выберите новую или существующую машину для возврата из реплики.
   b. Выберите хост ESXi и укажите имя новой машины или выберите существующую машину.
   c. Нажмите кнопку **ОК**.
5. [Необязательно] При возврате из реплики на новую машину также можно выполнить следующие действия:
   - Щелкните **Хранилище данных**, чтобы выбрать хранилище данных для виртуальной машины.
   - Чтобы изменить размер памяти, количество процессоров и сетевые подключения виртуальной машины, щелкните **Настройки ВМ**.
6. [Необязательно] Щелкните **Параметры восстановления**, чтобы изменить параметры возврата из реплики (стр. 230).
7. Нажмите кнопку **Запуск восстановления**.
8. Подтвердите операцию.

16.2.1.4 Параметры репликации

Чтобы изменить параметры репликации, щелкните значок шестерни рядом с именем плана репликации и нажмите кнопку **Параметры репликации**.

Функция Changed Block Tracking (CBT)

Этот параметр подобен параметру резервного копирования «Changed Block Tracking (CBT)» (стр. 115).

Распределение ресурсов диска

Этот параметр определяет настройки распределения ресурсов диска для реплики.

Значение по умолчанию: **Экономное распределение**.

Доступны следующие значения: **Экономное распределение**, **Неэкономное распределение**, **Сохранить первоначальную настройку**.

Обработка ошибок

Этот параметр подобен параметру резервного копирования «Обработка ошибок» (стр. 118).

Команды до и после процедуры

Этот параметр подобен параметру резервного копирования «Команды до и после процедуры» (стр. 125).

Служба теневого копирования томов (VSS) для виртуальных машин

Этот параметр подобен параметру резервного копирования «Служба теневого копирования томов (VSS) для виртуальных машин» (стр. 134).

16.2.1.5 Параметры возврата из реплики

Чтобы изменить параметры возврата из реплики, щелкните **Параметры восстановления** при настройке возврата из реплики.

Обработка ошибок

Этот параметр подобен параметру восстановления «Обработка ошибок» (стр. 153).

Производительность

Этот параметр подобен параметру восстановления «Производительность» (стр. 155).

Команды до и после процедуры

Этот параметр подобен параметру восстановления «Команды до и после процедуры» (стр. 155).

Управление питанием ВМ

Этот параметр подобен параметру восстановления «Управление питанием ВМ» (стр. 157).

16.2.1.6 Сохранение первоначальной реплики

Чтобы ускорить репликацию в удаленное расположение и сэкономить пропускную способность сети, можно выполнить сохранение реплики.

Внимание! *Для сохранения реплики агент для VMware (виртуальное устройство) должен работать на целевом хосте ESXi.*

Сохранение первоначальной реплики

1. Выполните одно из следующих действий:
   - Если исходную виртуальную машину можно выключить, сделайте это, а затем перейдите к шагу 4.
   - Если исходную виртуальную машину нельзя выключить, перейдите к следующему шагу.
2. Создайте план репликации (стр. 227).

   При создании плана в разделе **Целевая машина** выберите пункт **Создать реплику** и хост ESXi, на котором размещена исходная машина.
3. Запустите план однократно.

   На исходном хосте ESXi будет создана реплика.
4. Экспортируйте файлы виртуальной машины (или реплики) на внешний жесткий диск.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к исходному хосту vCenter\ESXi.
   c. Выберите только что созданную реплику в списке.
   d. Выберите пункты **Файл** > **Экспорт** > **Экспорт шаблона OVF**.
   e. В поле **Папка** укажите папку на внешнем жестком диске.
   f. Нажмите кнопку **ОК**.
5. Перенесите жесткий диск в удаленное расположение.
6. Импортируйте реплику на целевой хост ESXi.
   a. Подключите внешний жесткий диск к машине, на которой работает клиент vSphere.
   b. Подключите клиент vSphere к целевому хосту vCenter\ESXi.
   c. Выберите пункт **Файл** > **Развернуть шаблон OVF**.
   d. В поле **Развернуть из файла или URL-адреса** укажите шаблон, экспортированный на шаге 4.
   e. Завершите процедуру импорта.
7. Измените план репликации, созданный на шаге 2. В поле **Целевая машина** выберите значение **Существующая реплика**, а затем выберите импортированную реплику.

В результате программа продолжит обновлять реплику. Все репликации будут инкрементными.

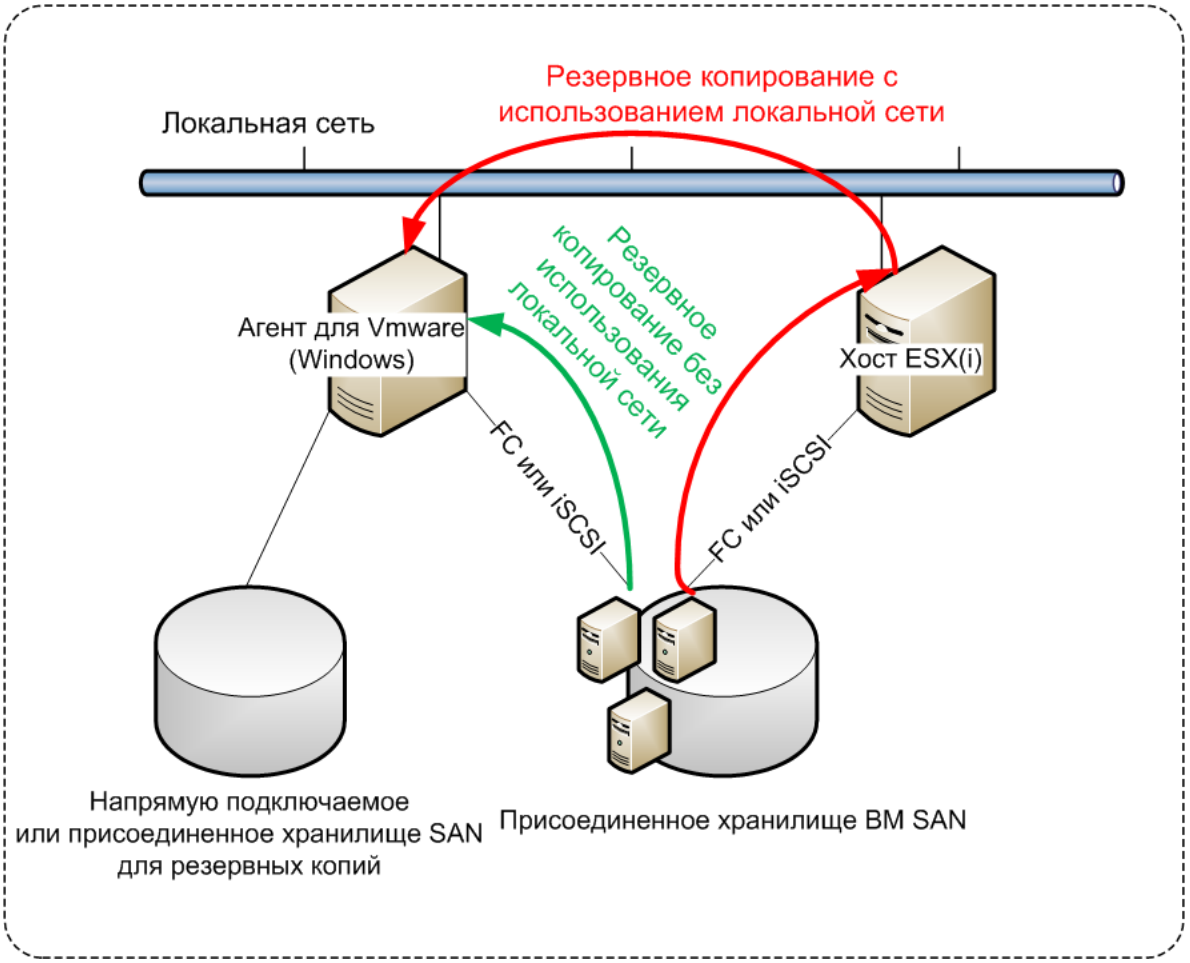
16.2.2 Резервное копирование без использования локальной сети

Если нагрузка на производственные хосты ESXi слишком велика и запуск виртуальных устройств нежелателен, можно установить агент для VMware (Windows) на физическую машину за пределами инфраструктуры ESXi.

Если с ESXi используется SAN-хранилище, установите агент на машину, подключенную к той же сети SAN. Агент будет создавать резервные копии виртуальных машин прямо из хранилища данных, а не через хост ESXi и локальную сеть. Эта возможность называется резервным копированием без использования локальной сети.

На следующем рисунке показано резервное копирование с использованием и без использования локальной сети. Доступ к виртуальным машинам без использования локальной сети возможен при наличии оптоволоконного канала (FC) или сети хранения данных (SAN) iSCSI. Чтобы полностью исключить передачу резервных копий данных по локальной сети, храните

резервные копии на локальном диске машины с установленным агентом или в присоединенном хранилище SAN.



Порядок включения прямого доступа к хранилищу данных для агента.

1. Установите агент для VMware на машину Windows, на которой есть сетевой доступ к vCenter Server.
2. Подключите к машине логическое устройство, на котором расположено хранилище данных. Примите во внимание следующие соображения:
   - Используйте тот же протокол (iSCSI или FC), который использовался для подключения хранилища данных к ESXi.
   - Логическое устройство *не должно* инициализироваться. Вместо этого оно должно появится как «автономный» диск в разделе **Управление дисками**. Если Windows инициализирует логическое устройство, оно может быть повреждено и стать нечитаемым для VMware vSphere.

     Чтобы избежать инициализации логического устройства, для параметра **Политика SAN Policy** автоматически устанавливается значение**Перевод в автономное состояние всех ресурсов** во время установки агента для VMware (Windows).

В результате агент будет использовать режим транспорта сети SAN для доступа к виртуальным дискам, т. е. он будет посекторно считывать секторы логического устройства по iSCSI/FC, не распознавая файловой системы VMFS (которая неизвестна для Windows).

Ограничения

- В vSphere 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. Type **`san policy=offlineall`**.
   b. Нажмите клавишу **Ввод**.
   c. Чтобы проверить правильность применения настройки, выполните шаг 2.
   d. Перезапустите машину.

Настройка инициатора iSCSI

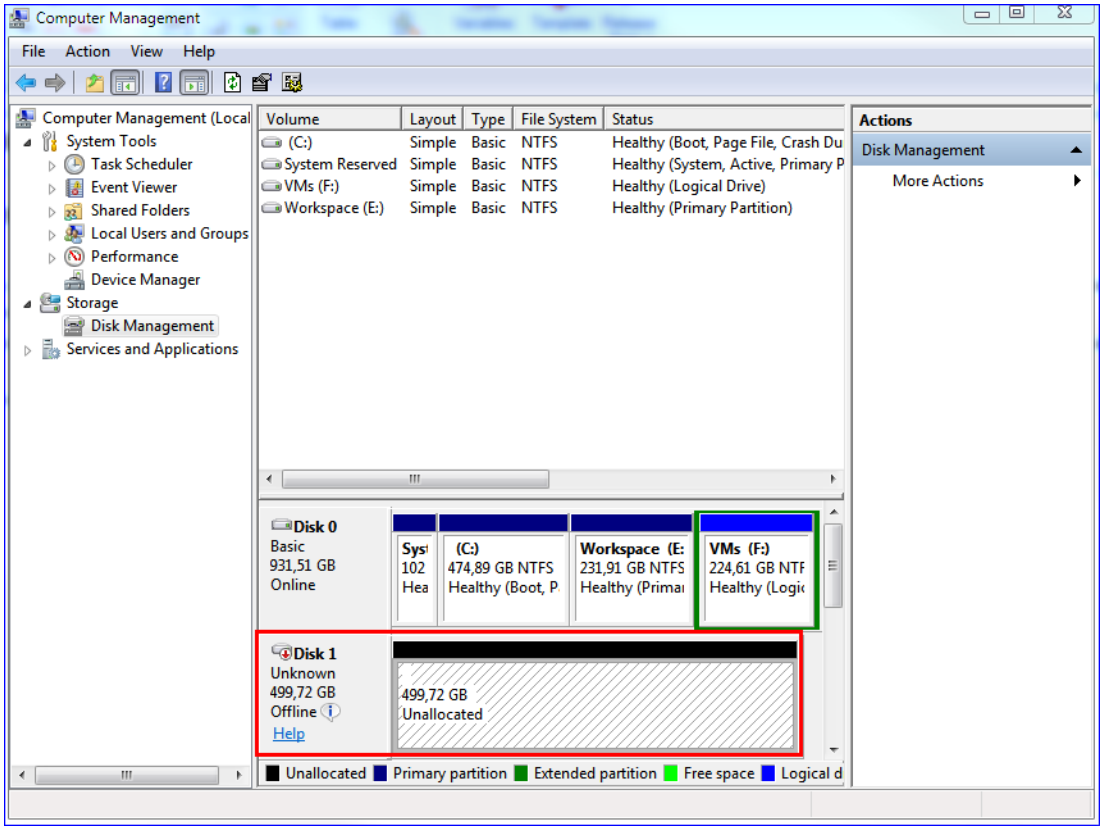
1. Последовательно выберите пункты **Панель управления** > **Администрирование** > **Инициатор iSCSI**.

   ***Подсказка**. 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 **ОК**.

Готовое логическое устройство SAN должно появится в разделе **Управление дисками**, как показано на снимке экрана ниже.



16.2.3 Использование моментальных снимков оборудования SAN

Если VMware vSphere использует систему хранения Storage area network (SAN) в качестве хранилища данных, вы можете подключить агент для VMware (Windows) для использования моментальных снимков оборудования SAN при выполнении резервного копирования.

Важно! *Поддерживается только хранилище NetApp SAN.*

Смысл использования моментальных снимков оборудования SAN

Агенту для VMware требуются моментальные снимки виртуальных машин для выполнения согласованного резервного копирования. Агент считывает содержимое виртуального диска с моментального снимка диска, поэтому моментальный снимок должен хранится в течение всего процесса резервного копирования.

По умолчанию агент использует встроенные моментальные снимки приложения VMware, созданные хостом ESXi. Во время хранения снимка файлы виртуального диска находятся в режиме «только чтение» и хост записывает все внесенные на диск изменения в отдельные разностные файлы. После завершения процесса резервного копирования хост удаляет моментальные снимки, то есть, объединяет разностные файлы с файлами виртуального диска.

Хранение и удаление моментальных снимков влияет на производительность виртуальной машины. На виртуальных дисках большого объема с быстрым изменением данных эти операции занимают много времени и приводят к падению производительности. В исключительных случаях при одновременном проведении резервного копирования

нескольких машин, возрастающий объем разностных файлов может привести к чрезмерному заполнению хранилища данных и привести к отключению всех виртуальных машин.

Вы можете снизить использование ресурсов гипервизором разгрузкой моментальных снимков в SAN. В данном случае последовательность операций будет следующей.

1. ESXi выполняет моментальный снимок VMware в начале процесса резервного копирования для согласования виртуальных дисков.
2. SAN создает моментальный снимок оборудования тома или LUN, содержащих виртуальную машину, и моментальный снимок VMware. Эта операция, как правило, займет несколько секунд.
3. ESXi удаляет моментальный снимок VMware. Агент для VMware считывает содержимое виртуального диска с моментального снимка оборудования SAN.

Моментальный снимок VMware сохраняется в течение нескольких секунд, поэтому снижение производительности виртуальной машины минимально.

Что необходимо для использования моментальных снимков оборудования SAN?

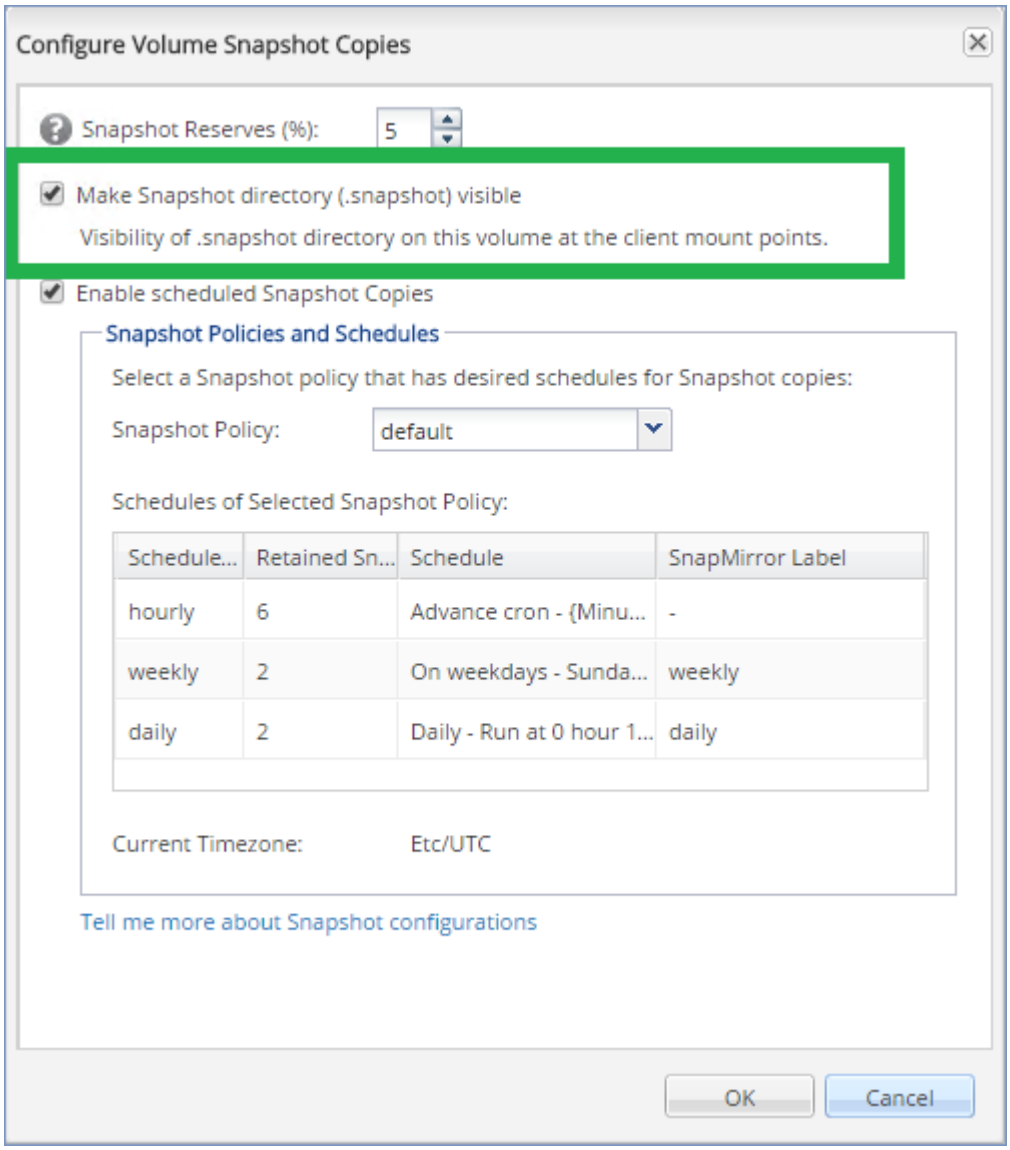
Для использования моментальных снимков оборудования SAN при резервном копировании виртуальных машин убедитесь в выполнении следующих условий.

- Хранилище SAN NetApp соответствует требованиям, описанным в «Требования хранилища SAN NetApp» (стр. 235).
- Машина, на которой запущен агент для VMware (Windows) сконфигурирована в соответствии с описанным в «Настройка машины, на которой работает агент для VMware» (стр. 237).
- Хранилище SAN зарегистрировано на сервере управления (стр. 238).
- [При наличии агентов для VMware, не принимавших участие в вышеуказанной регистрации] Виртуальные машины в хранилище SAN назначены агентам с подключенным SAN, как описано в «Привязка виртуальной машины» (стр. 239).
- Опция резервного копирования «Моментальные снимки оборудования SAN» (стр. 128) подключена в параметрах плана резервного копирования.

16.2.3.1 Требуется хранилище данных NetApp SAN

- Хранилище SAN должно использовать хранилище данных NFS или iSCSI.
- SAN должен работать с ПО Data ONTAP версии 8.1 или более новой в режиме **Clustered Data ONTAP (cDOT)**. Режим **7-mode**не поддерживается.

- В менеджере системы NetApp OnCommand System Manager должен быть установлен флажок **Моментальные копии** > **Конфигурирование** > **Сделать видимой папку моментальных копий (.snapshot)** для тома, в котором находится хранилище данных.

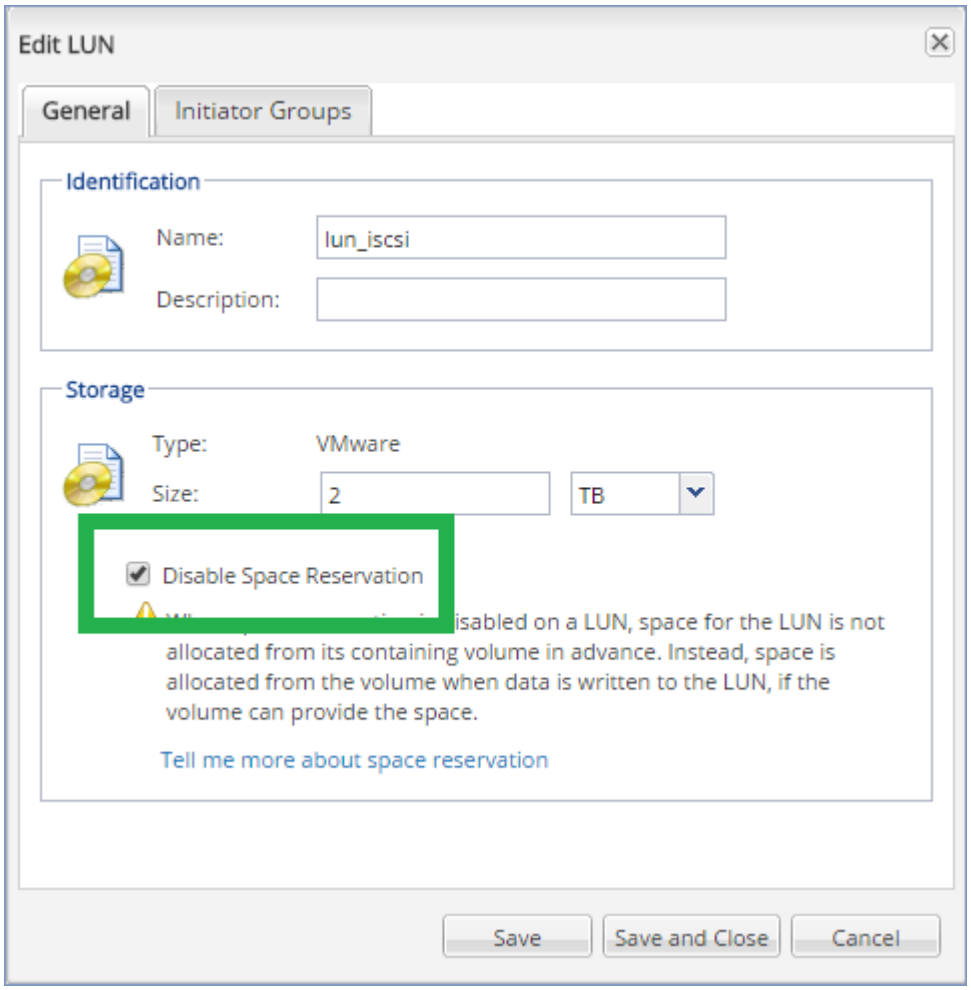


- [Для хранилищ данных NFS] На указанной при создании хранилища данных виртуальной должен быть разрешен доступ до общих папок NFS для клиентов Windows NFSv3. Доступ можно разрешить посредством следующей команды:

```
vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
```

Дополнительные сведения см. в документе с рекомендациями NetApp: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices

- [Для хранилищ данных iSCSI] В менеджере системы NetApp OnCommand должен быть установлен флажок **Отключить резервирование пространства** для iSCSI LUN, в котором находится хранилище данных.



16.2.3.2 Настройка машины, на которой работает агент для VMware

В зависимости от использования хранилища SAN в качестве хранилища данных NFS или iSCSI см. соответствующий раздел ниже.

Настройка инициатора iSCSI

Убедитесь, что выполнены все последующие условия:

- Инициатор iSCSI установлен.
- Тип запуска службы инициатора iSCSI (Microsoft) имеет значение **Автоматический** или **Ручной**. Это можно сделать в оснастке **Службы**.
- Инициатор iSCSI настроен как описано в примере раздела «Резервное копирование без использования локальной сети» (стр. 231).

Настройка NFS-клиента

Убедитесь, что выполнены все последующие условия:

- **Службы для NFS** Microsoft (в Windows Server 2008) или **Клиент для NFS** (в Windows Server 2012 и более поздних версиях) установлены.
- NFS-клиент настроен на анонимный доступ. Это можно сделать следующим образом:

a. Откройте редактор реестра.

b. Найдите следующий раздел реестра:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default

c. В этом ключе создайте новый параметр **DWORD** с именем **AnonymousUID** и задайте ему значение, равное 0.

d. В этом же ключе создайте новый параметр **DWORD** с именем **AnonymousGID** и задайте ему значение, равное 0.

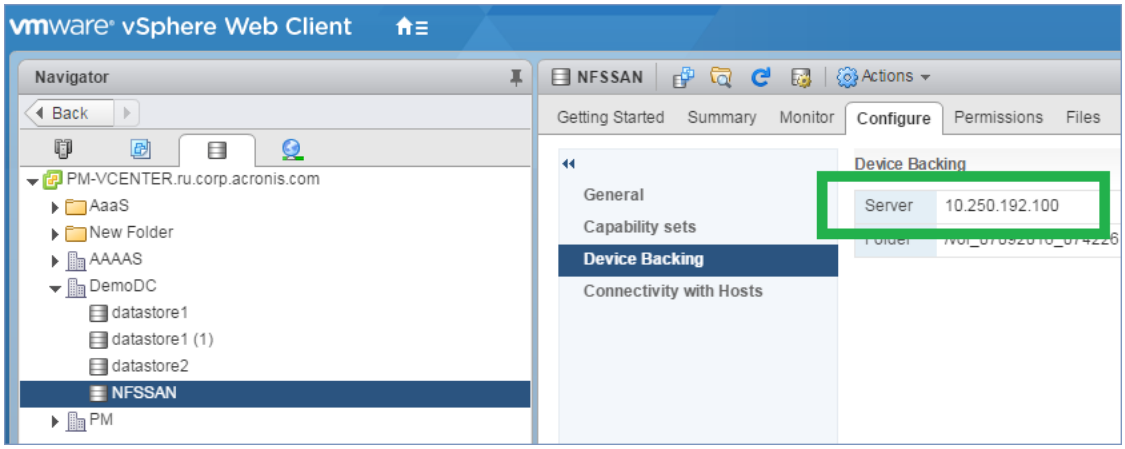
e. Перезапустите машину.

16.2.3.3 Регистрация хранилища данных SAN на сервере управления.

1. Нажмите**Настройки** > **Хранилище данных SAN**.
2. Нажмите**Добавить хранилище**.
3. [Необязательно] В **Имя** измените имя хранилища.

   Это имя будет отображено на вкладке **Хранилище данных SAN**.
4. В **Имя хоста или IP-адрес**укажите виртуальную машину хранилища NetApp Storage Virtual Machine (SVM, также называемое систематизатором), которая была указана при создании хранилища данных.

   Для нахождения требуемой информации в веб-клиенте VMware vSphere выберите хранилище данных и затем нажмите **Настроить** > **Резервная копия устройства**. Имя хоста или IP-адрес отобразится в поле **Сервер**.



5. В полях **Имя пользователя** и **Пароль** укажите учетные данные администратора SVM.

   Важно! *Указанная учетная запись должна иметь права локального администратора SVM, а не права администратора менеджера системы NetApp.*

   Выберите существующего пользователя или создайте нового. Для создания нового пользователя в менеджере системы NetApp OnCommand перейдите по пути **Настройки** > **Безопасность** > **Пользователи** и создайте нового пользователя.
6. Выберите один или несколько агентов для VMware (Windows), которым будет предоставлено право на чтение для устройства SAN.
7. Нажмите кнопку **Добавить**.

16.2.4 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 (стр. 239) 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 (стр. 45).

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 резервного копирования (стр. 72), в **Место сохранения резервной копии** выберите **Локальные папки** и введите букву диска, соответствующую локально присоединенному хранилищу, например**D:**.

16.2.5 Привязка виртуальной машины

В этом разделе показано, как сервер управления организует работу нескольких агентов в VMware vCenter.

Нижеуказанный алгоритм распределения работает как для виртуальных устройств, так и для агентов, установленных в Windows.

Алгоритм распределения

Виртуальные машины автоматически равномерно распределяются между агентами для VMware. Под равномерностью имеется в виду, что все агенты управляют равным количеством машин. Объем пространства, занимаемого в хранилище виртуальной машиной, не учитывается.

При выборе агента для машины программное обеспечение пытается оптимизировать общую производительность системы. В частности, программное обеспечение учитывает расположение агента и виртуальной машины. Предпочтительным является агент, размещенный на том же хосте. Если на том же хосте агента нет, по возможности выбирается агент из того же кластера.

Когда виртуальная машина назначается агенту, все централизованные резервные копии этой машины делегируются этому агенту.

Перераспределение

Перераспределение происходит каждый раз, когда нарушается этот баланс, или, точнее, когда дисбаланс нагрузки между агентами достигает 20 процентов. Это может произойти при добавлении или удалении машины или агента, при переносе машины на другой хост или в другой кластер или если машина привязывается к агенту вручную. В этом случае сервер управления перераспределяет машины с помощью того же алгоритма.

Например, вы понимаете, что для необходимой пропускной способности требуется больше агентов, и развертываете в кластере дополнительное виртуальное устройство. Сервер управления назначит новому агенту наиболее подходящие машины. Нагрузка на старые агенты уменьшится.

Если агент удаляется с сервера управления, то машины, назначенные этому агенту, распределяются между оставшимися агентами. Однако этого не произойдет, если агент поврежден или вручную удален из vSphere. Перераспределение начнется только после удаления такого агента из веб-интерфейса.

Просмотр результата распределения

Можно просмотреть результат автоматического распределения:

- в столбце **Агент** для каждой виртуальной машины в разделе **Все машины**;
- в разделе **Назначенные виртуальные машины** на панели **Сведения** при выборе агента в разделе **Настройки** > **Агенты**.

Привязка вручную

Привязка агента для VMware позволяет исключить виртуальную машину из этого процесса распределения, указав агент, который должен всегда выполнять резервное копирование этой машины. Общий баланс будет поддерживаться, но конкретная машина может быть передана другому агенту только в случае удаления исходного агента.

Порядок привязки машины к агенту

1. Выберите машину.
2. Нажмите **Сведения**.

   В разделе**Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Вручную**.
5. Выберите агент, к которому вы хотите привязать машину.
6. Нажмите кнопку **Сохранить**.

Как отвязать машину от агента

1. Выберите машину.

2. Нажмите **Сведения**.

   В разделе**Назначенные агенты** программное обеспечение отобразит агент, который в данный момент управляет выбранной машиной.
3. Нажмите **Изменить**.
4. Выберите **Автоматически**.
5. Нажмите кнопку **Сохранить**.

Отключение автоматического назначения для агента

Для отключения автоматического назначения для агента VMware, чтобы исключить его из процесса распределения, укажите список машин, для которых этот агент должен выполнять резервное копирование. Прочие агенты будут поддерживать общий баланс.

Невозможно отключить автоматическое назначение для агента при отсутствии прочих зарегистрированных агентов или при отключенном автоматическом назначении для прочих агентов.

Отключение автоматического назначения для агента

1. 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.
- Привязка вручную необходима при использовании моментальных снимков оборудования SAN (стр. 234). Привяжите агент для VMware (Windows), для которого сконфигурированы моментальные снимки оборудования SAN, к машинам, расположенным в хранилище данных SAN.
- Виртуальные машины необходимо привязать к агенту, если к агенту локально прикреплено хранилище. (стр. 238)
- 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.

16.2.6 Изменение учетных данных доступа vSphere

Можно изменить учетные данные доступа vCenter Server или автономного хоста ESXi без переустановки агента.

Изменение учетных данных доступа vCenter Server или хоста ESXi

1. В разделе **Устройства** выберите **VMware**.
2. Выберите **Хосты и кластеры**.
3. В списке **Хосты и кластеры** (справа от дерева **Хосты и кластеры**) выберите vCenter Server или автономный хост ESXi, который был указан при установке агента для VMware.
4. Нажмите **Сведения**.
5. В области **Учетные данные** выберите имя пользователя.
6. Укажите новые учетные данные доступа, а затем нажмите кнопку **ОК**.

16.2.7 Агент для VMware: необходимые привилегии

В этом разделе описаны права, необходимые для операций с виртуальными машинами ESXi, а также для развертывания виртуальных устройств. Агент для VMware (виртуальное устройство) доступен только в локальном развертывании.

Для выполнения операций на всех хостах и во всех кластерах, которые находятся под управлением vCenter Server, агент для VMware должен иметь привилегии в vCenter Server. Чтобы обеспечить работу агента только на определенном хосте ESXi, укажите агента с такими же привилегиями на данном хосте.

Укажите учетную запись с необходимыми привилегиями при установке или настройке агента для VMware. Чтобы изменить учетную запись позже, см. информацию в разделе «Изменение учетных данных доступа vSphere» (стр. 241).

		Операция				
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
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**	+	+	+	+	

		Операция				
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
	Методы отключения	+	+	+		
	Методы включения	+	+	+		
Хост > Конфигурация	**Конфигурация автозапуска ВМ**					+
	Конфигурация раздела хранения данных				+	
Хост > Инвентаризация	**Изменение кластера**					+
Хост > Локальные операции	**Создание ВМ**				+	+
	Удаление ВМ				+	+
	Перенастройка ВМ				+	+
Сеть	**Назначение сети**		+	+	+	+
Ресурс	**Назначение ВМ пулу ресурсов**		+	+	+	+
Импорт	**Добавить виртуальную машину**				+	
	vApp					+
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	+	+	+	+	

		Операция				
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
	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		+	+		
	Взаимодействие с консолью					+
	Управление гостевой операционной системой с помощью API VIX (в vSphere 5.1 и более поздних версий)				+	+
	Отключение			+	+	+
	Включение		+	+	+	+
Виртуальная машина > Инвентаризация	**Создание из существующей**		+	+	+	
	Создание новой		+	+	+	+
	Перемещение					+
	Регистрация				+	
	Удаление		+	+	+	+
	Отмена регистрации				+	

		Операция				
Объект	**Привилегия**	**Резервное копирование ВМ**	**Восстановление в новую ВМ**	**Восстановление в существующую ВМ**	**Запуск ВМ из резервной копии**	**Развертывание виртуального устройства**
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	+		+	+	+

* Эта привилегия требуется только для резервного копирования зашифрованных машин.

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

16.3 Миграция машины

Чтобы выполнить миграцию машины, можно восстановить ее резервную копию на другой машине.

Доступные варианты миграции приведены в таблице ниже.

Тип машины для резервного копирования	**Доступные места восстановления**		
	Физическая машина	Виртуальная машина ESXi	Виртуальная машина Hyper-V
Физическая машина	+	+	+
Виртуальная машина VMware ESXi	+	+	+
Виртуальная машина Hyper-V	+	+	+

Инструкции по выполнению миграции см. в следующих разделах:

- Миграция систем с физической машины на виртуальную (P2V): Миграция систем с физической машины на виртуальную (стр. 138)
- Миграция систем с виртуальной машины на виртуальную (V2V): Виртуальная машина (стр. 140)
- Миграция систем с виртуальной машины на физическую (V2P): Виртуальная машина (стр. 140) или Восстановление дисков с помощью загрузочного носителя (стр. 141)

Миграцию типа V2P можно выполнять в веб-интерфейсе, но в определенных случаях рекомендуется использовать загрузочный носитель. Иногда носитель может потребоваться для миграции в ESXi или Hyper-V.

Используя носитель, можно выполнять следующие действия:

- выбирать отдельные диски или тома для восстановления;
- вручную сопоставлять диски из резервной копии с дисками целевой машины;
- повторно создавать логические тома (LVM) или программные RAID-массивы Linux на целевой машине;
- предоставлять драйверы для определенного оборудования, необходимого для нормальной загрузки системы.

16.4 Виртуальные машины Windows Azure и Amazon EC2

Чтобы создать резервную копию виртуальной машины Windows Azure или Amazon EC2, установите на эту машину агент резервного копирования. Операции резервного копирования и восстановления выполняются точно так же, как и на физической машине. Тем не менее машина считается виртуальной, если заданы квоты на количество машин в облачном развертывании.

Отличие от физической машины состоит в том, что виртуальные машины Windows Azure и Amazon EC2 невозможно загрузить с загрузочного носителя. Если необходимо выполнить восстановление в новую виртуальную машину Windows Azure или Amazon EC2, следуйте указанной ниже процедуре.

Порядок восстановления машины как виртуальной машины Windows Azure или Amazon EC2

1. Создайте новую виртуальную машину из образа/шаблона в Windows Azure или Amazon EC2. Новая машина должна иметь такую же конфигурацию диска, как и машина, которую необходимо восстановить.
2. Установите агент для Windows или агент для Linux на новой машине.
3. Восстановите машину из резервной копии, как описано в разделе «Физическая машина» (стр. 136). При настройке восстановления выберите новую машину в качестве целевой.

Требования к сети

Агенты, установленные на машинах, для которых выполняется резервное копирование, должны иметь возможность обмениваться данными с сервером управления по сети.

Локальное развертывание

- Если и агенты, и сервер управления установлены в облаке Azure/EC2, все машины уже находятся в одной сети. Никаких дополнительных действий не требуется.
- Если сервер управления находится вне облака Azure/EC2, то машины в облаке не будут иметь доступа к локальной сети, в которой он установлен. Чтобы агенты, установленные на таких машинах, могли связываться с сервером управления, необходимо создать подключение виртуальной частной сети (VPN) между локальной и облачной (Azure/EC2) сетями. Инструкции по созданию подключений VPN см. в следующих статьях:

  Amazon EC2:
  http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure:
  https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

Облачное развертывание

В облачном развертывании сервер управления находится в одном из центров обработки данных Acronis, и поэтому доступен агентам. Никаких дополнительных действий не требуется.

17 Мониторинг и отчеты

Важно! *Эта функция была представлена в версии 12.5, и влияет только на локальные развертывания. Эта функция пока недоступна в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Раздел **Панель мониторинга** дает возможность отслеживать текущее состояние инфраструктуры резервного копирования. Раздел **Отчеты** дает возможность создавать запланированные отчеты и отчеты по требованию по инфраструктуре резервного копирования. Раздел **Отчеты** доступен только при наличии расширенной лицензии.

Разделы **Панель мониторинга** и **Отчеты** появляются на вкладке **Обзор** только при установленном на сервере управления компоненте **Служба мониторинга** (установлен по умолчанию).

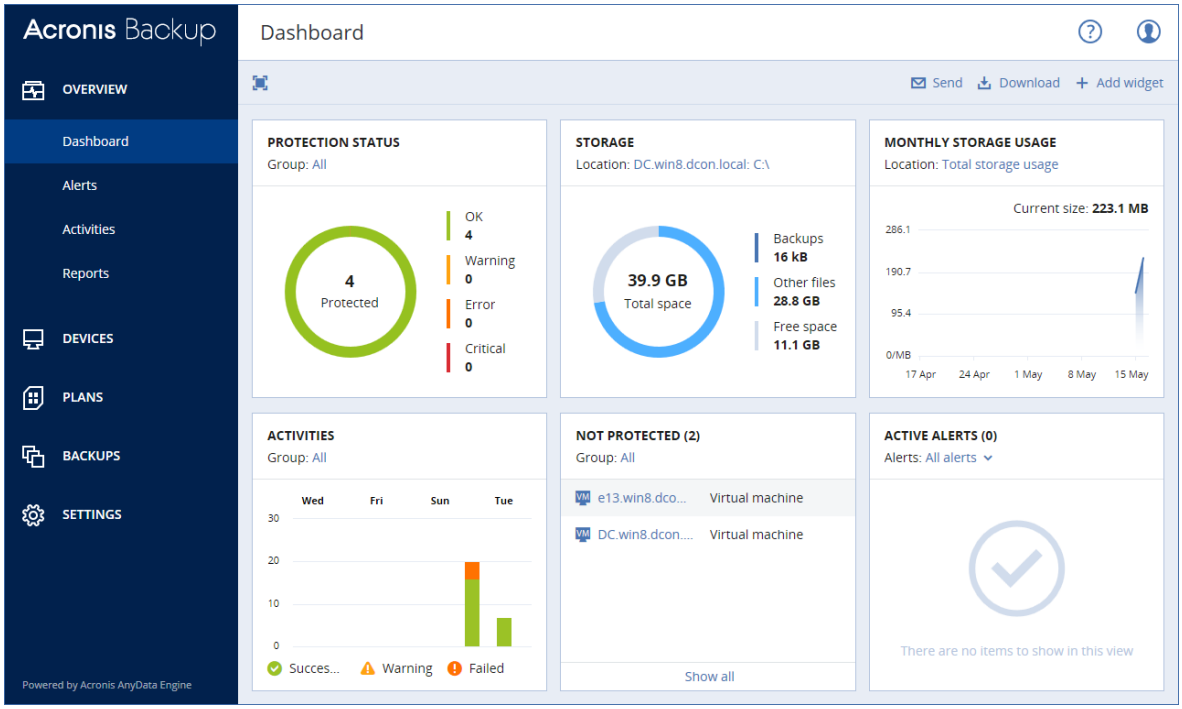
17.1 Панель мониторинга

Панель мониторинга предоставляет некоторое количество настраиваемых виджетов для обзора инфраструктуры резервного копирования. Виджеты обновляются в реальном времени. Вы можете выбирать из более чем 20 виджетов, представленных в виде круговых диаграмм, таблиц, графиков, линейчатых диаграмм и списков.

Следующие виджеты отображаются по умолчанию:

- **Статус защиты**. Показывает статусы защиты выбранной группы устройств.
- **Хранилище**. Показывает общее, свободное и занятое пространство для выбранного хранилища резервных копий.
- **Ежемесячное использование хранилища**. Показывает ежемесячное использование пространства для выбранного хранилища резервных копий.
- **Действия**. Показывает результаты действий за последние семь дней.
- **Не защищено**. Показывает устройства без плана резервного копирования.

- **Активные оповещения**. Показывает пять последних активных оповещений.



У виджетов есть активные элементы, на которые вы можете нажать для исследования возникших неполадок, их диагностики и устранений.

Вы можете загрузить текущее состояние панели мониторинга в виде файла формата .pdf или .xlsx, либо же переслать эти данные по электронной почте. Для отправки данных панели мониторинга по электронной почте убедитесь в том, что у вас сконфигурированы настройки **почтового сервера** (стр. 284).

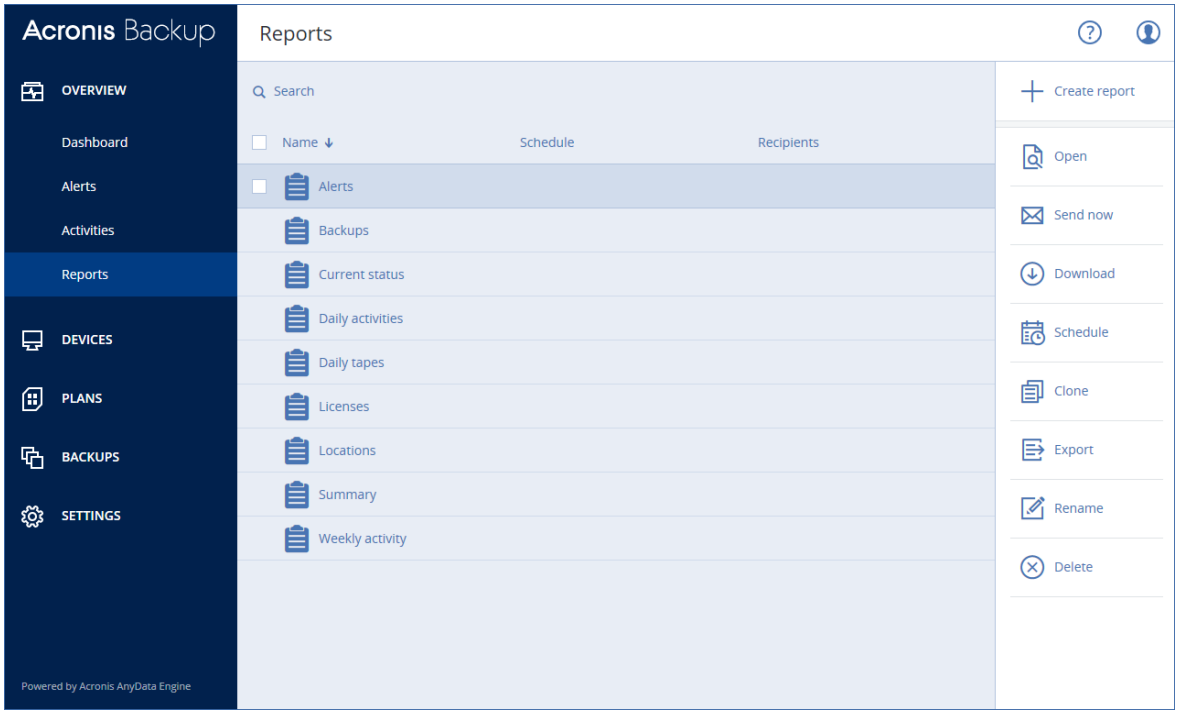
17.2 Отчеты

Примечание *Эта функция доступна только при наличии лицензии Advanced для Acronis Backup.*

Отчет может включать набор виджетов панели мониторинга. Вы можете использовать предварительно созданные отчеты или создать пользовательский отчет.

Отчеты могут быть отправлены по электронной почте или загружены по расписанию. Для отправки отчетов по электронной почте убедитесь в том, что у вас сконфигурированы настройки **Почтового сервера** (стр. 284).

При создании отчета с использованием стороннего программного обеспечения запланируйте сохранение отчетов в формате .xlsx в указанную папку.



Основные операции с отчетами

Нажмите**Обзор** > **Отчеты** выберите отчет и выполните одно из следующих действий.

- Для просмотра отчета нажмите **Открыть**.
- Для отправки отчета по электронной почте нажмите **Отправить сейчас**, укажите электронный адрес, выберите формат отчета и затем нажмите **Отправить**.
- Для загрузки отчета нажмите **Загрузить**.

Планирование отчета

1. Выберите отчет и затем нажмите **Запланировать**.
2. Включите переключатель **Отправить запланированный отчет**.
3. Выберите: отправлять отчеты по электронной почте, сохранять в папку, и то, и другое. В зависимости от выбора укажите адрес электронной почты, путь к папке или и то, и другое.
4. Выберите формат отчета: .pdf, .xlsx или и то, и другое.
5. Выберите отчетный период: 1 день, 7 дней или 30 дней.
6. Выберите дни и время отправки/сохранения отчета.
7. Нажмите кнопку **Сохранить**.

Экспорт и импорт структуры отчета

Вы можете экспортировать и импортировать структуру отчета (набор виджетов и настройки расписания) в файл .json. Это может оказаться полезным при переустановке сервера управления или для копирования структуры отчета на другой сервер управления.

Для экспорта структуры отчета выберите отчет и затем нажмите **Экспорт**.

Для импорта структуры отчета нажмите **Создать отчет** и затем нажмите **Импорт**.

Дамп данных отчета

Вы можете сохранить дамп данных отчета в файл .csv. Дамп содержит все данные отчета (без фильтрации) за определенный промежуток времени.

ПО динамически генерирует дамп данных. При указании большого промежутка времени данное действие может долго выполняться.

Дамп данных отчета

1. Выберите отчет и затем нажмите **Открыть**.
2. Нажмите значок в виде вертикального эллипса в правом верхнем углу и затем нажмите **Дамп данных**.
3. В **Хранилище** укажите путь к папке для файла .csv.
4. В **Диапазон времени** укажите диапазон времени.
5. Нажмите кнопку **Сохранить**.

17.3 Настройка важности оповещений

Оповещение — это сообщение, предупреждающее о текущей или потенциальной проблеме. Можно использовать оповещения разными способами:

- Раздел **Оповещения** на вкладке**Обзор**позволяет быстро определять и решать проблемы путем мониторинга текущих оповещений.
- В области **Устройства** статус устройства основывается на оповещениях. Колонка **Статус** позволяет фильтровать устройства с проблемами.
- При настройке уведомлений по электронной почте (стр. 283) можно выбрать, какие оповещения запустят уведомление.

Оповещение может иметь одну из следующих степеней серьезности:

- **Критическая**
- **Ошибка**
- **Предупреждение**

Можно изменить степень серьезности оповещения или полностью отключить их с помощью файла настройки оповещений, как описано ниже. Эта операция требует перезапуска сервера управления.

Изменение степени серьезности оповещения не повлияет на уже созданные оповещения.

Файл настройки оповещений

Файл настройки оповещений расположен на машине, где работает сервер управления.

- В ОС Windows: <путь_установки>**\AMS\alerts.config**

  Здесь <путь_установки> – путь установки сервера управления. По умолчанию, это **%ProgramFiles%\Acronis**.
- В ОС Linux: **/usr/lib/Acronis/AMS/alerts.config**

Файл имеет структуру XML-документа. Каждое оповещение включено в отдельный элемент **<alert>**.

Атрибут **severity** определяет степень серьезности оповещения. Он может иметь одно из следующих значений: **critical**, **error** или **warning**.

Атрибут **enable** определяет, включено оповещение или нет. Значение должно быть **true** или **false**.

Для изменения степени серьезности оповещения или его отключения

1. На машине, на которой установлен сервер управления, откройте в текстовом редакторе файл **alerts.config**.
2. Измените описанные выше атрибуты.
3. Сохраните файл.
4. Перезапустите службу сервера управления, как описано ниже.

Для перезапуска службы сервера управления в ОС Windows

1. В меню **Пуск** выберите команду **Выполнить** и введите: **cmd**
2. Нажмите кнопку **ОК**.
3. Выполните следующие команды:

```
net stop ams
net start ams
```

Для перезапуска службы сервера управления в ОС Linux

1. Откройте **приложение терминала**.
2. Выполните следующую команду в любом каталоге:

```
sudo service acronis_ams restart
```

18 Группы устройств

Важно! *Некоторые из функций, описанные в этом разделе были представлены в версии 12.5 и влияют только на локальные развертывания. Эти функции пока недоступны в облачных развертываниях. Дополнительную информацию см. в разделе «Что нового в Acronis Backup» (стр. 7).*

Группы устройств призваны обеспечить простое управление большим количеством устройств, зарегистрированных на сервере управления.

Вы можете применить план резервного копирования 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 **Машины** с агентами вы можете создать группу машин с агентами. Во **Все машины** невозможно создать группу.

Одно устройство может входить в несколько групп.

Встроенные группы

После регистрации устройства на сервере управления, устройство появляется в одной из встроенных корневых групп на вкладке **Устройства**.

Корневые группы *невозможно* редактировать или удалить. *Невозможно* применить план к корневым группам.

Некоторые корневые группы содержат встроенные подкорневые группы. Такие группы *невозможно* редактировать или удалить. Однако *возможно* применить планы к подкорневым встроенным группам.

Пользовательские группы

Защита всех устройств во встроенной группе с помощью одного плана резервного копирования 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 резервного копирования, 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 резервного копирования, 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. Имена хостов машин, принадлежащих к отделу бухгалтерии, содержат слово «**бухгалтерия**». Достаточно задать часть имени машины в качестве критерия членства в группе и применить к ней план резервного копирования. Машина нового бухгалтера будет добавлена в группу сразу после ее регистрации на сервере управления и таким образом будет автоматически защищена.

18.1 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 **ОК**.

   Новая группа появится на дереве групп.

18.2 Добавление устройств в статические группы

1. Нажмите кнопку **Устройства**, а затем выберите устройство, которое необходимо добавить 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**.

18.3 Создание динамической группы

1. Нажмите **Устройства**и выберите группу, которая содержит устройства, для которых необходимо создать динамическую группу.
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.
4. Укажите имя группы, а затем щелкните **OK**.

Условия поиска

Доступные условия поиска приведены в следующей таблице.

Критерий	Значение	Примеры поисковых запросов
`name`	▪ Имя хоста для физических машин ▪ Имя для виртуальных машин ▪ Имя базы данных ▪ Адрес электронной почты для почтовых ящиков	`name = 'ru-00'`
`ip`	IP-адрес (только для физических машин)	`ip RANGE ('10.250.176.1','10.250.176.50')`
`memorySize`	Размер ОЗУ в мегабайтах (Мб)	`memorySize < 1024`
`insideVm`	Данный флаг указывает на то, что машина с агентом фактически является виртуальной машиной. Возможные значения: ▪ `true` ▪ `false`	`insideVm = true`
`osName`	Название операционной системы.	`osName LIKE '%Windows XP%'`
`osType`	Тип операционной системы. Возможные значения: ▪ `'windows'` ▪ `'linux'` ▪ `'macosx'`	`osType IN ('linux', 'macosx')`

Критерий	Значение	Примеры поисковых запросов
osProductType	Тип продукта операционной системы. Возможные значения: ▪ **'dc'** Означает контроллер домена. ▪ **'server'** ▪ **'workstation'**	**osProductType = 'server'**
isOnline	Доступность машины. Возможные значения: ▪ **true** ▪ **false**	**isOnline = true**
tenant	Название отдела, которому принадлежит устройство.	**tenant = 'Unit 1'**
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'**
state	Состояние устройства. Возможные значения: ▪ **'idle'** ▪ **'interactionRequired'** ▪ **'canceling'** ▪ **'backup'** ▪ **'recover'** ▪ **'install'** ▪ **'reboot'** ▪ **'failback'** ▪ **'testReplica'** ▪ **'run_from_image'** ▪ **'finalize'** ▪ **'failover'** ▪ **'replication'** ▪ **'createAsz'** ▪ **'deleteAsz'** ▪ **'resizeAsz'**	**state = 'backup'**

Критерий	Значение	Примеры поисковых запросов
status	Статус устройства Возможные значения: ▪ **'notProtected'** ▪ **'ok'** ▪ **'warning'** ▪ **'error'** ▪ **'critical'**	**status = 'ok'**
protectedByPlan	Устройство защищено посредством плана резервного копирования с указанным идентификатором. Для получения идентификатора плана нажмите **Планы** > **Резервное копирование**, выберите план, нажмите на диаграмму в колонке **Статус** и затем нажмите на статус. Будет создан новый поиск с идентификатором плана.	**protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
okByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **OK**.	**okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
errorByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Ошибка**.	**errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
warningByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Внимание**.	**warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
runningByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Выполняется**.	**runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
interactionByPlan	Устройства, защищенные посредством плана резервного копирования с указанным идентификатором и со статусом **Требуется вмешательство**.	**interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**
id	Идентификатор устройства. Для получения идентификатора устройства напротив пункта **Устройства** выберите устройство и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле **id**.	**id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**

Критерий	Значение	Примеры поисковых запросов
lastBackupTime	Дата и время последнего успешного создания резервной копии. Формат данных следующий: 'ГГГГ-ММ-ДД ЧЧ:ММ'.	**lastBackupTime > '2016-03-11'** **lastBackupTime <= '2016-03-11 00:15'** **lastBackupTime is null**
lastBackupTryTime	Время последней попытки резервного копирования. Формат данных следующий: 'ГГГГ-ММ-ДД ЧЧ:ММ'.	**lastBackupTryTime >= '2016-03-11'**
nextBackupTime	Время следующего резервного копирования. Формат данных следующий: 'ГГГГ-ММ-ДД ЧЧ:ММ'.	**nextBackupTime >= '2016-03-11'**
agentVersion	Версия установленного агента резервного копирования.	**agentVersion LIKE '12.0.*'**
hostId	Внешний идентификатор агента резервного копирования. Для получения идентификатора агента резервного копирования напротив пункта **Устройства** выберите машину и выберите пункт **Сведения** > **Все свойства**. Идентификатор отобразится в поле **hostId**.	**hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'**

Операторы

Доступные операторы приведены в следующей таблице.

Оператор	Значение	Примеры
AND	Логический оператор конъюнкции.	**name like 'ru-00' AND status = ok**
OR	Логический оператор дизъюнкции.	**state=backup OR status = ok**
NOT	Логический оператор отрицания.	**NOT(osProductType = 'workstation')**
LIKE	Этот оператор используется для сравнения значения с подобными значениями с использованием операторов подстановочного знака. 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 'ru-00'** **name LIKE '*ru-00'** **name LIKE '*ru-00*'** **name LIKE 'ru-00_'**
ILIKE	Схож с оператором LIKE, но чувствителен к регистру.	**name ILIKE 'Ru-00'**

IN	Этот оператор используется для проверки того, соответствует ли выражение любому значению из указанного списка значений.	**osType IN ('windows', 'linux')**
RANGE((<начальное_значение>**,** <конечное_значение>**))**	Этот оператор используется для проверки того, находится ли значение в диапазоне значений (включительно).	**ip RANGE('10.250.176.1','10.250.176.50')**

18.4 Применение плана резервного копирования к группе

1. Щелкните **Устройства**, а затем выберите встроенную группу, к которой необходимо применить план резервного копирования.

   В программе будет выведен список дочерних групп.
2. Выберите группу, к которой необходимо применить план резервного копирования.
3. Нажмите кнопку **Резервное копирование**.
4. Продолжите создание плана резервного копирования, как описано в разделе «Резервное копирование» (стр. 72).

19 Расширенный выбор вариантов хранения

Примечание *Эта функция доступна только при наличии лицензии Advanced для Acronis Backup.*

19.1 Ленточные устройства

В следующих разделах подробно описано использование ленточных устройств для хранения резервных копий.

19.1.1 Что такое ленточное устройство?

Ленточное устройство — общий термин, который обозначает библиотеку ленточных носителей или изолированный ленточный носитель.

Библиотека ленточных носителей (автоматизированная библиотека) — устройство хранения большой емкости, содержащее следующие элементы:

- одно или несколько ленточных устройств;
- слоты для лент (до нескольких тысяч);
- одно или несколько устройств смены носителей (робототехнических механизмов) для перемещения лент между слотами и ленточными устройствами.

Библиотека может содержать и другие компоненты, например устройства чтения штрихкодов или принтеры штрихкодов.

Автоматический загрузчик — это особая разновидность библиотеки ленточных носителей. Он содержит один привод, несколько слотов, устройство смены носителей и устройство чтения штрихкодов (дополнительно).

Изолированное ленточное устройство (называемое также **стримером**) содержит один слот и в каждый момент времени может содержать только одну ленту.

19.1.2 Поддержка резервного копирования на ленту

Агенты резервного копирования могут выполнять резервное копирование данных на ленточное устройство напрямую или через узел хранения. В любом случае обеспечивается полностью автоматическая работа ленточного устройства. Если ленточное устройство с несколькими накопителями подключено к узлу хранения, несколько агентов могут одновременно выполнять резервное копирование на магнитные ленты.

19.1.2.1 Совместимость с RSM и программным обеспечением других поставщиков

Сосуществование с программным обеспечением других поставщиков

Невозможно работать с лентами на машине, на которой установлено программное обеспечение других поставщиков с фирменными средствами управления лентами. Для использования лент на таких машинах необходимо удалить или отключить программное обеспечение других поставщиков.

Взаимодействие с диспетчером съемных носителей Windows (RSM)

Агенты резервного копирования и узлы хранения не используют RSM. При обнаружении ленточного устройства (стр. 268) они отключают устройство от RSM (если они не используются другим программным обеспечением). Чтобы работать с ленточным устройством, убедитесь, что устройство не включается в RSM ни пользователями, ни программным обеспечением других поставщиков. Если ленточное устройство включено в RSM, повторите процедуру распознавания ленточного устройства.

19.1.2.2 Поддерживаемое оборудование

Acronis Backup поддерживает внешние устройства SCSI. Это устройства, подключаемые к Fibre Channel или с помощью интерфейсов SCSI, iSCSI, Serial Attached SCSI (SAS). Кроме того, Acronis Backup поддерживает ленточные устройства, подключенные через USB.

В Windows Acronis Backup может выполнять резервное копирование на ленточное устройство, даже если не установлены драйверы для соответствующего устройства смены носителей. Такое ленточное устройство отображается в **диспетчере устройств** как **неизвестный сменщик носителей**. Однако драйверы для накопителей устройства должны быть установлены. В Linux и при загрузке с носителя резервное копирование на ленточное устройство без драйверов невозможно.

Распознавание устройств, подключенных к IDE или SATA, не гарантируется. Это зависит от того, установлены ли в операционной системе необходимые драйверы.

Чтобы узнать, поддерживается ли конкретное устройство, используйте инструмент совместимости оборудования согласно описанию в следующей статье базы знаний Acronis: http://kb.acronis.com/content/57237. Можно отправить отчет с результатами теста в Acronis. Оборудование, которое гарантировано поддерживается, указано в списке совместимости оборудования: https://go.acronis.com/acronis-backup-advanced-tape-hcl.

19.1.2.3 База данных управления лентами

Информация обо всех ленточных устройствах, подключенных к машине, хранится в базе метаданных управления лентами. Путь к базе данных по умолчанию:

- В ОС Windows XP/Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database**.
- В ОС Windows Vista и более поздних версиях ОС Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database**.
- В ОС Linux: **/var/lib/Acronis/BackupAndRecovery/ARSM/Database**.

Размер базы данных зависит от количества резервных копий, которые хранятся на ленточных носителях, и приблизительно равен 10 МБ на каждые сто резервных копий. База данных может быть больше, если библиотека ленточных носителей содержит тысячи резервных копий. В таком случае, возможно, потребуется сохранить базу данных ленточных носителей на другом томе.

Как изменить расположение базы данных в Windows

1. Остановите службу управления съемными носителями.
2. Переместите файлы из расположения по умолчанию в новое расположение.
3. В реестре перейдите на ключ HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings.
4. Укажите новый путь к каталогу в значении реестра **ArsmDmlDbProtocol**. Строка может содержать до 32765 символов.
5. Запустите службу управления съемными носителями.

Как изменить расположение базы данных в Linux

1. Остановите службу **`acronis_rsm`**.
2. Переместите файлы из расположения по умолчанию в новое расположение.
3. Откройте файл конфигурации **/etc/Acronis/ARSM.config** в текстовом редакторе.
4. Найдите строку **`<value name="ArsmDmlDbProtocol" type="TString">`**.
5. Измените путь под этой строкой.
6. Сохраните файл.
7. Запустите службу **`acronis_rsm`**.

19.1.2.4 Параметры записи на ленты

Параметры записи на ленту (размер блока данных и размер кэша) позволяют выполнить тонкую настройку программного обеспечения для получения максимальной производительности. Для записи на ленту требуются оба параметра, но обычно необходимо настроить только размер блока данных. Оптимальное значение зависит от типа ленточного устройства и от данных, подлежащих резервному копированию, например, от количества файлов и их размера.

Примечание *Программа читает ленту блоками данных такого же размера, который был использован для записи данных на ленту. Если ленточное устройство не поддерживает этот размер блоков данных, чтение завершится сбоем.*

Параметры заданы на каждой машине, к которой подключено ленточное устройство. Это может быть машина, на которой установлен агент или узел хранения. На машине под управлением Windows настройка выполняется в реестре. На машине Linux она выполняется в файле конфигурации **/etc/Acronis/BackupAndRecovery.config**.

В Windows создайте соответствующие разделы реестра и их значения DWORD. На машине Linux добавьте следующий текст в конце файла конфигурации непосредственно перед тегом **`</registry>`**:

```
<key name="TapeLocation">
    <value name="WriteCacheSize" type="Dword">
        "значение"
    </value>
    <value name=DefaultBlockSize" type="Dword">
        "значение"
    </value>
</key>
```

DefaultBlockSize

Это размер блока данных (в байтах), используемый для записи на ленты.

Возможные значения: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Если данное значение равно 0 или параметр отсутствует, размер блока данных определяется следующим образом:

- В Windows данное значение принимается от драйвера ленточного устройства.
- В Linux данное значение составляет **64 КБ**.

Раздел реестра (на машине под управлением Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize

Строка в файле /etc/Acronis/BackupAndRecovery.config (на машине под управлением Linux):

```
    <value name=DefaultBlockSize" type="Dword">
        "значение"
    </value>
```

Если указанное значение не принимается ленточным устройством, то программа делит его на два до тех пока, пока не будет достигнуто приемлемое значение или значение 32 байта. Если приемлемое значение не найдено, то программа умножает указанное значение на два до тех пока, пока не будет достигнуто приемлемое значение или значение 1 МБ. Если ни одно значение не принимается диском, резервное копирование завершится сбоем.

WriteCacheSize

Это размер буфера (в байтах), используемый для записи на ленты.

Возможные значения: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, но не меньше значения параметра **DefaultBlockSize**.

Если значение составляет 0 или данный параметр отсутствует, размер буфера составляет **1 МБ**. Если операционная система не поддерживает это значение, то программа делит его на два до тех пока, пока не будет достигнуто приемлемое значение или значение параметра **DefaultBlockSize**. Если значение, поддерживаемое операционной системой, не найдено, резервное копирование завершится сбоем.

Раздел реестра (на машине под управлением Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Строка в файле /etc/Acronis/BackupAndRecovery.config (на машине под управлением Linux):

```
    <value name="WriteCacheSize" type="Dword">
        "значение"
    </value>
```


Если указать ненулевое значение, которое не поддерживается операционной системой, резервное копирование завершится сбоем.

19.1.2.5 Связанные с лентой параметры резервного копирования

Настраиваемые параметры резервного копирования **Управление лентами** (стр. 130) позволяют определить следующие возможности.

- Следует ли включить восстановление файлов из резервных копий дисков, хранящихся на лентах.
- Следует ли возвращать ленты в слот после завершения плана резервного копирования.
- Следует ли извлекать ленты после завершения резервного копирования.
- Следует ли использовать свободную ленту для каждой резервной копии.
- Следует ли перезаписывать данные на ленте при создании полной резервной копии (только для изолированных ленточных устройств).
- Следует ли использовать наборы лент для различения использованных лент, например, для резервных копий, созданных в разные дни недели или для резервных копий разных типов машин.

19.1.2.6 Параллельные операции

Acronis Backup может одновременно выполнять операции с различными компонентами ленточного устройства. В ходе операции с накопителем (резервное копирование, восстановление, повторный просмотр (стр. 273) или стирание (стр. 274)) можно запустить операцию, в которой используется устройство смены носителей (перемещение (стр. 270) ленты в другой слот или извлечение (стр. 275) ленты), и наоборот. Если в библиотеке ленточных носителей больше одного накопителя, можно запустить операцию с одним накопителем во время операции с другим. Например, несколько машин могут одновременно выполнять резервное копирование или восстановление, используя разные устройства одной и той же библиотеки ленточных носителей.

Операция обнаружения новых ленточных устройств (стр. 268) может выполняться одновременно с любой другой операцией. Во время инвентаризации (стр. 271) недоступны никакие другие операции, кроме обнаружения новых ленточных устройств.

Операции, которые нельзя выполнить параллельно, помещаются в очередь.

19.1.2.7 Ограничения

Существуют следующие ограничения использования ленточных устройств:

1. Ленточные устройства не поддерживаются, если машина загружается с 32-разрядного загрузочного носителя на базе Linux.
2. Невозможно создать резервную копию следующих типов данных на лентах: Почтовые ящики Microsoft Office 365, почтовые ящики Microsoft Exchange.
3. Невозможно выполнить резервное копирование физических и виртуальных машин с поддержкой приложений.
4. В macOS поддерживается только резервное копирование на уровне файлов в хранилище на основе ленточных устройств.
5. Консолидация резервных копий на лентах невозможна. В результате, схема резервного копирования **Всегда инкрементное** недоступна при резервном копировании на ленты.

6. Дедупликация резервных копий на лентах невозможна.
7. Программное обеспечение не может автоматически перезаписать ленту, содержащую хотя бы одну не удаленную резервную копию или при наличии зависимых резервных копий на других лентах.
8. Восстановление из резервной копии на ленте под управлением операционной системы невозможно, если это восстановление требует перезагрузки операционной системы. Для такого восстановления используйте загрузочный носитель.
9. Можно проверить (стр. 163) любые резервные копии на лентах, однако выбрать для проверки целое хранилище на ленте или ленточное устройство невозможно.
10. Управляемое хранилище на лентах невозможно защитить шифрованием. Вместо этого зашифруйте резервные копии.
11. Программа не может одновременно записать одну резервную копию на несколько лент или несколько резервных копий через одно устройство на одну ленту.
12. Устройства, использующие протокол NDMP (Network Data Management Protocol), не поддерживаются.
13. Принтеры штрихкодов не поддерживаются.
14. Ленты, форматированные в файловую систему Linear Tape File System (LTFS), не поддерживаются.

19.1.2.8 Читаемость лент, записанных посредством более старых продуктов Acronis

В следующей таблице приведена краткая информация о читаемости лент, записанных посредством продуктов семейств Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10 и Acronis Backup & Recovery 11 в Acronis Backup. Таблица также содержит сведения о совместимости магнитных лент, записанных с помощью различных компонентов Acronis Backup.

Повторно сканируемые резервные копии, которые были созданы в Acronis Backup 11.5 и Acronis Backup 11.7, можно дополнить инкрементными и дифференциальными резервными копиями.

			...читается на ленточном устройстве, подключенном к машине с...			
			Загрузочный носитель Acronis Backup	Агент Acronis Backup для Windows	Агент Acronis Backup для Linux	Узел хранения Acronis Backup
Магнитная лента, записанная на локально подключенном ленточном устройстве (ленточный накопитель или библиотека ленточных	Загрузочный носитель	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+
	Агент для Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+

носителей) с помощью...		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+
	Агент для Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+
Магнитная лента, записанная на ленточном устройстве посредством...	Сервер хранения резервных копий	9.1	–	–	–	–
		Echo	–	–	–	–
	Узел хранения	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+

19.1.3 Начало работы с ленточным устройством

19.1.3.1 Резервное копирование машины на локально подключенное ленточное устройство

Предварительные требования

- Ленточное устройство должно быть подключено к машине в соответствии с инструкциями производителя.
- На машине установлен агент резервного копирования.

Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите на консоль резервного копирования.
3. В разделе **Настройки** > **Управление лентами** разверните узел машины и щелкните **Ленточные устройства**.
4. Убедитесь, что отображается подключенное ленточное устройство. Если нет, нажмите кнопку **Обнаружить устройства**.
5. Проведите инвентаризацию лент:
   a. Щелкните имя ленточного устройства.
   b. Щелкните **Инвентаризация** для обнаружения загруженных лент. Оставьте включенным параметр **Полная инвентаризация**. Не включайте функцию **Перенести нераспознанные или импортированные ленты в пул «Свободные ленты»**. Щелкните **Начать инвентаризацию сейчас**.

      Результат: Загруженные ленты перенесены в соответствующие пулы, как указано в разделе «Инвентаризация» (стр. 271).

      Полная инвентаризация всего ленточного устройства может занять длительное время.

c. Если загруженные ленты перенесены в пул **Нераспознанные ленты** или **Импортированные ленты**, но требуются для резервного копирования, переместите (стр. 270) такие ленты в пул **Свободные ленты** вручную.

*Ленты, отправленные в пул **Импортированные ленты**, содержат резервные копии, записанные программой Acronis.. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.*

Резервное копирование

Создайте план резервного копирования, как описано в разделе «Резервное копирование» (стр. 72). Затем укажите хранилище резервных копий, щелкнув **Пул лент «Acronis»**.

Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Резервные копии** > **Пул лент Acronis**.
- Ленты с резервными копиями будут перемещены в пул **Acronis**.

19.1.3.2 Резервное копирование на ленточное устройство, подключенное к узлу хранения

Предварительные требования

- Узел хранения должен быть зарегистрирован на сервере управления.
- Ленточное устройство должно быть подключено к узлу хранения в соответствии с инструкциями производителя.

Перед резервным копированием

1. Загрузите ленты в ленточное устройство.
2. Войдите на консоль резервного копирования.
3. Щелкните **Настройки** > **Управление лентами**, разверните узел с именем узла хранения и щелкните **Ленточные устройства**.
4. Убедитесь, что отображается подключенное ленточное устройство. Если нет, нажмите кнопку **Обнаружить устройства**.
5. Проведите инвентаризацию лент:
   a. Щелкните имя ленточного устройства.
   b. Щелкните **Инвентаризация** для обнаружения загруженных лент. Оставьте включенным параметр **Полная инвентаризация**. Не включайте функцию **Переместить нераспознанные или импортированные пулы лент в пул «Свободные ленты»**. Щелкните **Начать инвентаризацию сейчас**.

      Результат: Загруженные ленты перенесены в соответствующие пулы, как указано в разделе «Инвентаризация» (стр. 271).

      Полная инвентаризация всего ленточного устройства может занять длительное время.

   c. Если загруженные ленты перенесены в пул **Нераспознанные ленты** или **Импортированные ленты**, но требуются для резервного копирования, переместите (стр. 270) такие ленты в пул **Свободные ленты** вручную.

      *Ленты, отправленные в пул **Импортированные ленты**, содержат резервные копии, записанные программой Acronis.. Перед перемещением таких лент в пул **Свободные ленты** убедитесь, что эти резервные копии больше не нужны.*

d. Определите, что требуется сделать: выполнить резервное копирование в пул (стр. 268) **Acronis** или создать новый пул (стр. 269).

   Подробнее. Наличие нескольких пулов позволяет использовать отдельный набор лент для каждой машины или каждого отдела компании. Разные пулы помогают не путать резервные копии, находящиеся на одной ленте, но созданные с помощью разных планов резервного копирования.

e. Если выбранный пул может, при необходимости, принимать ленты из пула **Свободные ленты**, пропустите этот шаг.

   В противном случае перенесите ленты из пула **Свободные ленты** в выбранный пул.

   Подсказка. Чтобы узнать, может ли пул принимать ленты из пула **Свободные ленты**, щелкните пул, а затем щелкните **Информация**.

Резервное копирование

Создайте план резервного копирования, как описано в разделе «Резервное копирование» (стр. 72). При указании хранилища резервных копий выберите созданный пул ленты.

Результаты

- Для доступа к хранилищу, где будут созданы резервные копии, выберите **Резервные копии**, затем выберите имя созданного пула ленты.
- Ленты с резервными копиями будут перемещены в выбранный пул.

Советы по дальнейшему использованию библиотеки ленточных носителей

- Полная инвентаризация не требуется каждый раз, когда загружается новая лента. Для экономии времени используйте процедуру, описанную в разделе «Инвентаризация» (стр. 271), подраздел «Сочетание быстрой и полной инвентаризации».
- В той же библиотеке ленточных носителей можно создать другие пулы и выбрать любой из них в качестве места назначения резервных копий.

19.1.3.3 Восстановление с ленточного устройства из операционной системы

Как выполнить восстановление с ленточного устройства из операционной системы

1. Войдите на консоль резервного копирования.
2. Нажмите **Устройства** и выберите машину, для которой есть резервная копия.
3. Щелкните **Восстановление**.
4. Выберите точку восстановления. Обратите внимание на то, что точки восстановления отфильтрованы по хранилищу.
5. Данное ПО отобразит /список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
6. Настройте (стр. 136) другие параметры восстановления.
7. Нажмите **Запуск восстановления**, чтобы запустить операцию восстановления.
8. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
   a. Загрузите ленту.
   b. Выполните быструю инвентаризацию (стр. 271).
   c. Нажмите **Обзор** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.

d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

Если не отображаются резервные копии, хранящиеся на лентах

Это может означать, что база данных с содержимым лент не найдена или повреждена.

Для восстановления базы данных выполните следующие действия.

1. Выполните быструю инвентаризацию (стр. 271).

   Во время инвентаризации не *включайте функцию* ***Перенести нераспознанные и импортированные ленты в пул «Свободные ленты»****. Если этот переключатель включен, можно потерять все резервные копии.*

2. Проведите Повторное сканирование (стр. 273) пула **Нераспознанные ленты**. В результате будет получено содержимое загруженных лент.
3. Если какие-либо из обнаруженных резервных копий продолжаются на других лентах, которые еще не сканировались, загрузите эти ленты по запросу и выполните их повторное сканирование.

19.1.3.4 Восстановление с загрузочного носителя из локально прикрепленного ленточного устройства

Как выполнить восстановление с загрузочного носителя из локально прикрепленного ленточного устройства

1. Загрузите в ленточное устройство ленты, необходимые для восстановления.
2. Загрузите машину с загрузочного носителя.
3. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
4. Если ленточное устройство подключено с использованием интерфейса iSCSI настройте устройство как описано в «Настройка устройств iSCSI и NDAS» (стр. 186).
5. Выберите **Управление лентами**.
6. Нажмите кнопку **Инвентаризация**.
7. В **Объекты для инвентаризации** выберите ленточное устройство.
8. Нажмите**Запуск** для запуска инвентаризации.
9. После завершения инвентаризации нажмите **Закрыть**.
10. Нажмите**Действия** > **Восстановить**.
11. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
12. Разверните **Ленточные устройства**, а затем выберите необходимое устройство.Система запросит подтверждение повторного сканирования. Нажмите**Да**.
13. Выберите пул **Нераспознанные ленты**.
14. Выберите ленты для повторного сканирования. Чтобы выбрать все ленты пула, установите флажок рядом с заголовком столбца **Имя ленты**.
15. Если ленты содержат защищенную паролем резервную копию, установите соответствующий флажок и укажите пароль для резервной копии в поле **Пароль**. Если пароль не указан или недействителен, резервная копия не будет обнаружена. Помните об этом в случае, если после повторного сканирования резервные копии не обнаружены.

    Подсказка. Если ленты содержат несколько резервных копий, защищенных разными паролями, необходимо повторить сканирование несколько раз, поочередно указывая пароли.

16. Нажмите**Запуск** для запуска повторного сканирования. В результате будет получено содержимое загруженных лент.
17. Если какие-либо из обнаруженных резервных копий продолжаются на других лентах, которые еще не сканировались, загрузите эти ленты по запросу и выполните их повторное сканирование.
18. После завершения повторного сканирования нажмите кнопку **ОК**.
19. В **представлении «Архив»** выберите резервную копию, затем выберите данные, которые требуется восстановить. После нажатия кнопки **ОК** на странице **Восстановление данных** отобразится список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
20. Настройте другие параметры восстановления.
21. Нажмите кнопку **ОК**, чтобы начать восстановление.
22. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    a. Загрузите ленту.
    b. Выполните быструю инвентаризацию (стр. 271).
    c. Нажмите **Обзор** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.
    d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

19.1.3.5 Восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения

Как выполнить восстановление с помощью загрузочного носителя с ленточного устройства, прикрепленного к узлу хранения

1. Загрузите в ленточное устройство ленты, необходимые для восстановления.
2. Загрузите машину с загрузочного носителя.
3. Выберите **Локальное управление этой машиной** или дважды щелкните **Загрузочный носитель** в зависимости от того, какой тип носителя используете.
4. Нажмите кнопку **Восстановить**.
5. Щелкните **Выбрать данные** и нажмите кнопку **Обзор**.
6. В поле **Путь** введите **bsp://**<адрес узла хранения>**/**<имя пула>**/**, где <адрес узла хранения> — это IP-адрес узла хранения, содержащего нужную резервную копию, а <имя пула> — имя пула лент. Нажмите кнопку **ОК** и укажите учетные данные для доступа к пулу.
7. Выберите резервную копию, а затем данные для восстановления. После нажатия кнопки **ОК** на странице **Восстановление данных** отобразится список лент, необходимых для восстановления. Отсутствующие ленты помечены как неактивные. Если в ленточном устройстве есть пустые слоты, загрузите эти ленты в устройство.
8. Настройте другие параметры восстановления.
9. Нажмите кнопку **ОК**, чтобы начать восстановление.
10. Если какие-либо из необходимых лент не загружены, программа отобразит сообщение с идентификатором нужной ленты. Необходимо сделать следующее:
    a. Загрузите ленту.
    b. Выполните быструю инвентаризацию (стр. 271).

c. Нажмите **Обзор** > **Действия**, после чего нажмите на действие восстановления со статусом **Требуется вмешательство**.

d. Нажмите **Показать сведения** и затем нажмите **Повторить** для продолжения восстановления.

19.1.4 Управление лентами

19.1.4.1 Обнаружение ленточных устройств

При обнаружении ленточных устройств программа резервного копирования находит ленточные устройства, подключенные к машине, и помещает информацию о них в базу данных управления лентами. Обнаруженные ленточные устройства отключены от RSM.

Как правило, ленточное устройство обнаруживается автоматически сразу же после подключения устройства к машине, на которой установлен продукт. Однако вам может потребоваться определение ленточных устройств в следующих случаях.

- После подключения или повторного подключения ленточного устройства.
- После установки или переустановки программы резервного копирования на машине, к которой подключено ленточное устройство.

Как обнаружить ленточные устройства

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину, к которой подключено ленточное устройство.
3. Выберите **Обнаружение ленточных устройств**. Будут отображены подключенные ленточные устройства, их накопители и слоты.

19.1.4.2 Пулы лент

В программе резервного копирования используются пулы лент, представляющие собой логические группы лент. Программное обеспечение содержит следующие стандартные пулы лент: **Нераспознанные ленты**, **Импортированные ленты**, **Свободные ленты** и **Acronis**. Кроме того, предусмотрена возможность создания собственных пользовательских пулов.

Пул **Acronis** и пользовательские пулы также используются в качестве хранилищ резервных копий./

Предварительно заданные пулы

Нераспознанные ленты

Пул содержит ленты, которые записывались сторонними приложениями. Для записи на такие ленты их необходимо явным образом переместить (стр. 270) в пул **Свободные ленты**. Переместить ленты из этого пула в какой-либо другой, кроме пула **Свободные ленты**, нельзя.

Импортированные ленты

Пул содержит ленты, которые записывались программой Acronis Backup на ленточном устройстве, подключенном к другому узлу хранения или агенту. Для записи на такие ленты их необходимо явным образом переместить в пул **Свободные ленты**. Переместить ленты из этого пула в какой-либо другой, кроме пула **Свободные ленты**, нельзя.

Свободные ленты

Пул содержит свободные (пустые) ленты. В этот пул можно вручную перемещать ленты из других пулов.

При переносе ленты в пул **Свободные ленты** программа помечает ее как пустую. Если лента содержит резервные копии, они помечаются  значкомКогда программа начнет перезаписывать ленту, данные, связанные с резервными копиями, будут удалены из базы данных.

Acronis

Пул используется по умолчанию для резервного копирования, когда не требуется создавать собственные пулы. Обычно он применяется к одному ленточному устройству с небольшим числом лент.

Пользовательские пулы

Для разделения резервных копий с различными данными необходимо создать несколько пулов. Например, можно создать пользовательские пулы для разделения:

- резервных копий разных отделов компании;
- резервных копий разных машин;
- резервных копий системных томов и пользовательских данных.

19.1.4.3 Операции с пулами

Создание пула

Как создать пул

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Нажмите **Создать пул**.
4. Введите имя пула.
5. [Необязательно] Снимите флажок напротив пункта **Автоматически брать ленты из пула «Свободные ленты»...**. Если флажок снят, только ленты, включенные в пул в определенный момент, будут использоваться для резервного копирования.
6. Нажмите кнопку **Создать**.

Изменение пула

Можно изменить параметры пула **Acronis** или пользовательского пула.

Как изменить пул

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Выберите требуемый пул и нажмите кнопку **Редактировать пул**.
4. Можно изменить имя или настройки пула. Дополнительные сведения о настройках пула см. в разделе Создание пула (стр. 269).
5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

Удаление пула

Можно удалять только пользовательские пулы. Нельзя удалить предварительно заданные пулы лент (**Нераспознанные ленты**, **Импортированные ленты**, **Свободные ленты** и **Acronis**).

Примечание *После удаления пула не забудьте отредактировать планы резервного копирования, в которых данный пул указан в качестве хранилища резервной копии. В ином случае при выполнении плана резервного копирования произойдет сбой.*

Как удалить пул

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Выберите требуемый пул и нажмите кнопку **Удалить**.
4. Выберите пул, в который будут перемещаться ленты из удаляемого пула после удаления.
5. Нажмите кнопку **ОК**, чтобы удалить пул.

19.1.4.4 Операции с лентами

Перемещение в другой слот

Используйте эту операцию в следующих ситуациях:

- необходимо извлечь несколько лент из ленточного устройства одновременно;
- ленточное устройство не имеет устройства оперативной смены носителя, и извлекаемые ленты находятся в слотах несъемных магазинов.

Необходимо переместить ленты в слоты одного магазина, а затем извлечь магазин вручную.

Как перенести ленту в другой слот

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите **Переместить в слот**.
5. Выберите новый слот, в который нужно перенести выбранную ленту.
6. Нажмите **Переместить**, чтобы начать операцию.

Перемещение в другой пул

Операция позволяет перенести одну или несколько лент из одного пула в другой.

При переносе ленты в пул **Свободные ленты** программа помечает ее как пустую. Если лента содержит резервные копии, они помечаются  значком Когда программа начнет перезаписывать ленту, данные, связанные с резервными копиями, будут удалены из базы данных.

Примечания о конкретных типах лент

- В пул **Свободные ленты** нельзя перенести защищенные от записи и однократно записанные ленты WORM (Write-Once-Read-Many — однократная запись, множественное чтение).

- Чистящие ленты всегда отображаются в пуле **Нераспознанные ленты**; перенести их в другой пул нельзя.

Перенос лент в другой пул:

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Переместить в пул**.
5. [Необязательно] Нажмите **Создать новый пул**, если требуется создать другой пул для выбранных лент. Выполните действия, описанные в разделе «Создание пула» (стр. 269).
6. Выберите пул, в который необходимо перенести ленты.
7. Нажмите **Переместить** для сохранения изменений.

Инвентаризация

Операция инвентаризации обнаруживает ленты, загружаемые в ленточное устройство, и присваивает имена лентам, у которых их нет.

Методы инвентаризации

Существует два метода инвентаризации.

Быстрая инвентаризация

Агент или узел хранения сканирует штрихкоды лент. С помощью штрихкодов программное обеспечение может быстро вернуть ленту в пул, где она находилась раньше.

Используйте этот метод для распознания лент, которые используются одним и тем же ленточным устройством, подключенным к одной и той же машине. Другие ленты будут направлены в пул **нераспознанных лент**.

Если в библиотеке ленточных носителей нет обработчика штрихкода, все ленты направляются в пул **нераспознанных лент**. Для распознания лент выполните полную инвентаризацию или используйте комбинацию быстрой и полной инвентаризации, как описано далее в этом разделе.

Полная инвентаризация

Агент или узел хранения считывает теги, записанные ранее, и анализирует прочую информацию о содержимом загружаемых лент. Выберите этот метод для распознания пустых лент и лент, записанных программным обеспечением, на любом ленточном устройстве и любой машине.

В следующей таблице показаны пулы, куда направляются ленты в результате полной инвентаризации.

Кто использовал ленту	**Кто считывает ленту**	**В какой пул направляется лента**
Агент	тот же агент	пул, где лента была раньше
	другой агент	**Импортированные ленты**
	Узел хранения	**Импортированные ленты**

Узел хранения	тот же узел хранения	пул, где лента была раньше
	другой узел хранения	**Импортированные ленты**
	Агент	**Импортированные ленты**
приложение стороннего производителя для резервного копирования	агент или узел хранения	**Нераспознанные ленты**

Ленты определенных типов направляются в определенные пулы.

Тип ленты	**В какой пул направляется лента**
Пустая лента	**Свободные ленты**
Пустая лента, защищенная от записи	**Нераспознанные ленты**
Очистка ленты	**Нераспознанные ленты**

Быструю инвентаризацию можно применять только к целым ленточным устройствам. Полную инвентаризацию можно применять к целым ленточным устройствам, отдельным приводам и слотам. Однако для автономных ленточных устройств всегда выполняется полная инвентаризация, даже если выбрана быстрая инвентаризация.

Комбинация быстрой и полной инвентаризации

Полная инвентаризация всего ленточного устройства может занять длительное время. Если требуется инвентаризация только нескольких лент, сделайте следующее.

1. Выполните быструю инвентаризацию ленточного устройства.
2. Щелкните пул **нераспознанных лент**. Найдите ленты, которые нужно инвентаризировать, и отметьте, в каких слотах они находятся.
3. Выполните полную инвентаризацию этих слотов.

Что делать после инвентаризации

Если вы хотите создавать резервные копии на лентах, которые были помещены в пул **нераспознанных лент** или пул **импортированных лент**, переместите (стр. 270) их в пул **свободных лент**, а затем в пул **Acronis** или пользовательский пул. Если пул, в котором вы хотите создавать резервные копии, пополняем, можно оставить ленты в пуле **свободных лент**.

Если требуется восстановление с ленты, которая была помещена в пул **нераспознанных лент** или **импортированных лент**, необходимо повторно сканировать (стр. 273) эту ленту. Лента будет перемещена в пул, который вы выбрали во время повторного сканирования, и резервные копии, которые хранятся на ленте, появятся в хранилище.

Последовательность действий

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину, к которой подключено ленточное устройство, а затем выберите ленточное устройство, для которого необходимо выполнить инвентаризацию.
3. Нажмите кнопку **Инвентаризация**.
4. [Необязательно] Для выбора быстрой инвентаризации отключите функцию **Полная инвентаризация**.
5. [Необязательно] Включите функцию **Перенести неопознанные и импортированные ленты в пул «Свободные ленты»**.

Предупреждение. *Подключайте эту функцию только в том случае, если вы абсолютно уверены, что данные, которые хранятся на лентах, больше не нужны и ленты можно перезаписать.*

6. Нажмите **Начать инвентаризацию сейчас** для запуска инвентаризации.

Повторное сканирование

Сведения о содержимом лент хранятся в особой базе данных. В ходе операции повторного сканирования выполняется чтение содержимого лент и, если содержимое не соответствует информации, имеющейся в базе данных, обновляется база данных. Резервные копии, обнаруженные в результате этой операции, помещаются в заданный пул.

За одну операцию можно просканировать ленты из одного пула. Для операции могут быть выбраны только ленты устройств, находящихся в оперативном режиме.

Повторное сканирование рекомендуется в следующих случаях:

- Если база данных узла хранения или управляемой машины потеряна или повреждена.
- Если сведения о ленте в базе данных устарели (например, содержимое ленты было изменено другим узлом хранения или агентом).
- Если требуется получить доступ к резервным копиям, сохраненным на лентах при работе с загрузочным носителем.
- Если по ошибке удалены (стр. 275) сведения о ленте из базы данных. При повторном сканировании удаленной ленты резервные копии, сохраненные на ней, вновь появляются в базе данных и становятся доступными для восстановления данных.
- Если резервные копии были удалены из ленты вручную или с помощью правил хранения, но нужно сделать их доступными для восстановления данных. Перед повторным сканированием такой ленты извлеките (стр. 275) ее, удалите (стр. 275) сведения о ней из базы данных, а затем снова вставьте ленту в устройство.

Как повторно сканировать ленты

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Ленточные устройства** около необходимой машины.
3. Выберите ленточное устройство, в которое загружены ленты.
4. Выполните быструю инвентаризацию (стр. 271).

Примечание. *Во время инвентаризации* не *включайте функцию* ***Перенести нераспознанные и импортированные ленты в пул «Свободные ленты»****.*

5. Выберите пул **Нераспознанные ленты**. После быстрой инвентаризации большинство лент направляются именно в этот пул. Также возможно повторное сканированиелюбого другого пула.
6. /[Необязательно] Выберите отдельные ленты для индивидуального сканирования./
7. Нажмите **Повторное сканирование**.
8. Выберите пул, в которое будут помещаться резервные копии после обнаружения..
9. При необходимости установите флажок **Включить восстановление файлов из образов дисков на лентах**.

   Подробнее. Если этот флажок установлен, программа создает специальные дополнительные файлы на жестком диске машины, к которой подсоединено ленточное устройство. Восстановление файлов из резервных копий дисков возможно до тех пор, пока эти дополнительные файлы будут в порядке. Обязательно установите флажок, если ленты

содержат резервные копии с поддержкой приложений (стр. 203). В противном случае вы не сможете восстановить данные приложений из этих резервных копий.

10. Если ленты содержат защищенные паролем резервные копии, установите соответствующий флажок и укажите пароль для этих резервных копий в поле пароля. Если пароль не указан или недействителен, резервные копии не будет обнаружены. Помните об этом в случае, если после повторного сканирования резервные копии не обнаружены.

    Подсказка. Если ленты содержат несколько резервных копий, защищенных разными паролями, необходимо повторить сканирование несколько раз, поочередно указывая пароли.
11. Нажмите **Запуск повторного сканирования** для запуска повторного сканирования.

Результат: Выбранные ленты перемещаются в выбранный пул. Резервные копии, сохраненные на лентах находятся в этом пуле. Резервная копия, расположенная на нескольких лентах, не появится в пуле, пока не будут повторно сканированы все эти ленты.

Переименование

Если программой обнаружена новая лента, ей автоматически назначается имя в следующем формате: **Лента XXX**, где **XXX** — уникальный номер. Ленты нумеруются последовательно. Операция переименования позволяет вручную изменить имя ленты.

Как переименовать ленту

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите **Переименовать**.
5. Введите новое имя выбранной ленты.
6. Нажмите **Переименовать** для сохранения изменений.

Стирание

При стирании физически удаляются все резервные копии, сохраненные на ленте, а из базы данных удаляется информация об этих резервных копиях. Однако информация о самой ленте сохраняется в базе данных.

Если стертая лента находилась в пуле **Нераспознанные ленты** или **Импортированные ленты**, она перемещается в пул **Свободные ленты**. Лента, размещенная в любом другом пуле, не перемещается.

Как стереть ленты.

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Стереть**. Система попросит подтвердить операцию.
5. Выберите способ стирания: быстрый или полный.
6. Нажмите кнопку **Стереть**, чтобы начать операцию.

   Подробнее. Операцию стирания отменить невозможно.

Извлечение

Для успешного извлечения ленты из библиотеки ленточных носителей библиотека ленточных носителей должна иметь устройство оперативной смены носителя (mail-slot), которое не должно быть блокировано пользователем или другой программой.

Как извлечь ленты.

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Извлечь**. Программа попросит ввести описание ленты. Рекомендуется описать физическое место, в котором будут храниться ленты. Во время восстановления программа покажет это описание, и вы легко найдете ленты.
5. Нажмите кнопку **Извлечь**, чтобы начать операцию.

После того как лента извлечена вручную или автоматически (стр. 130), рекомендуется написать на ленте ее имя.

Удаление

В ходе операции удаления из базы данных удаляются данные о резервных копиях, хранимых на выбранной ленте, и о самой ленте.

Можно удалить только автономную (извлеченную (стр. 275)) ленту.

Как удалить ленту

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимую ленту, а затем выберите требуемую ленту.
4. Нажмите кнопку **Удалить**. Система попросит подтвердить операцию.
5. Нажмите **Удалить**, чтобы удалить ленту.

Действия в случае удаления ленты по ошибке

В отличие от стертой (стр. 274) ленты, данные из удаленной ленты не удаляются физически. Поэтому можно вновь сделать доступными резервные копии, сохраненные на такой ленте. Выполните следующие действия.

1. Загрузите ленту в ленточное устройство.
2. Выполните быструю инвентаризацию (стр. 271), чтобы обнаружить ленту.

   Примечание. *Во время инвентаризации* не *включайте функцию* ***Перенести нераспознанные и импортированные ленты в пул «Свободные ленты»****.*
3. Выполните повторное сканирование (стр. 273), чтобы сопоставить данные, сохраненные на лентах, с базой данных.

Указание набора лент

Данная операция позволяет указать набор лент.

Набор лент представляет собой группу лент одного пула.

В отличие от указания набора лент в параметрах резервного копирования (стр. 130), где допустимо использование переменных, здесь допустимо указание только строковых значений.

Выполнение данной операции приведет к созданию программным обеспечением резервной копии *указанных* лент в соответствии с определенным правилом (например, для сохранений резервных копий за понедельник на ленте 1, резервных копий за вторник на ленте 2 и т. д.). Укажите определенный набор лент для каждой требуемой ленты и затем укажите тот же тип лент или используйте соответствующие переменные в параметрах резервного копирования.

В вышеупомянутом примере следует указать набор лент **Monday** для ленты 1, **Tuesday** для ленты 2 и т. д. В параметрах резервного копирования укажите **[Weekday]**. В данном случае надлежащая лента будет использована в соответствующий день недели.

Указание набора лент для одной или нескольких лент

1. Нажмите **Настройки** > **Управление лентами**.
2. Выберите машину или узел хранения, к которому прикреплено ленточное устройство и затем нажмите **Пулы лент** около необходимой машины.
3. Щелкните пул, который содержит необходимые ленты, а затем выберите требуемые ленты.
4. Нажмите **Набор лент**.
5. Введите имя набора лент. Если для указанных лент уже был задан набор лент, он будет заменен. Для исключения лент из набора лент без перемещения их в другой набор удалите существующее имя набора лент.
6. Нажмите кнопку **Сохранить**, чтобы сохранить изменения.

19.2 Узлы хранения

Узел хранения — это сервер, предназначенный для оптимизации использования различных ресурсов (таких как объем корпоративного хранилища, пропускная способность сети или загрузка процессоров производственных серверов), требуемых для защиты корпоративных данных. Это достигается путем организации хранилищ и управления хранилищами, выделенными для корпоративных резервных копий (управляемыми хранилищами).

19.2.1 Установка узла хранения и службы каталогизации

Перед установкой узла хранения убедитесь, что машина соответствует системным требованиям (стр. 28).

Мы рекомендуем устанавливать узел хранения и службу каталогов на отдельные машины. Системные требования к машине, на которой установлена служба каталогизации, описаны в разделе «Лучшие практики каталогизации» (стр. 283).

Порядок установки узла хранения и (или) службы каталогизации

1. Войдите как администратор и запустите программу установки Acronis Backup Advanced.
2. [Необязательно] Чтобы изменить язык программы установки, щелкните **Установка языка**.
3. Примите условия лицензионного соглашения и укажите, будет ли машина участвовать в программе улучшения качества Acronis Customer Experience Program (CEP).
4. Нажмите **Установить агент резервного копирования**.
5. Щелкните **Настройка параметров установки**.
6. Рядом с пунктом **Устанавливаемые компоненты** щелкните **Изменить**.
7. Выберите устанавливаемые компоненты:

- Для установки узла хранения установите флажок **Узел хранения**. Флажок **Агент для Windows** будет установлен автоматически.
- Для установки службы каталогов установите флажок **Служба каталогов**.
- Если на этой машине не нужно устанавливать другие компоненты, снимите соответствующие флажки.

Чтобы продолжить, нажмите кнопку **Готово**.

8. Укажите сервер управления, на котором будут зарегистрированы компоненты:
   a. Перейдите на **Сервер управления Acronis Backup**, нажмите**Указать**.
   b. Укажите имя хоста или IP-адрес машины, на которой установлен сервер управления.
   c. Укажите учетные данные администратора сервера управления. Можно использовать текущие учетные данные сеанса Windows или явно указать имя пользователя и пароль.

      Если вы вошли не как администратор сервера управления, машину можно зарегистрировать, оставив значение параметра **Подключиться к серверу управления как** по умолчанию.
   d. Нажмите кнопку **Готово**.
9. При поступлении запроса выберите, добавлять ли машину с узлом хранения и (или) службой каталогизации в организацию или в один из отделов.

   Этот запрос появляется, если вы являетесь администратором одного отдела или организации как минимум с одним отделом. В противном случае машина будет добавлена в отдел, который вы администрируете, или в организацию. Дополнительные сведения см. в разделе «Администраторы и отделы» (стр. 286).
10. [Необязательно] Измените другие настройки установки, как описано в разделе «Настройка параметров установки» (стр. 33).
11. Нажмите **Установить**, чтобы продолжить установку.
12. После завершения установки нажмите кнопку **Закрыть**.

19.2.2 Добавление управляемого хранилища

Управляемое хранилище может быть организовано:

- В локальной папке.
  - На жестком диске, локальном по отношению к узлу хранения.
  - На хранилище SAN, которое операционная система определяет как локально подключенное устройство.
- В сетевой папке.
  - В общей папке SMB/CIFS
  - На хранилище SAN, которое операционная система определяет как сетевую папку
  - На устройстве NAS
- В ленточном устройстве, локально подключенном к узлу хранения.

  Хранилища на основе ленточных устройств создаются в виде пулов лент (стр. 268). Один пул лент присутствует по умолчанию. При необходимости можно создать другие пулы лент, как описано далее в этом разделе.

Порядок создания управляемого хранилища в локальной или сетевой папке

1. Выполните одно из следующих действий:
   - Щелкните **Резервные копии** > **Добавить расположение**, затем щелкните **Узел хранения**.

- При создании плана резервного копирования щелкните **Место сохранения резервной копии** > **Добавить хранилище**, затем щелкните **Узел хранения**.
- Щелкните **Настройки** > **Узла хранения**, выберите узел хранения, который будет управлять расположением, затем щелкните **Добавить хранилище**.

2. В поле **Имя** укажите уникальное имя для хранилища. «Уникальный» означает, что не должно быть другого расположения с тем же именем, которое управляется тем же узлом хранения.
3. [Необязательно] Выберите узел хранения, который будет управлять этим хранилищем. Если вы выбрали последний параметр в шаге 1, вы не сможете изменять узел хранения.
4. Выберите имя узла хранения или IP-адрес, которые будут использоваться агентом для доступа к хранилищу.

   По умолчанию выбрано имя узла хранения. Возможно, нужно будет изменить эту настройку, если DNS не может привязать имя хоста к IP-адресу, что приводит к сбою доступа. Чтобы изменить эту настройку позже, щелкните **Резервные копии** > харнилаще > **Изменить**, затем измените значение поля **Адрес**.
5. Введите путь к папке или выберите ее в проводнике.
6. Нажмите кнопку **Готово**. Программа проверит доступ к указанной папке.
7. [Необязательно] Включите дедупликацию резервных копий в хранилище.

   Дедупликация минимизирует трафик резервного копирования и уменьшает размеры резервных копий в хранилище, удаляя дублированные блоки на диске.
8. [Только если включена дедупликация] Укажите или измените значение в поле **Путь к базе данных дедупликации**.

   Это должна быть папка на жестком диске, локальном по отношению к узлу хранения. Для повышения производительности системы рекомендуется создавать базу данных дедупликации и управляемое хранилище на разных дисках.

   Дополнительную информацию о базе данных дедупликации см. в разделе «Рекомендации по дедупликации» (стр. 279).
9. [Необязательно] Укажите, нужно ли защитить хранилище шифрованием. Все данные, которые записываются в это хранилище, будут зашифрованы, а при чтении нужная информация будет расшифрована узлом хранения с помощью специального ключа шифрования для хранилища, который находится на этом узле хранения, и это произойдет незаметно для пользователя.

   Дополнительную информацию о шифровании см. в разделе «Шифрование хранилища» (стр. 279).
10. Если на сервере управления зарегистрировано несколько служб каталогизации, можно выбрать службу каталогизации, которая выполнит каталогизацию резервных копий, которые находятся в хранилище.
11. Нажмите кнопку **Готово**, чтобы создать хранилище.

Для создания управляемого хранилища на ленточном устройстве

1. Щелкните **Резервные копии** > **Добавить хранилище**, или при создании плана резервного щелкните **Место сохранения резервной копии** > **Добавить хранилище**.
2. Выберите **Ленты**.
3. [Необязательно] Выберите узел хранения, который будет управлять этим хранилищем.
4. Выполните действия, описанные в разделе «Создание пула» (стр. 269), начиная с шага 4.

Примечание *По умолчанию агенты используют имя узла хранения для доступа к управляемому хранилищу на основе ленточных устройств. Чтобы агенты использовали IP-адрес узла хранения, щелкните* ***Резервные копии*** *> хранилище >* ***Изменить****, затем измените значение поля* ***Адрес****.*

19.2.3 Шифрование хранилища

Если хранилище защищено шифрованием, то все данные, которые в него заносятся, будут зашифрованы, а при чтении нужная информация будет расшифрована узлом хранения с помощью специального ключа шифрования для хранилища, и это произойдет незаметно для пользователя. Ключ находится на узле хранения. Если носитель хранилища украден или доступ к нему получил неавторизованный пользователь, злоумышленник не сможет расшифровать содержимое хранилища без доступа к узлу хранения.

Это шифрование не имеет ничего общего с шифрованием резервной копии, которое задано в плане резервного копирования и выполняется агентом. Если резервная копия уже зашифрована, шифрование на стороне узла хранения применяется поверх шифрования, выполненного агентом.

Как защитить хранилище шифрованием

1. Укажите и подтвердите слово (пароль), на основе которого будет сформирован ключ шифрования.

   В слове учитывается регистр. Это слово потребуется только при подключении хранилища к другому узлу хранения.
2. Выберите один из следующих алгоритмов шифрования:
   - **AES 128** — содержимое хранилища будет зашифровано с использованием алгоритма AES и 128-разрядного ключа.
   - **AES 192** — содержимое хранилища будет зашифровано с использованием алгоритма AES и 192-разрядного ключа.
   - **AES 256** — содержимое хранилища будет зашифровано с использованием алгоритма AES и 256-разрядного ключа.
3. Нажмите кнопку **ОК**.

Алгоритм шифрования AES выполняется в режиме CBC (цепочка шифроблоков) и использует сформированный случайным образом ключ указанного пользователем размера (128, 192 или 256 бит). Чем больше размер ключа, тем дольше программа будет шифровать резервные копии, находящиеся в хранилище, и тем лучше будут защищены резервные копии.

Затем ключ шифрования шифруется с помощью алгоритма AES-256, используя хэш SHA-256 выбранного слова в качестве ключа. Само слово на диске не хранится. Для проверки используется хэш слова. Такая двухуровневая схема защиты позволяет обезопасить резервные копии от несанкционированного доступа, но восстановить утраченное слово невозможно.

19.2.4 Рекомендации по дедупликации

Дедупликация — это сложный процесс, зависящий от многих факторов.

Наиболее важные факторы, влияющие на скорость дедупликации:

- скорость доступа к базе данных дедупликации;
- объем оперативной памяти узла хранения;
- количество дедуплицирующих хранилищ, созданное в узле хранения.

Для увеличения производительности дедупликации следуйте рекомендациям ниже.

Размещайте базу данных дедупликации и дедуплицирующее хранилище на разных физических носителях.

В базе данных дедупликации содержатся хэш-значения всех элементов, которые хранятся в хранилище, кроме тех, которые не могут дедуплицироваться (например, зашифрованные файлы).

Для увеличения скорости доступа к базе данных дедупликации база данных и хранилище должны быть размещены на разных физических носителях.

Рекомендуется выделить специальные устройства для хранилища и базы данных. Если это невозможно, по крайней мере не размещайте хранилище или базу данных на диске с операционной системой. При работе операционной системы выполняется большое количество операций чтения/записи на жесткий диск, что существенно замедляет процесс дедупликации.

Выбор диска для базы данных дедупликации

- База данных должна находиться на стационарном диске. Не пытайтесь разместить базу данных дедупликации на внешних съемных носителях.
- Чтобы минимизировать время доступа к базе данных, сохраните ее на диске, подключенном напрямую, а не на подключенном сетевом томе. Задержка в сети может существенно снизить производительность дедупликации.
- Примерный объем дискового пространства, необходимого для базы данных дедупликации, вычисляется по следующей формуле:

  $$S = U * 90 / 65536 + 10$$

  В этой формуле

  S — размер диска в ГБ;

  U — планируемый объем уникальных данных в хранилище дедуплицированных данных (ГБ).

  Например, если планируемый объем уникальных данных в хранилище дедуплицированных данных U = 5 ТБ, для базы данных дедупликации потребуется объем свободного пространства не менее

  $$S = 5 * 90 / 65536 +10 = 17 ГБ$$

Выбор диска для дедуплицирующего хранилища

Для предотвращения потери данных рекомендуется использовать RAID 10, 5 или 6. RAID 0 не рекомендуется, поскольку не является отказоустойчивым. RAID 1 не рекомендуется из-за относительно низкой скорости. Можно использовать как локальные диски, так и SAN.

От 40 до 160 МБ ОЗУ на 1 ТБ уникальных данных

По достижении ограничения дедупликация выполняться не будет, а резервное копирование и восстановление продолжат выполняться. Если вы добавите ОЗУ в узел хранения после следующего резервного копирования, дедупликация восстановится. В общем, чем больше ОЗУ, тем больше размер томов с уникальными данными, которые можно сохранить.

Одно дедуплицирующее хранилище на каждый узел хранения

Настоятельно рекомендуется создавать только одно дедуплицирующее хранилище на узле хранения. В противном случае весь доступный объем ОЗУ будет распределен пропорционально количеству хранилищ.

Отсутствие приложений, конкурирующих за ресурсы

На машине с узлом хранения не должны быть запущены приложения, требующие большого количества системных ресурсов, например, системы управления базами данных (СУБД) или системы планирования ресурсов предприятия (ERP).

Многоядерный процессор с тактовой частотой не менее 2,5 ГГц

Рекомендуется использовать процессор с количеством ядер не менее 4 и тактовой частотой не менее 2,5 ГГц.

Достаточное свободное пространство в хранилище

Для дедупликаии в месте назначения требуется столько же свободного пространства, сколько занимают данные резервной копии сразу после сохранения в хранилище. Без выполнения сжатия или дедупликации в источнике это значение равно размеру исходных данных, резервная копия которых создана во время данной операции резервного копирования.

Высокоскоростная локальная сеть

Рекомендуется скорость локальной сети 1 Гбит. Это позволит программе выполнить 5–6 операций резервного копирования параллельно с дедупликацией без заметного снижения скорости.

Выполните резервное копирование типичной машины перед резервным копированием нескольких машин со сходным содержимым.

При резервном копировании нескольких машин со сходным содержимым рекомендуется сначала выполнить резервное копирование одной машины и подождать завершения индексирования данных резервной копии. После этого резервное копирование остальных машин будет выполняться быстрее за счет эффективной дедупликации. Поскольку резервная копия первой машины была проиндексирована, большая часть данных уже находится в хранилище дедуплицированных данных.

Выполняйте резервное копирование разных машин в разное время.

При резервном копировании большого количества машин распределите операции резервного копирования по времени. Для этого необходимо создать несколько планов резервного копирования с различными расписаниями.

19.2.5 Каталог данных

Каталог данных позволяет легко найти требуемую версию данных и выбрать ее для восстановления. В каталоге данных отображены все данные, хранящиеся во всех управляемых хранилищах.

Раздел **Каталог** появляется на вкладке **Резервные копии** только в том случае, если по меньшей мере одна служба каталога зарегистрирована на сервере управления. Информацию по установке сервиса каталога см. по ссылке «Installing a storage node and a cataloging service (Установка узла хранения и службы каталогизации)» (стр. 276).

Раздел **Каталог** видим только для администраторов организации (стр. 286).

Ограничения

Каталогизация поддерживается только для резервных копий физических машин на уровне файлов и резервных копий виртуальных машин.

В каталоге не отображаются следующие данные:

- данные зашифрованных резервных копий;
- данные зашифрованных управляемых хранилищ;
- данные, резервная копия которых находится на ленточных носителях;
- данные, резервная копия которых находится в облаке;
- Данные, резервная копия которых создана Acronis Backup версий, предшествующих 12.5

Выбор данных резервной копии для восстановления

1. Нажмите **Резервные копии** > **Каталог**.
2. Если на сервере управления зарегистрированы несколько служб каталогизации, выберите службу каталогизации, которая выполнит каталогизацию резервных копий, которые находятся в хранилище.

   Совет *Чтобы увидеть, какая служба каталогизирует хранилище, выберите хранилище в* ***Резервные копии*** > ***Хранилища*** > ***Хранилища****, после чего щелкните* ***Сведения****.*
3. В программном обеспечении отобразятся машины, резервные копии которых находятся в управляемых хранилищах, каталогизированных выбранной службой каталогизации.

   Выберите данные для восстановления через обзор или поиск.

   - **Обзор**

     Дважды щелкните машину, чтобы посмотреть резервные копии дисков, томов, папок и файлов.

     Чтобы восстановить диск, выберите диск, обозначенный указанным ниже значком:

     Чтобы восстановить том, дважды щелкните диск с этим томом и выберите том.

     Чтобы восстановить файлы и папки, найдите том в месте его расположения. Через обзор можно найти тома, которые отмечены значком папки: 
   - **Поиск**

     В поле поиска введите информацию, которая позволит идентифицировать требуемые данные (это может быть имя машины, файла или папки либо метка диска), после чего нажмите кнопку **Поиск**.

     Можно использовать подстановочные символы звездочки (*) и вопросительного знака (?).

     Как результат поиска отобразится список резервных копий данных, имена которых полностью или частично совпадают с введенным значением.
4. По умолчанию данные будут возвращены к состоянию на момент времени создания последней резервной копии. Если выбран один элемент, для выбора точки восстановления можно использовать кнопку **Версии**.
5. Выбрав необходимые данные, выполните один из следующих вариантов.

- Нажмите **Восстановление**, после чего сконфигурируйте параметры операции восстановления в соответствии с описанным на странице«Recovery» (стр. 135) (Восстановление).
- [Только для файлов и папок] Если вы хотите сохранить файл в виде архива с расширением .zip, нажмите кнопку **Загрузить**, выберите, куда вы хотите сохранить данные, и затем нажмите кнопку **Сохранить**.

19.2.6 Рекомендации по каталогизации

Для увеличения производительности каталогизации следуйте рекомендациям ниже.

Установка

Мы рекомендуем устанавливать службу каталогов и узел хранения на отдельные машины. В противном случае, эти компоненты будут конкурировать с ресурсами ЦП и ОЗУ.

Если на сервере управления зарегистрированы несколько узлов хранения, одной службы каталогов будет достаточно без потери производительности индексирования и поиска. Например, если наблюдается работа каталогизации в режиме 24/7 (что означает отсутствие пауз между действиями каталогизации), установите еще одну службу каталогов на отдельную машину. Затем удалите некоторые управляемые хранилища и заново создайте их с новой службой каталогов. Резервные копии, сохраненные в этих хранилищах, будут оставаться без изменений.

Требования к системе

Параметр	Минимальное значение	Рекомендуемое значение
Количество ядер ЦП	2	4 и более
ОЗУ	8 ГБ	16 ГБ и более
Жесткий диск	Жесткий диск 7200 об/мин	SSD (твердотельный накопитель)
Сетевое подключение между машиной с узлом хранения и машиной со службой каталогов	100 Мбит/с	1 Гбит/с

20 Настройки системы

Эти настройки доступны только в локальных развертываниях.

Чтобы получить доступ к этим настройкам, щелкните **Настройки** > **Настройки системы**.

Раздел **Настройки системы** видим только для администраторов организации (стр. 286).

20.1 Уведомления по электронной почте

Можно задать глобальные настройки, общие для всех уведомлений, отправляемых по электронной почте с сервера управления.

В окне Параметры восстановления по умолчанию (стр. 285) пользователь может переопределить эти параметры исключительно для событий, возникающих во время резервного копирования. В этом случае глобальные настройки будут иметь силу для операций, не являющихся операциями резервного копирования.

При создании плана резервного копирования (стр. 117) можно выбрать, какие настройки будут использоваться: глобальные настройки или настройки, указанные в параметрах резервного копирования по умолчанию. Можно переопределить их, заменив на пользовательские значения, относящееся только к данному плану.

Важно! *При изменении глобальных настроек уведомлений по электронной почте будут изменены все планы резервного копирования, в которых используются глобальные настройки.*

Перед настройкой этих параметров обязательно настройте параметры **почтового сервера** (стр. 284).

Для определения глобальных настроек почтовых уведомлений

1. Выберите **Настройки** > **Настройки системы** > **Уведомления по электронной почте**.
2. В поле **Адрес электронной почты получателя** введите адрес электронной почты получателя. Можно указать несколько адресов, разделяя их точкой с запятой.
3. [Необязательно] В поле **Тема** измените тему уведомления по электронной почте.

   Можно использовать следующие переменные:

   - **`[Alert]`**: сводка оповещений
   - **`[Device]`**: имя устройства
   - **`[Plan]`**: название плана, для которого создано оповещение.
   - **`[ManagementServer]`**: имя хоста машины, на которой установлен сервер управления.
   - **`[Unit]`**: название отдела, которому принадлежит машина.

   Тема по умолчанию: **`[Alert]` устройство: `[Device]` План: `[Plan]`**
4. [Необязательно] Установите флажок **Ежедневные краткие сведения об активных оповещениях**, а затем выполните следующие действия:
   a. Укажите время отправки кратких сведений.
   b. [Необязательно] Установите флажок **Не отправлять сообщения «Нет активных оповещений»** .
5. [Необязательно] Выберите язык, который будет использоваться в уведомлениях по электронной почте.
6. Установите флажки для событий, о которых необходимо получать уведомления. Их можно выбрать из списка всех возможных оповещений, сгруппированных по степени серьезности.
7. Нажмите кнопку **Сохранить**.

20.2 Почтовый сервер

Можно указать почтовый сервер, который будет использоваться для отправки уведомлений с сервера управления.

Выбор почтового сервера

1. Последовательно выберите пункты **Настройки** > **Настройки системы** > **Почтовый сервер**.
2. В разделе **Почтовая служба** выберите один из перечисленных ниже пунктов.
   - **Пользовательские**
   - **Gmail**

     В учетной записи Gmail должен быть включен параметр **Ненадежные приложения**. Дополнительную информацию см. по ссылке https://support.google.com/accounts/answer/6010255.
   - **Yahoo Mail**

- **Outlook.com**

3. [Только для пользовательской почтовой службы] Задайте указанные ниже настройки.
   - В поле **Сервер SMTP** введите имя сервера исходящей почты (SMTP).
   - В поле **Порт SMTP** укажите порт сервера исходящей почты. По умолчанию это порт 25.
   - Укажите, следует ли использовать шифрование SSL или TLS. Выберите **Нет**, чтобы отключить шифрование.
   - Если SMTP требует выполнять проверку подлинности, установите флажок **Для сервера SMTP требуется проверка подлинности**, а затем укажите учетные данные учетной записи, которая будет использоваться для отправки сообщений. Если вы не уверены, требует ли сервер SMTP проверки подлинности, обратитесь за помощью к сетевому администратору или поставщику услуг электронной почты.
4. [Только для Gmail, Yahoo Mail и Outlook.com] Укажите данные учетной записи, которая будет использоваться для отправки сообщений.
5. [Только для пользовательской почтовой службы] В поле **Отправитель** введите имя отправителя. Это имя будет указываться в поле **От** уведомлений по электронной почте. Если оставить это поле пустым, в сообщениях будет указана учетная запись, заданная на шаге 3 или 4.
6. [Необязательно] Щелкните **Отправить тестовое сообщение**, чтобы проверить, правильно ли работают уведомления по электронной почте с заданными настройками. Введите адрес электронной почты, на который следует отправить тестовое сообщение.

20.3 Обновления

Этот параметр определяет, будет ли Acronis Backup проверять наличие новой версии при каждом входе администратора организации на консоль резервного копирования.

Значение по умолчанию: **Включено**.

Если этот параметр отключен, администратор может проверить обновления вручную, как описано в разделе «Проверка наличия обновлений программного обеспечения» (стр. 53).

20.4 Параметры резервного копирования по умолчанию

Параметры резервного копирования (стр. 106) по умолчанию являются общими для всех планов резервного копирования на сервере управления. При создании плана резервного копирования вы можете записать поверх заданных по умолчанию значений свои пользовательские значения для конкретного плана.

Для некоторых параметров резервного копирования вы можете настроить используемый по умолчанию параметр, изменив его предопределенное значение. Новое значение будет использовано по умолчанию для всех планов резервного копирования, которые будут созданы на этой машине после внесения изменений.

Для изменения используемых по умолчанию параметров

1. Нажмите **Настройки** > **Настройки системы**.
2. Увеличьте область раздела **Параметры резервного копирования по умолчанию**.
3. Выберите параметр и внесите необходимые изменения.
4. Нажмите кнопку **Сохранить**.

21 Управление учетными записями пользователей и отделами организации

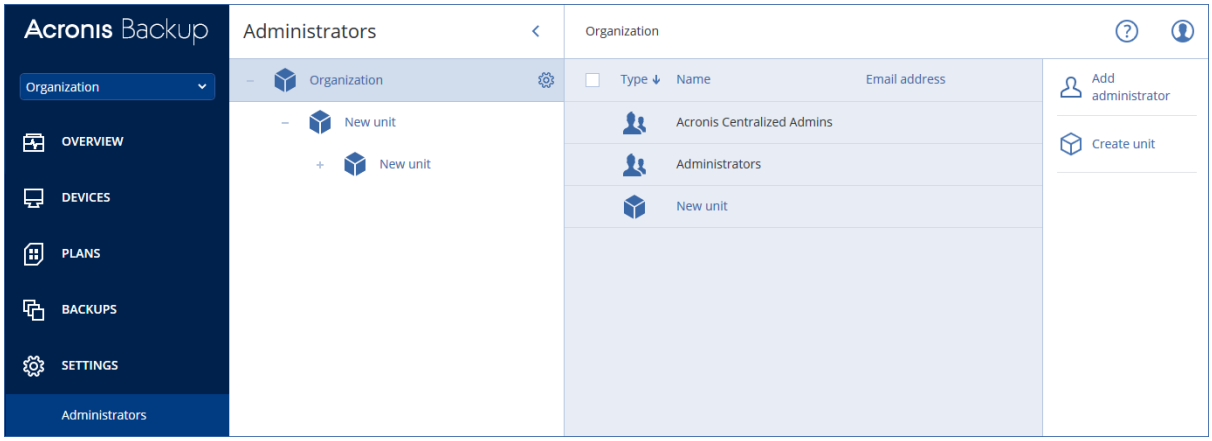
21.1 Локальное развертывание

Функциональные возможности, описанные в этом разделе, доступны только для администраторов организации (стр. 286).

Для получения доступа к этим настройкам нажмите **Настройки** > **Администраторы**.

21.1.1 Администраторы и отделы

На панели **Администраторы** отображается группа **Организация** с деревом отделов (при наличии) и список администраторов отдела, который выбран в дереве.



Кто такие администраторы сервера управления?

Любой пользователь, учетная запись которого позволяет войти в консоль резервного копирования, является администратором сервера управления.

Администраторы организации — это администраторы высшего уровня. *Администраторы отдела* — это администраторы дочерних групп (отделов).

В консоли резервного копирования у каждого администратора есть подконтрольная область. Администратор может просматривать и управлять элементами на своем уровне иерархии или на уровнях ниже.

Кто такие администраторы по умолчанию?

В ОС Windows

При установке сервера управления на машине происходит следующее:

- Группа пользователей **Централизованные администраторы Acronis** создается на машине.

  На контроллере домена группе присваивается название *DCNAME* **$ Централизованные администраторы Acronis**; где *DCNAME* означает имя NetBIOS контроллера домена.
- Все члены группы **«Администраторы»** добавлены в группу **Acronis Centralized Admins**.

  На домене контроллера сама группа **«Администраторы»** включена в группу **Acronis Centralized Admins**

- Группы **Acronis Centralized Admins** и **«Администраторы»** добавлены к серверу управления как **администраторы организации**.

Можно удалить группу **«Администраторы»** из списка администраторов организации. Однако группа **Acronis Centralized Admins** не может быть удалена. В маловероятном случае, если удалены все администраторы организации, в Windows можно добавить учетную запись в группу **Acronis Centralized Admins**, а затем войти в консоль резервного копирования используя эту учетную запись.

В ОС Linux

При установке сервера управления на машину пользователь **root** добавляется на сервер управления в качестве **администратора организации**.

Можно добавить других пользователей Linux в список администраторов сервера управления, как описано далее, а затем удалить пользователя **root** из этого списка. В маловероятном случае, если удалены все администраторы организации, можно перезапустить службу `acronis_asm`. В результате пользователь **root** будет автоматически заново добавлен в качестве администратора организации.

Кто может быть администратором?

Если на машине Windows, включенной в домен Active Directory, установлен сервер управления, любой локальный пользователь или пользователь домена, или группа пользователей могут быть добавлены к администраторам сервера управления. В противном случае, могут быть добавлены только локальные пользователи и группы.

Информацию о добавлении администратора к серверу управления см. в разделе «Добавление администраторов» (стр. 288).

Отделы и администраторы отделов

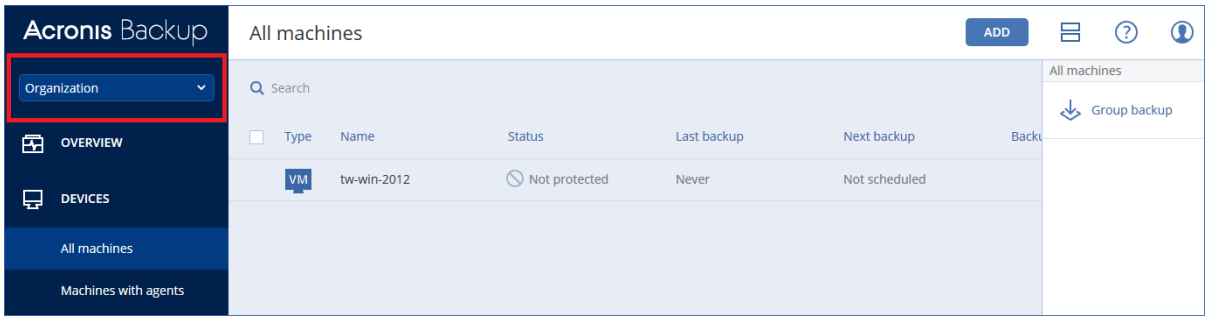
Группа **Организация** автоматически создается при установке сервера управления. При наличии лицензии Acronis Backup Advanced можно создать дочерние группы, называемые «отделами», которые, как правило, соответствуют отделам или подразделениям организации, и добавить в них администраторов.

Таким образом, можно делегировать управление резервным копированием другим пользователям, для которых разрешения на доступ явным образом ограничены соответствующими отделами.

Информацию о том, как создать отдел, см. в разделе «Создание отдела» (стр. 289).

Что делать, если учетная запись добавлена нескольким отделам?

Учетная запись **администратора отдела** может быть добавлена любому количеству отделов. Для такой учетной записи, а также для администраторов организации в консоли резервного копирования отображается селектор отдела. С помощью этого селектора администратор может просматривать и управлять каждым отделом раздельно.



Для учетной записи, которая имеет разрешения на все отделы, отсутствуют разрешения на организацию. Администраторы организации должны быть добавлены в группу **Организация** явным образом.

Как заполнить отделы данными о машинах?

Когда администратор добавляет машину с помощью веб-интерфейса (стр. 36), она добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, машина добавляется отдел, выбранный с помощью селектора. Следовательно, администратору необходимо выбрать отдел перед тем, как щелкнуть **Добавить**.

При локальной установке агентов (стр. 42) администратор предоставляет свои учетные данные. Машина добавляется в отдел, управляемый администратором. Если администратор управляет несколькими отделами, установщик попросит выбрать, в какой отдел добавить машину.

21.1.2 Добавление администраторов

Порядок добавления администраторов

1. Нажмите **Настройки** > **Администраторы**.

   Программное обеспечение отобразит список администраторов сервера управления и дерево отделов (при его наличии).
2. Выберите **Организация** или выберите отдел, в котором необходимо добавить администратора.
3. Нажмите кнопку **Добавить администратора**.
4. В окне **Домен** выберите домен, содержащий учетные записи, которые необходимо добавить Если сервер управления не входит в домен Active Directory или установлен в Linux, могут быть добавлены только локальные пользователи.
5. Выполните поиск имени пользователя или имени группы пользователей.
6. Нажмите «+» рядом с именем пользователя или группы.
7. Повторите шаги 4-6 для всех пользователей или групп, которые необходимо добавить.
8. По окончании нажмите **Готово**.
9. [Только в Linux] Добавьте имена пользователей в Acronis Linux Pluggable Authentication Module (PAM), как описано ниже.

Порядок добавления имен пользователя в Acronis Linux PAM

1. На машине, где работает сервер управления, в текстовом редакторе откройте файл **/etc/security/acronisagent.conf** от имени привилегированного пользователя.
2. В этом файле введите имена пользователей, которые добавлены как администраторы сервера управления. В каждой строке должно быть по одному имени.
3. Сохраните и закройте файл.

21.1.3 Создание отделов

1. Нажмите **Настройки** > **Администраторы**.
2. Программное обеспечение отобразит список администраторов сервера управления и дерево отделов (при его наличии).
3. Выберите **Организация** или выберите родительский отдел для нового отдела.
4. Нажмите **Создать отдел**.
5. Укажите имя нового отдела и затем нажмите **Создать**.

21.2 Облачное развертывание

Управление учетными записями пользователей и отделами организации доступно на портале управления. Для доступа к порталу управления щелкните **Портал управления** при входе в сервис резервного копирования или щелкните **Управление учетными записями** в верхнем левом углу консоли резервного копирования. Доступ к порталу могут получить только те пользователи, которые имеют права администратора.

Информацию об администрировании учетных записей пользователя и отделов организации см. в документе «Руководство администратора портала управления». Для доступа к этому документу щелкните значок вопроса на портале управления.

В этом разделе предоставлена дополнительная информация по управлению сервисом резервного копирования.

Квоты

Можно указать квоту облачного хранилища данных и максимальное количество машин/устройств/почтовых ящиков, которые может защитить пользователь. Чтобы задать квоты, выберите пользователя на вкладке **Пользователи**, затем щелкните значок карандаша в разделе **Квоты**.

Доступны указанные ниже квоты:

- **Рабочие станции**
- **Серверы**
- **Windows Server Essentials**
- **Виртуальные хосты**
- **Мобильные устройства**
- **Почтовые ящики Office 365**
- **Облачное хранилище**

Машина/почтовый ящик считаются защищенными, если к ним применен как минимум один план резервного копирования. Мобильное устройство становится защищенным после первого резервного копирования.

При превышении квоты на адрес электронной почты пользователя отправляется оповещение. Если превышение квоты не задано, квота рассматривается как «мягкая». Это значит, что ограничения по использованию сервиса резервного копирования, не применяются.

Также можно задать превышения квоты. Превышение позволяет превысить квоты на указанное значение. При превышении квоты хранения резервное копирование не выполняется. При превышении количества устройств пользователь не может применить план резервного копирования к дополнительным устройствам.

Внимание! *Если квота и ее превышение будут одновременно иметь нулевые значения, то соответствующая функциональность будет скрыта от пользователя.*

Уведомления

Чтобы изменить настройки уведомлений для пользователя, выберите пользователя на вкладке **Пользователи**, затем щелкните значок карандаша в разделе **Настройки**. Доступны следующие настройки уведомлений:

- **Отправлять рабочие уведомления** (включено по умолчанию)

  Оповещения о превышенных квотах.
- **Сбой резервного копирования**, **Резервное копирование выполнено с предупреждениями** и **Резервное копирование выполнено успешно** (отключено по умолчанию)

  Уведомления о результатах резервного копирования для каждого устройства.
- **Ежедневные краткие сведения об активных оповещениях** (включено по умолчанию)

  Краткие сведения о неудавшихся процессах резервного копирования, отсутствующих процессах резервного копирования и других проблемах. Краткие сведения отправляются в 10:00 (время центра обработки данных)). Если по состоянию на данный момент никаких проблем не возникало, краткие сведения не отправляются.

Все уведомления отправляются на адрес электронной почты пользователя.

Отчеты

В отчете об использовании сервиса резервного копирования содержатся следующие данные об организации или отделе:

- Размер резервных копий по отделам, учетным записям и типам устройств.
- Количество защищенных устройств по отделам, учетным записям и типам устройств.
- Цена по отделам, учетными записям, типам устройств.
- Общий размер резервных копий.
- Общее количество защищенных устройств.
- Общая стоимость.

22 Устранение неисправностей

В этом разделе объясняется, как сохранить журнал агента в ZIP-файл. Этот файл поможет сотрудникам технической поддержки определить проблему в случае неудачного резервного копирования по неясной причине.

Получение журналов

1. Выполните одно из следующих действий:

- В разделе **Устройства** выберите машину, на которой необходимо собрать журналы, и нажмите кнопку **Действия**.
- В разделе **Настройки** > **Агенты** выберите машину, на которой необходимо собрать журналы, и нажмите кнопку **Подробнее**.

2. Нажмите кнопку **Сбор сведений о системе**.
3. Укажите расположение для сохранения файла, если поступит соответствующий запрос веб-браузера.

Заявление об авторских правах

Запатентованные технологии Acronis

Технологии, которые использованы в этом продукте, регламентированы и защищены одним или несколькими нижеуказанными патентами США: 7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; а также патентами, ожидающими выдачи.

23 Словарь терминов

Д

Дифференциальное резервное копирование

В дифференциальной резервной копии хранятся изменения, произведенные в данных относительно самой поздней версии полной (стр. 293) резервной копии. Для восстановления данных из дифференциальной резервной копии необходимо иметь доступ к полной резервной копии.

И

Инкрементное резервное копирование

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.

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 выберите **Параметры резервного копирования** > **Еженедельная резервная копия**).
- Ежедневная резервная копия — это первая копия, которая создается после начала дня.
- Почасовая резервная копия — это первая копия, которая создается после начала месяца.

П

Полная резервная копия

Самостоятельная резервная копия, содержащая все необходимые данные. Для восстановления данных полной резервной копии не требуется иметь доступ к любой другой резервной копии.

У

Управляемое хранилище

Узел хранения обеспечивает управление хранилищем резервных копий.

Физически управляемое хранилище может находиться на общем сетевом ресурсе, в сети хранения данных (SAN), в сетевом хранилище данных (NAS), на локальном жестком диске узла хранения или в библиотеке ленточных носителей, локально подключенной к узлу хранения. Узел хранения выполняет очистку и проверку (если таковые включены в план резервного копирования) для каждой резервной копии в управляемом хранилище. Вы можете указать дополнительные операции, которые должен выполнять узел хранения (дедупликация, шифрование).

Ф

Формат резервной копии в виде одного файла

Новый формат резервных копий, в котором начальная полная и последующие инкрементные резервные копии сохраняются в одном TIB-файле вместо цепочки файлов. 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, например, на сервера SFTP.